The weight distribution of a family of $p$-ary cyclic codes

Long Yu · Hongwei Liu

Abstract Let $m, k$ be positive integers, $p$ be an odd prime and $\pi$ be a primitive element of $\mathbb{F}_{p^m}$. In this paper, we determine the weight distribution of a family of cyclic codes $C_t$ over $\mathbb{F}_p$, whose duals have two zeros $\pi^{-t}$ and $-\pi^{-t}$, where $t$ satisfies $t \equiv \frac{p^k+1}{2} p^\tau \pmod{p^{m-1}}$ for some $\tau \in \{0, 1, \ldots, m-1\}$.

Keywords Cyclic code · Quadratic form · Weight distribution

Mathematics Subject Classification 11T71 · 94B15

1 Introduction

Let $p$ be an odd prime and $q$ be a power of $p$. An $[n, k, d]$ linear code over the finite field $\mathbb{F}_q$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance $d$. A linear code $C$ of length $n$ is called cyclic if $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies that $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. By identifying a codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$ with the polynomial $c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \in \mathbb{F}_q[X]/(X^n - 1)$, a cyclic code $C$ of length $n$ over $\mathbb{F}_q$ corresponds to an ideal of $\mathbb{F}_q[X]/(X^n - 1)$. The generator $g(X)$ is required to have the least degree among all generators of the ideal. The monic generator $g(X)$ of a nonzero ideal is called the generator polynomial of the nonzero code $C$, which satisfies that $g(X)|(X^n - 1)$. The polynomial $h(X) = (X^n - 1)/g(X)$ is referred to as the parity-check polynomial of $C$ [14].
Let $A_i$ denote the number of codewords with Hamming weight $i$ in a linear code $C$ of length $n$. The weight enumerator of $C$ is defined by

$$A_0 + A_1X + A_2X^2 + \cdots + A_nX^n, \quad \text{where } A_0 = 1.$$ 

The sequence $(A_0, A_1, \ldots, A_n)$ is called the weight distribution of the code $C$. In general, the weight distribution of cyclic codes is difficult to determine. There are some results on the weight distribution of cyclic codes whose duals have two or more zeros (see [2,3,5,6,8,10–12,15–26]).

Let $\mathbb{Z}_m$ be the residue ring modulo an integer $m$, $\Gamma_i$ be the $p$-cyclotomic coset modulo $p^m - 1$ containing $i$, i.e.,

$$\Gamma_i = \{i \cdot p^j \mod p^m - 1 \mid j = 0, 1, \ldots, m - 1\},$$

where $i \in \mathbb{Z}_{p^m - 1}$. A subset $\{i_1, i_2, \ldots, i_r\}$ of $\{0, 1, \ldots, p^m - 2\}$, where $r \geq 1$, is called a complete set of representatives of all $p$-cyclotomic cosets modulo $p^m - 1$ if $\Gamma_{i_1}, \Gamma_{i_2}, \ldots, \Gamma_{i_r}$ are pairwise disjoint and $\bigcup_{k=1}^{r} \Gamma_{i_k} = \{0, 1, \ldots, p^m - 2\}$.

Throughout this paper, we assume that $m, k$ are positive integers, $\pi$ is a primitive element of $\mathbb{F}_{p^m}$ and $\zeta_p$ is a complex primitive $p$-th root of unity. Let $t$ be an integer such that $(\pi^t)^{p^k} \neq -\pi^t$ for all $i \in \mathbb{Z}_m$. Let $h_1(x)$ and $h_2(x)$ be the minimal polynomials of $\pi^{-t}$ and $-\pi^{-t}$ over $\mathbb{F}_p$, respectively. In this paper, we let $h(x) = h_1(x)h_2(x)$ and $C_t$ be the cyclic code with parity-check polynomial $h(x)$. By the well-known Delsarte’s Theorem [1], the cyclic code $C_t$ can be expressed as

$$C_t = \left\{ \mathbf{c}(a, b) = \left( \text{Tr}^{m}_{1}(a\pi^{t}\alpha + b(-\pi^{t})^{i}) \right)_{i=0}^{p^m-2} \mid a, b \in \mathbb{F}_{p^m} \right\}, \quad (1.1)$$

where $\text{Tr}^{m}_{1}(\cdot)$ is the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. In particular, in the case of $t = 1$, Vega and Wolfmann in [17] have studied the cyclic code $C_1$. They constructed this class of cyclic codes from the direct sum of two one-weight irreducible cyclic codes for odd $m$ and proved that $C_1$ has only two nonzero weights. In [13], Ma et al. further investigated the cyclic code $C_1$ for the case of even $m$, and gave the weight distribution of the code $C_1$.

The goal of this paper is to determine the weight distribution of a family of the cyclic codes $C_t$ over $\mathbb{F}_p$ defined by (1.1) in the case of $t \equiv \frac{p^k + 1}{2}p^{r} \mod \frac{p^m - 1}{2}$ for some $\tau \in \mathbb{Z}_m$. By applying the value distribution of the exponential sum $\sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{x\alpha(x\pi^{b} + 1)}$, $\alpha \in \mathbb{F}_{p^m}$, which is given in [4,7,9], we obtain the value distribution of the exponential sum $\sum_{a \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \left( \zeta_p^{a\text{Tr}^{m}_{1}((a+b)x\pi^{b} + 1)} + \zeta_p^{a\text{Tr}^{m}_{1}((a-b)\pi^{b/2} + x\pi^{b} + 1)} \right)$, $a, b \in \mathbb{F}_{p^m}$. Based on these results, we characterize the weight distribution of the code $C_t$ defined by (1.1).

This paper is organized as follows. Section 2 gives some basic definitions and results over finite fields. In Sect. 3, we determine the weight distribution of a family of cyclic codes $C_t$ defined by (1.1) over $\mathbb{F}_p$.

## 2 Preliminaries

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, where $q$ is a power of an odd prime $p$. In the following, we give a brief introduction to the theory of quadratic forms over finite fields, which is needed to calculate the weight distribution of the cyclic codes in the next section.
Quadratic forms have been well studied ([9]), and they have many applications in sequence design and coding theory.

**Definition 2.1** Let \( \{\omega_1, \omega_2, \ldots, \omega_s\} \) be a basis for \( \mathbb{F}_{q^s} \) over \( \mathbb{F}_q \) and \( x = \sum_{i=1}^{s} x_i \omega_i \), where \( x_i \in \mathbb{F}_q \). A function \( f(x) \) from \( \mathbb{F}_{q^s} \) to \( \mathbb{F}_q \) is called a quadratic form if it can be represented as

\[
f(x) = f\left(\sum_{i=1}^{s} x_i \omega_i\right) = \sum_{1 \leq i \leq j \leq s} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{F}_q.
\]

The rank of the quadratic form \( f(x) \) is defined as the codimension of the \( \mathbb{F}_q \)-vector space

\[
V = \{x \in \mathbb{F}_{q^s} | f(x + z) - f(x) - f(z) = 0, \text{ for all } z \in \mathbb{F}_{q^s}\},
\]

denoted by rank \((f)\). Then \( |V| = q^{s - \text{rank}(f)} \).

For a quadratic form \( f(x) \) with \( s \) variables over \( \mathbb{F}_q \), there exists a symmetric matrix \( A \) of order \( s \) over \( \mathbb{F}_q \) such that \( f(x) = XAX' \), where \( X = (x_1, x_2, \ldots, x_s) \in \mathbb{F}_q^s \) and \( X' \) denotes the transpose of \( X \). It is known that there exists a nonsingular matrix \( T \) over \( \mathbb{F}_q \) such that \( TAT' \) is a diagonal matrix [9]. Making a nonsingular linear substitution \( X = ZT \) with \( Z = (z_1, z_2, \ldots, z_s) \in \mathbb{F}_q^s \), we have

\[
f(x) = Z(TAT')Z' = \sum_{i=1}^{r} a_i z_i^2, \quad a_i \in \mathbb{F}_q^*,
\]

where \( r \) is the rank of \( f(x) \).

**Definition 2.2** Let \( j \) be a positive integer. The 2-adic valuation of \( j \), denoted by \( v_2(j) \), which is the maximum integer \( k \) such that \( 2^k | j \).

We denote the quadratic character of \( \mathbb{F}_{p^m} \) by

\[
\eta_m(x) = \begin{cases} 
0, & \text{if } x = 0; \\
x^{p^m-1}x^{-\frac{x}{2}}, & \text{if } x \in \mathbb{F}_{p^m}^*.
\end{cases}
\]

**Lemma 2.3** [4,7] Let \( k, m \) be positive integers. Then

\[
gcd(p^k + 1, p^m - 1) = \begin{cases} 
p^{\gcd(k, m)} + 1, & \text{if } v_2(m) > v_2(k); \\
2, & \text{otherwise}.
\end{cases}
\]

The following lemma could be found in [4,7,9].

**Lemma 2.4** [4,7,9] Let \( T_\alpha(x) = \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{T_\alpha^m(x)} \zeta_p^{\alpha x^k+1} \), where \( k \) is a positive integer. Then for any \( \alpha \in \mathbb{F}_{p^m} \),

- if \( v_2(k) \geq v_2(m) \), then

\[
T_\alpha(x) = \begin{cases} 
\eta_m(\alpha)(-1)^{m-1} p^{\frac{m}{2}}, & \text{if } p \equiv 1 \pmod{4}; \\
\eta_m(\alpha)(\sqrt{-1})^{m-1} p^{\frac{m}{2}}, & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

- if \( v_2(k) + 1 = v_2(m) \), then

\[
T_\alpha(x) = \begin{cases} 
p^{\frac{m}{2}+d}, & \text{times; } \frac{p^{m-1}}{p^d+1} \times; \\
p^{\frac{m}{2}}, & \text{times; } \frac{p^{m-1}}{p^d+1} \times; \\
p^m, & \text{1 time}.
\end{cases}
\]
• if \( v_2(k) + 1 < v_2(m) \), then

\[
T_\alpha(x) = \begin{cases} 
-p^m & \text{times;} \\
p^m - 1 & \text{times;} \\
p^m & \text{times;}
\end{cases}
\]

3 The weight distribution of the code \( C_t \)

In this section, we let \( n = p^m - 1 \). For a given positive divisor \( l \) of \( m \), the trace function from \( \mathbb{F}_{p^m} \) to \( \mathbb{F}_{p^l} \) is defined by \( \text{Tr}_{p^l}^m(x) = \sum_{i=0}^{m-1} x^{p^i} \), where \( x \in \mathbb{F}_{p^m} \). Let \( SQ \) denote the set of square elements in \( \mathbb{F}_{p^m}^* \), \( SQ_p \) denote the set of square elements in \( \mathbb{F}_p^* \) and let \( u_p \) be a primitive element in \( \mathbb{F}_p \). In the following, we compute the weight of the codeword \( c(a, b) \in C_t \) defined by (1.1):

\[
\text{wt}(c(a, b)) = \# \{0 \leq i \leq p^m - 2 : c_i \neq 0\} = n - \frac{1}{p} \sum_{i=0}^{p^m-2} \sum_{u \in \mathbb{F}_p} \xi_p \text{Tr}_{p^l}^m(a \pi^{ti} + b(-\pi^t)^i)
\]

\[
= n - \frac{1}{p} \sum_{u \in \mathbb{F}_p} \sum_{i=0}^{p^m-3} \left( \xi_p \text{Tr}_{p^l}^m(a \pi^{2ti} + b(-\pi^{2t})^{2i}) + \xi_p \text{Tr}_{p^l}^m(a \pi^{(2i+1)t} + b(-\pi^{(2i+1)t})^{2(2i+1)}) \right)
\]

\[
= n - \frac{1}{p} \sum_{u \in \mathbb{F}_p} \sum_{x \in SQ} \left( \xi_p \text{Tr}_{p^l}^m(a \pi^x + bx^2) + \xi_p \text{Tr}_{p^l}^m(a \pi^x - bx^2) \right)
\]

\[
= n - \frac{1}{2p} \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}^*} \left( \xi_p \text{Tr}_{p^l}^m((a+b)x^2) + \xi_p \text{Tr}_{p^l}^m((a-b)x^2) \right). \tag{3.1}
\]

Therefore, we have the following lemma.

**Lemma 3.1** Let the notations be the same as above. If \( t, e \in \mathbb{Z}_{p^m-1} \) are two positive integers such that \( t \equiv ep^\tau \pmod{\frac{p^m-1}{2}} \) for some \( \tau \in \mathbb{Z}_m \), then the cyclic codes \( C_t \) and \( C_e \) defined by (1.1) have the same weight distribution.

**Proof** By (3.1), we have that the weight distribution of \( C_t \) and \( C_e \) are respectively determined by the value distribution of

\[
\Delta_t = \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}^*} \left( \xi_p \text{Tr}_{p^l}^m((a+b)x^2) + \xi_p \text{Tr}_{p^l}^m((a-b)x^2) \right)
\]

and

\[
\Delta_e = \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}^*} \left( \xi_p \text{Tr}_{p^l}^m((a+b)x^2) + \xi_p \text{Tr}_{p^l}^m((a-b)x^2) \right).
\]
Let $e \equiv rp^{m-\tau} \pmod{p^m - 1}$, then the integers $t$ and $r$ satisfy $t \equiv r \pmod{\frac{p^m - 1}{2}}$, i.e. $t = r + l\frac{p^m - 1}{2}$ for some integer $l$. Hence

$$\Delta_t = \sum_{u \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \left( \zeta_p u \text{Tr}_1^m((a+b)x^{2t}) + \zeta_p u \text{Tr}_1^m((a-b)x^{2t}) \right)$$

$$= \sum_{u \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \left( \zeta_p u \text{Tr}_1^m((a+b)x^{2r+1}(p^m-1)) + \zeta_p u \text{Tr}_1^m((a-b)p^{r+1}x^{2r+1}(p^m-1)) \right)$$

$$= \sum_{u \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \left( \zeta_p u \text{Tr}_1^m((a+b)x^{2r}) + \zeta_p u \text{Tr}_1^m((a-b)x^{2r}) \right)$$

$$= \Delta_r$$

where the fourth identity is obtained by $u^2 \equiv u \pmod{p^m}$. As we know, $\{\Delta_r | a, b \in \mathbb{F}_{p^m}\} = \{\Delta_e | a, b \in \mathbb{F}_{p^m}\}$, since $e \equiv rp^{m-\tau} \pmod{p^m - 1}$. Therefore, the multi-sets $\{\Delta_r | a, b \in \mathbb{F}_{p^m}\}$ and $\{\Delta_e | a, b \in \mathbb{F}_{p^m}\}$ have the same value distribution. \hfill \qed

In this section, we study the weight distribution of the cyclic codes $C_t$ in the case of $t \equiv \frac{p+1}{2}p^r \pmod{\frac{p^m-1}{2}}$ for some $\tau \in \mathbb{Z}_m$. By Lemma 3.1, we have that the codes $C_t$ and $C_{p^{k+1}/2}$ have the same weight distribution. In order to determine the weight distribution of the code $C_t$, we just need to obtain the weight distribution of the code $C_{p^{k+1}/2}$. In the following, we calculate the weight distribution of the cyclic code $C_{p^{k+1}/2}$. By (1.1), we have

$$C_{p^{k+1}/2} = \left\{ c(a, b) = \left( \text{Tr}_1^m \left( a \pi^i \frac{p^{k+1}}{2} + b(-\pi^{k+1/2})^i \right) \right)^{p^m-2} | a, b \in \mathbb{F}_{p^m} \right\}, \tag{3.2}$$

whose dual has two zeros $\pi^{-\frac{p^{k+1}}{2}}$ and $-\pi^{-\frac{p^{k+1}}{2}}$, where $k$ satisfies $\pi^{-\frac{p^{k+1}}{2}-p^i} \neq -\pi^{-\frac{p^{k+1}}{2}}$ for all $i \in \mathbb{Z}_m$. Let $h_1(x)$ and $h_2(x)$ be the minimal polynomials of $\pi^{-\frac{p^{k+1}}{2}}$ and $-\pi^{-\frac{p^{k+1}}{2}}$ over $\mathbb{F}_p$, respectively. Then we have the following lemma.

**Lemma 3.2** Let the notations be the same as above. The degrees of $h_1(x)$ and $h_2(x)$ are both $m$.

**Proof** In order to calculate the degree of $h_1(x)$, we need to compute the size of $\Gamma_{p^{k+1}/2}$. Let the size of $\Gamma_{p^{k+1}/2}$ be $l$. Note that $\frac{p^{k+1}}{2}p^m \equiv \frac{p^{k+1}}{2} \pmod{p^m - 1}$, then we get that $l \mid m$. On the other hand, we have

$$\frac{p^k + 1}{2}p^l \equiv \frac{p^k + 1}{2} \pmod{p^m - 1},$$

which implies that

$$2(p^m - 1) \mid (p^k + 1)(p^l - 1). \tag{3.3}$$

\hfill \qed
Case I, when \(v_2(k) \geq v_2(m)\): By Lemma 2.3, we have \(\gcd(p^k + 1, p^m - 1) = 2\). From (3.3), we get \(m \mid l\). Since \(l \mid m\), hence, \(m = l\).

Case II, when \(v_2(k) < v_2(m)\): In this case, we obtain that \(\gcd(p^k + 1, p^m - 1) = p^d + 1\) by Lemma 2.3. From (3.3), we have \(2^{\frac{p^m-1}{p^d+1}} \mid (p^l - 1)\). Since \(v_2(k) < v_2(m)\), then \(p^d - 1 \mid p^m - 1\), which implies that \(p^d - 1 \mid 2^{\frac{p^m-1}{p^d+1}}\). This shows that \(p^d - 1 \mid p^l - 1\), i.e., \(d \mid l\). Let \(l = hd, m = sd\), where \(h \mid s\) since \(l \mid m\). From (3.3), we have

\[
2(p^{sd} - 1) \mid (p^d + 1)(p^{hd} - 1),
\]

which implies that \(h = s\). Then \(l = m\).

Similarly, we also get that the degree of \(h_2(x)\) is \(m\). \(\square\)

From (3.1), the weight of \(c(a, b) \in C_{\frac{p^k+1}{2}}\) can be expressed as

\[
wt(c(a, b)) = p^m - p^{m-1} - \frac{1}{2p} \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \left( u \text{Tr}_1^m((a+b)x^{p^k+1}) + u \text{Tr}_1^m((a-b)x^{p^k+1}) \right).
\]

(3.4)

3.1 The weight distribution of \(C_{\frac{p^k+1}{2}}\) for \(v_2(m) > v_2(k)\)

In this subsection, we always assume that \(v_2(m) > v_2(k)\), i.e., \(s = \frac{m}{d}\) is even, where \(d = \gcd(m, k)\). Following the above notations, we let

\[
T(a, b) = \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \left( u \text{Tr}_1^m((a+b)x^{p^k+1}) + u \text{Tr}_1^m((a-b)x^{p^k+1}) \right).
\]

(3.5)

From (3.4), the weight distribution of the cyclic code \(C_{\frac{p^k+1}{2}}\) is completely determined by the value distribution of \(T(a, b)\). To calculate the value distribution of \(T(a, b)\), we need a series of lemmas. Before introducing them, we define

\[
R_\alpha(x) = \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} u \text{Tr}_1^m(\alpha x^{p^k+1}), \quad \alpha \in \mathbb{F}_{p^m}.
\]

Lemma 3.3 Let the notations be the same as above, we have

\[
R_\alpha(x) = (p - 1) \sum_{x \in \mathbb{F}_{p^m}} \text{Tr}_1^m(\alpha x^{p^k+1}).
\]

(3.6)

Proof Note that \(v_2(m) > v_2(k)\), then \(m\) is even and \(\frac{k}{d}\) is odd. Hence, \(u_p = \pi^{\frac{p^m-1}{p^d+1}} = \pi^{p^m-1+\cdots+1}\) is a square element in \(\mathbb{F}_{p^m}\), i.e., \(u_p \in SQ\). Since \(\frac{k}{d}\) is odd and

\[
u_p^{\frac{k}{d}+1} = u_p^{\frac{k}{d}-1+1} = u_p u_p^{\frac{p^m-1}{p^d+1}} = u_p \left( u_p^{\pi -1} \right)^d + \cdots + 1,
\]

\(\square\) Springer
we have that $u_p^{-2} = -u_p$ for odd $d$, and $u_p^{-2} = u_p$ for even $d$, i.e., $u_p^{-2} = (-1)^d u_p$. Using $u_p \in SQ$, we have

$$R_\alpha(x) = \sum_{x \in \mathbb{F}_{p^m}} \sum_{\xi_p} u \text{Tr}_1^m (\alpha x^{p^k+1})$$

$$= \sum_{x \in SQ} \sum_{\xi_p} \left( \text{Tr}_1^m (\alpha x^{p^k+1}) + \xi_p u \text{Tr}_1^m (\alpha x^{p^k+1}) \right)$$

$$= \frac{p - 1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m (\alpha x^{p^k+1}) + \xi_p \text{Tr}_1^m (\alpha x^{p^k+1}) \right)$$

$$= \frac{p - 1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m (\alpha x^{p^k+1}) + \xi_p \text{Tr}_1^m (-\alpha x^{p^k+1}) \right)$$

$$= \left\{ \begin{array}{ll}
(p - 1) \sum_{x \in \mathbb{F}_{p^m}} \xi_p \text{Tr}_1^m (\alpha x^{p^k+1}), & \text{if } d \text{ is even;}

\frac{p - 1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \xi_p \text{Tr}_1^m (\alpha x^{p^k+1}) + \xi_p \text{Tr}_1^m (-\alpha x^{p^k+1}) \right), & \text{if } d \text{ is odd.}
\end{array} \right. \quad (3.7)$$

Since $v_2(m) > v_2(k)$, by Lemma 2.3, we have

$$\gcd \left( p^{k+1}, p^m - 1 \right) = p^d + 1.$$  

Note that $m = sd$ is even, then $2(p^d + 1) \mid p^m - 1$. Hence, we have

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

Since $\frac{k}{d}$ is odd, then $\frac{p^{k+1}}{p^d + 1} = p^{\frac{k}{2} - 1}d - p^{\frac{k}{2} - 2}d + p^{\frac{k}{2} - 3}d - \cdots - p + 1$ is odd, which implies that $(\frac{p^{m-1}}{2(p^d + 1)})^{p^{k+1}} = -1$. Therefore, we have

$$\sum_{x \in \mathbb{F}_{p^m}} \text{Tr}_1^m (\alpha x^{p^k+1}) = \sum_{x \in \mathbb{F}_{p^m}} \xi_p \text{Tr}_1^m \left( \alpha \left( \frac{p^{m-1}}{2(p^d + 1)} x \right)^{p^{k+1}} \right) = \sum_{x \in \mathbb{F}_{p^m}} \xi_p \text{Tr}_1^m (-\alpha x^{p^k+1}).$$

By (3.7), we obtain

$$R_\alpha(x) = (p - 1) \sum_{x \in \mathbb{F}_{p^m}} \xi_p \text{Tr}_1^m (\alpha x^{p^k+1}).$$

$\square$
Applying Lemmas 2.4 and 3.3, we have the following result.

**Lemma 3.4** Let the notations be the same as above.
- If \( v_2(k) + 1 = v_2(m) \), then
  \[
  R_a(x) = \begin{cases} 
  (p - 1)p^m, & 1 \text{ time;} \\
  -(p - 1)p^{\frac{m}{2}}, & p^d(p^d - 1) \text{ times;} \\
  (p - 1)p^m d, & p^{d+1} \text{ times.}
  \end{cases}
  \]
- If \( v_2(k) + 1 < v_2(m) \), then
  \[
  R_a(x) = \begin{cases} 
  (p - 1)p^m, & 1 \text{ time;} \\
  -(p - 1)p^{\frac{m}{2}}, & p^d(p^d - 1) \text{ times;} \\
  (p - 1)p^m d, & p^{d+1} \text{ times.}
  \end{cases}
  \]

**Lemma 3.5** Let the notations be the same as above. Suppose \((a, b)\) runs through \(\mathbb{Z}^2_{p^m}\).
- if \( v_2(k) + 1 = v_2(m) \), then \( T(a, b) \) takes on only the values from the following set
  \[
  \{ 2(p - 1)p^m, (p - 1)(p^m + p^{\frac{m}{2}}), (p - 1)(p^m - p^{\frac{m}{2}}), (p - 1)(p^m - p^{\frac{m}{2}}), \}
  \]
- if \( v_2(k) + 1 < v_2(m) \), then \( T(a, b) \) takes on only the values from the following set
  \[
  \{ 2(p - 1)p^m, (p - 1)(p^m - p^{\frac{m}{2}}), (p - 1)(p^m - p^{\frac{m}{2}}), (p - 1)(p^m - p^{\frac{m}{2}}), \}
  \]

**Proof** By (3.5) and (3.6), we have
\[
T(a, b) = R_{a+b}(x) + R_{(a-b)\pi}^{\frac{x}{2}}(x).
\]
We first discuss the value of \( T(a, b) \) in the case of \( v_2(k) + 1 = v_2(m) \).

Case I, when \( a = b = 0 \): It is easy to check that \( T(a, b) = 2(p - 1)p^m \).

Case II, when \( a = b \neq 0 \): We first discuss the case of \( a = b \neq 0 \), since the other case can be discussed by a similar way. By Lemma 3.4, we have \( R_{a+b}(x) \in \{(p - 1)p^{\frac{m}{2}} + d, -(p - 1)p^{\frac{m}{2}} \} \), and \( R_{(a-b)\pi}^{\frac{x}{2}}(x) = (p - 1)p^m \). Hence, \( T(a, b) \in \{(p - 1)(p^m + p^{\frac{m}{2}} + d), (p - 1)(p^m - p^{\frac{m}{2}}) \} \) in the case of \( a = b \neq 0 \).

Case III, when \( a \neq b, a \neq -b \): By Lemma 3.4, we have \( R_{a+b}(x) \in \{(p - 1)p^{\frac{m}{2}} + d, -(p - 1)p^{\frac{m}{2}} \} \) and \( R_{(a-b)\pi}^{\frac{x}{2}}(x) \in \{(p - 1)p^{\frac{m}{2}} + d, -(p - 1)p^{\frac{m}{2}} \} \). Therefore, \( T(a, b) \in \{2(p - 1)p^{\frac{m}{2}} + d, 2(p - 1)p^{\frac{m}{2}} - 2(p - 1)p^{\frac{m}{2}} \} \).

The case of \( v_2(k) + 1 < v_2(m) \) can be discussed by a similar way as the case of \( v_2(k) + 1 = v_2(m) \). This completes the proof. \( \square \)

With above preparation we can determine the value distribution of the exponential sum \( T(a, b) \) defined by (3.5).
Theorem 3.6 Let the notations be the same as above. Suppose \((a, b)\) runs through \(\mathbb{F}_p^2\),

- if \(v_2(k) + 1 = v_2(m)\), then the value distribution of \(T(a, b)\) is given as follows.

\[
\begin{align*}
2(p - 1)p^m, & \quad 1 \text{ time;} \\
(p - 1)\left(p^m + p^m \pi^d\right), & \quad 2\frac{p^{m-1}}{p^d+1} \text{ times;} \\
(p - 1)\left(p^m - p^m \pi\right), & \quad 2\frac{p^{d(p-1)}}{p^d+1} \text{ times;} \\
(p - 1)\left(p^m + p^m \pi^d\right), & \quad 2\frac{p^d(p_m-1)}{p^d+1} \text{ times;} \\
2(p - 1)p^m + d, & \quad 2\frac{p^d}{p^d+1} \text{ times;} \\
-2(p - 1)p^m, & \quad p^{2d}\left(\frac{p^{m-1}}{p^d+1}\right)^2 \text{ times.}
\end{align*}
\]

- if \(v_2(k) + 1 < v_2(m)\), then the value distribution of \(T(a, b)\) is given as follows.

\[
\begin{align*}
2(p - 1)p^m, & \quad 1 \text{ time;} \\
(p - 1)\left(p^m - p^m \pi^d\right), & \quad 2\frac{p^{m-1}}{p^d+1} \text{ times;} \\
(p - 1)\left(p^m + p^m \pi\right), & \quad 2\frac{p^{d(p-1)}}{p^d+1} \text{ times;} \\
(p - 1)\left(p^m - p^m \pi^d\right), & \quad 2\frac{p^d(p_m-1)}{p^d+1} \text{ times;} \\
-2(p - 1)p^m, & \quad p^{2d}\left(\frac{p^{m-1}}{p^d+1}\right)^2 \text{ times.}
\end{align*}
\]

Proof We only discuss the case of \(v_2(k) + 1 = v_2(m)\), since the other case can be discussed by a similar way. To determine the value distribution of \(T(a, b)\), we define

\[
\begin{align*}
N_1 &= \# \left\{a, b \in \mathbb{F}_p^m \mid T(a, b) = (p - 1)\left(p^m + p^m \pi^d\right)\right\}, \\
N_2 &= \# \left\{a, b \in \mathbb{F}_p^m \mid T(a, b) = (p - 1)\left(p^m - p^m \pi\right)\right\}, \\
N_3 &= \# \left\{a, b \in \mathbb{F}_p^m \mid T(a, b) = (p - 1)\left(p^m + p^m \pi^d\right)\right\}, \\
N_4 &= \# \left\{a, b \in \mathbb{F}_p^m \mid T(a, b) = 2(p - 1)p^m \pi^d\right\}, \\
N_5 &= \# \left\{a, b \in \mathbb{F}_p^m \mid T(a, b) = -2(p - 1)p^m\right\}.
\end{align*}
\]

It is easy to check that the value \(2(p - 1)p^m\) happens only once. Note that the value \((p - 1)(p^m + p^m \pi^d)\) occurs only if \(R_{a+b}(x) = (p - 1)p^m\), \(R_{(a-b)\pi}^k\pi^d(x) = (p - 1)p^m\), or \(R_{a+b}(x) = (p - 1)p^m \pi^d\), \(R_{(a-b)\pi}^k\pi^d(x) = (p - 1)p^m\). By Lemma 3.4, if \(R_{a+b}(x) = (p - 1)p^m\), \(R_{(a-b)\pi}^k\pi^d(x) = (p - 1)p^m\), then we have that the number of \((a, b)\in \mathbb{F}_p^2\) is \(\frac{p^{m-1}}{p^d+1}\). By Lemma 3.4, if \(R_{a+b}(x) = (p - 1)p^m \pi^d\), \(R_{(a-b)\pi}^k\pi^d(x) = (p - 1)p^m\), we get that the number of \((a, b)\in \mathbb{F}_p^2\) is \(\frac{p^{m-1}}{p^d+1}\). Therefore, we have \(N_1 = 2\frac{p^{m-1}}{p^d+1}\). Similarly, we obtain that \(N_2 = 2\frac{p^d(p^{m-1})}{p^d+1}\). On the other hand, we have
By Lemma 3.4, we obtain

$$
N_3 = \# \left\{ a, b \in \mathbb{F}_p^m \mid T(a, b) = R_{a+b}(x) + R_{(a-b)p^{k+1}}(x) = (p - 1) \left(p^\frac{m}{2} + d - p^{\frac{m}{2}}\right) \right\}
$$

$$
= \# \left\{ u, v \in \mathbb{F}_p^m \mid R_u(x) + R_v(x) = (p - 1) \left(p^\frac{m}{2} + d - p^{\frac{m}{2}}\right) \right\}
$$

$$
= \# \left\{ u, v \in \mathbb{F}_p^m \mid R_u(x) = (p - 1)p^\frac{m}{2} + d, R_v(x) = -(p - 1)p^\frac{m}{2} \right\}
$$

$$
+ \# \left\{ u, v \in \mathbb{F}_p^m \mid R_v(x) = (p - 1)p^\frac{m}{2} + d, R_u(x) = -(p - 1)p^\frac{m}{2} \right\}.
$$

By Lemma 3.4, we obtain $N_3 = 2p^d \left(\frac{p^m - 1}{p^d + 1}\right)^2$. Similarly, we get

$$
N_4 = \left(\frac{p^m - 1}{p^d + 1}\right)^2, \quad N_5 = p^{2d} \left(\frac{p^m - 1}{p^d + 1}\right)^2.
$$

This finishes the proof. ☐

**Theorem 3.7** Let the notations be the same as above.

- If $v_2(k) + 1 = v_2(m)$, then $C_{\frac{k}{2} + 1}$ is a cyclic code over $\mathbb{F}_p$ with parameters $\{p^m - 1, 2m, \frac{p^m - 1}{p^d}(p^{m-1} - p^{\frac{m}{2} + d-1})\}$ and the weight distribution of $C_{\frac{k}{2} + 1}$ is given in Table 1.
- If $v_2(k) + 1 < v_2(m)$, then $C_{\frac{k}{2} + 1}$ is a cyclic code over $\mathbb{F}_p$ with parameters $\{p^m - 1, 2m, \frac{p^m - 1}{p^d}(p^{m-1} - p^{\frac{m}{2} - 1})\}$ and the weight distribution of $C_{\frac{k}{2} + 1}$ is given in Table 2.

**Proof** Combining Theorem 3.6, Lemma 3.2 and (3.4), we finish the proof. ☐

### 3.2 The weight distribution of $C_{\frac{k}{2} + 1}$ for $v_2(m) \leq v_2(k)$

In this subsection, we always assume that $v_2(m) \leq v_2(k)$, i.e., $s = \frac{m}{d}$ is odd, where $d = \gcd(m, k)$.

**Lemma 3.8** Let the notations be the same as above, the codes $C_1$ and $C_{\frac{k}{2} + 1}$ have the same weight distribution.

Springer
Since the following, we only need to prove that

\[
\begin{align*}
\text{Table 2 & For the case of } v_2(k) + 1 < v_2(m) & \\
\text{Weight} & \quad \text{Frequency} \\
0 & \quad 1 \\
p^{-1} & \quad \left(p^{m-1} + p^{\frac{m}{2}+d-1}\right) \\
p^{-1} & \quad \left(p^{m-1} - p^{\frac{m}{2}}\right) \\
p^{-1} & \quad \left(2p^{m-1} + p^{\frac{m}{2}+d-1} - p^{\frac{m}{2}-1}\right) \\
(p-1) & \quad \left(p^{m-1} + p^{\frac{m}{2}+d-1}\right) \\
(p-1) & \quad \left(p^{m-1} - p^{\frac{m}{2}-1}\right)
\end{align*}
\]

\textbf{Proof} By (3.1), we have that the weight distribution of } \mathcal{C}_1 \text{ and } \mathcal{C}_{\frac{k+1}{2}} \text{ are respectively determined by the value distribution of}

\[
\Delta_1 = \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \left(\zeta_p u \text{Tr}_1^m((a+b)x^2) + \zeta_p u \text{Tr}_1^m((a-b)\pi x^2)\right)
\]

and

\[
\Delta_{\frac{k+1}{2}} = \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \left(\zeta_p u \text{Tr}_1^m((a+b)x^{pk+1}) + \zeta_p u \text{Tr}_1^m((a-b)\pi x^{pk+1})\right).
\]

Since } v_2(k) \geq v_2(m) \text{, by Lemma 2.3, we have } \gcd(p^m - 1, p^k + 1) = 2 \text{, which implies that } \{x p^k + 1 \mid x \in \mathbb{F}_{p^m}\} = \{x^2 \mid x \in \mathbb{F}_{p^m}\}. \text{ Hence}

\[
\Delta_{\frac{k+1}{2}} = \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \left(\zeta_p u \text{Tr}_1^m((a+b)x^{pk+1}) + \zeta_p u \text{Tr}_1^m((a-b)\pi x^{pk+1})\right)
\]

\[
= \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \left(\zeta_p u \text{Tr}_1^m((a+b)x^2) + \zeta_p u \text{Tr}_1^m((a-b)\pi x^2)\right)
\]

\[
= \begin{cases} 
\sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \left(\zeta_p u \text{Tr}_1^m((a+b)x^2) + \zeta_p u \text{Tr}_1^m((a-b)x^2)\right), & \text{if } p^k \equiv 3 \pmod{4}, \\
\sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \left(\zeta_p u \text{Tr}_1^m((a+b)x^2) + \zeta_p u \text{Tr}_1^m((a-b)\pi x^2)\right), & \text{if } p^k \equiv 1 \pmod{4}.
\end{cases}
\]

If } p^k \equiv 1 \pmod{4}, \text{ then } \Delta_1 = \Delta_{\frac{k+1}{2}}. \text{ On the other hand, if } p^k \equiv 3 \pmod{4}, \text{ then } k \text{ is odd. Since } s \text{ is odd, then } m \text{ is odd, which implies that } u_p \text{ is a nonsquare element in } \mathbb{F}_{p^m}. \text{ In the following, we only need to prove that}

\[
\sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p u \text{Tr}_1^m((a-b)x^2) = \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p u \text{Tr}_1^m((a-b)\pi x^2).
\]
On the other hand, we have that
\[
\sum_{u \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p u \text{Tr}_1^m((a-b)x^2)
\]
\[
= \sum_{u \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)(u \frac{1}{x})^2) + \text{Tr}_1^m(u_p(a-b)(u \frac{1}{x})^2) \right)
\]
\[
= \frac{p-1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)x^2) + \text{Tr}_1^m(u_p(a-b)x^2) \right)
\]
\[
= \frac{p-1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)x^2) + \text{Tr}_1^m\left(\frac{p^{m-1} + p^{m-2} + \ldots + p + 1}{x^2}\right) \right)
\]
\[
= \frac{p-1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)x^2) + \text{Tr}_1^m((a-b)\pi x^2) \right). \tag{3.8}
\]

and
\[
\sum_{u \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p u \text{Tr}_1^m((a-b)\pi x^2)
\]
\[
= \sum_{u \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)\pi (u \frac{1}{x})^2) + \text{Tr}_1^m(u_p(a-b)\pi (u \frac{1}{x})^2) \right)
\]
\[
= \frac{p-1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)\pi x^2) + \text{Tr}_1^m(u_p(a-b)\pi x^2) \right)
\]
\[
= \frac{p-1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)\pi x^2) + \text{Tr}_1^m\left(\frac{p^{m-1} + p^{m-2} + \ldots + p + 1}{x^2}\right) \right)
\]
\[
= \frac{p-1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)\pi x^2) + \text{Tr}_1^m((a-b)(\pi \frac{p^{m-1} + p^{m-2} + \ldots + p + 1}{x^2})^2) \right)
\]
\[
= \frac{p-1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left( \text{Tr}_1^m((a-b)\pi x^2) + \text{Tr}_1^m((a-b)x^2) \right). \tag{3.9}
\]

By comparing (3.8) and (3.9), we finish the proof. \(\square\)

By Lemma 3.8, the weight distribution of the code \(C_{\frac{p^k+1}{2}}\) is the same as the code \(C_1\). As we know, the weight distribution of the code \(C_1\) has been studied in [13] (see Theorems 5,6).
The weight distribution of the code $C \leq 1$ for all $i$

Combining Lemma 3.1, Theorems 3.7 and 3.10, we have the following main result in this paper.

**Lemma 3.9** [13] Let the notations be the same as above.

- If $v_2(m) = 0$, then $C_1$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2m, \frac{p^m - 1}{2}, (p^m - 1)]$ and the weight distribution of $C_{\frac{p^k + 1}{2}}$ is given in Table 3.

- If $1 \leq v_2(m) \leq v_2(k)$, then $C_1$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2m, \frac{p^m - 1}{2}(p^{m-1} - p^{\frac{m}{2}} - 1)]$ and the weight distribution of $C_{\frac{p^k + 1}{2}}$ is given in Table 4.

Applying Lemmas 3.8 and 3.9, we have the following theorem.

**Theorem 3.10** Let the notations be the same as above.

- If $v_2(m) = 0$, then $C_{\frac{p^k + 1}{2}}$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2m, \frac{p^m - 1}{2}, p^m - 1]$ and the weight distribution of $C_{\frac{p^k + 1}{2}}$ is given in Table 3.

- If $1 \leq v_2(m) \leq v_2(k)$, then $C_{\frac{p^k + 1}{2}}$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2m, \frac{p^m - 1}{2}(p^{m-1} - p^{\frac{m}{2}} - 1)]$ and the weight distribution of $C_{\frac{p^k + 1}{2}}$ is given in Table 4.

### Table 3

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

### Table 4

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

3.3 The weight distribution of the code $C_i$

Combining Lemma 3.1, Theorems 3.7 and 3.10, we have the following main result in this paper.

**Theorem 3.11** Let the notations be the same as above. Let $t \in \mathbb{Z}_{p^m - 1}$ be a positive integer such that $t \equiv \frac{p^k + 1}{2} p^i \mod \frac{p^m - 1}{2}$ for some $i \in \mathbb{Z}_m$, where $k$ satisfies $\pi \frac{p^k + 1}{2} p^i \neq -\pi \frac{p^k + 1}{2}$ for all $i \in \mathbb{Z}_m$.

- If $v_2(k) + 1 = v_2(m)$, then $C_i$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2m, \frac{p^m - 1}{2}(p^{m-1} - p^{\frac{m}{2}} + d - 1)]$ and the weight distribution of $C_i$ is given by Table 1.

- If $v_2(k) + 1 < v_2(m)$, then $C_i$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2m, \frac{p^m - 1}{2}(p^{m-1} - p^{\frac{m}{2}} - 1)]$ and the weight distribution of $C_i$ is given by Table 2.
• If $v_2(m) = 0$, then $C_t$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2m, \frac{p^m - 1}{2}]$ and the weight distribution of $C_t$ is given by Table 3.

• If $1 \leq v_2(m) \leq v_2(k)$, then $C_t$ is a cyclic code over $\mathbb{F}_p$ with parameters $[p^m - 1, 2m, \frac{p^m - 1}{2}(p^m - 1 - \frac{p^m - 1}{2})]$ and the weight distribution of $C_t$ is given by Table 4.

In the following, we give four examples to verify our main results in Theorem 3.11.

**Example 3.12** Let $p = 3, m = 6, k = 1$. If $t \equiv 2p^\tau \pmod{364}$ for some $\tau \in \mathbb{Z}_6$, then the code $C_t$ is a $[728, 12, 216]$ cyclic code over $\mathbb{F}_3$ with weight enumerator

$$1 + 364X^{216} + 1092X^{252} + 33124X^{432} + 198744X^{468} + 298116X^{504},$$

which agrees with the weight distribution in Table 1.

**Example 3.13** Let $p = 3, m = 4, k = 1$. If $t \equiv 2p^\tau \pmod{40}$ for some $\tau \in \mathbb{Z}_4$, then the code $C_t$ is a $[80, 8, 24]$ cyclic code over $\mathbb{F}_3$ with weight enumerator

$$1 + 120X^{24} + 40X^{36} + 3600X^{48} + 2400X^{60} + 400X^{72},$$

which agrees with the weight distribution in Table 2.

**Example 3.14** Let $p = 5, m = 3, k = 1$. If $t \equiv 3p^\tau \pmod{62}$ for some $\tau \in \mathbb{Z}_3$, then the code $C_t$ is a $[124, 6, 50]$ cyclic code over $\mathbb{F}_5$ with weight enumerator

$$1 + 248X^{50} + 15376X^{100},$$

which agrees with the weight distribution in Table 3.

**Example 3.15** Let $p = 3, m = 6, k = 2$. If $t \equiv 5p^\tau \pmod{364}$ for some $\tau \in \mathbb{Z}_6$, then the code $C_t$ is a $[728, 12, 234]$ cyclic code over $\mathbb{F}_3$ with weight enumerator

$$1 + 728X^{234} + 728X^{252} + 132496X^{468} + 264992X^{486} + 132496X^{504},$$

which agrees with the weight distribution in Table 4.

**Acknowledgments** This work was supported by NSFC (Grant No. 11171370) and self-determined research funds of CCNU from the colleges’ basic research and operation of MOE (Grant No. CCNU14F01004). We sincerely thank the anonymous reviewers for their helpful comments and suggestions.

**References**

1. Delsarte P.: On subfield subcodes of modified Reed–Solomon codes. IEEE Trans. Inf. Theory 21(5), 575–576 (1975).
2. Ding C., Yang J.: Hamming weight in irreducible codes. Discret. Math. 313(4), 434–446 (2013).
3. Ding C., Liu Y., Ma C., Zeng L.: The weight distributions of the duals of cyclic codes with two zeros. IEEE Trans. Inf. Theory 57(12), 8000–8006 (2011).
4. Draper S., Hou X.: Explicit evaluation of certain exponential sums of quadratic functions over $\mathbb{F}_{p^m}$, $p$ odd. http://arxiv.org/pdf/0708.3619v1.
5. Feng T.: On cyclic codes of length $2^r - 1$ with two zeros whose dual codes have three weights. Des. Codes Cryptogr. 62(3), 253–258 (2012).
6. Feng K., Luo J.: Weight distribution of some reducible cyclic codes. Finite Fields Appl. 14(2), 390–409 (2008).
7. Helleseth T., Kholosha A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory 52(5), 2018–2032 (2006).
8. Li C., Li N., Helleseth T., Ding C.: On the weight distributions of several classes of cyclic codes from APN monomials. IEEE Trans. Inf. Theory 60(8), 4710–4721 (2014).
9. Lidl R., Niederreiter H.: “Finite Fields”, Encyclopedia of Mathematics, vol. 20. Cambridge University Press, Cambridge (1983).
10. Liu Y., Yan H., Liu C.: A class of six-weight cyclic codes and their weight distribution. Des. Codes Cryptogr. (2014). doi:10.1007/s10623-014-9984-y.
11. Luo J., Feng K.: Cyclic codes and sequences from generalized Coulter–Matthews function. IEEE Trans. Inf. Theory 54(12), 5345–5353 (2008).
12. Luo J., Feng K.: On the weight distributions of two classes of cyclic codes. IEEE Trans. Inf. Theory 54(12), 5332–5344 (2008).
13. Ma C., Zeng L., Liu Y., Feng D., Ding C.: The weight enumerator of a class of cyclic codes. IEEE Trans. Inf. Theory 57(1), 397–402 (2011).
14. MacWilliams F., Sloane N.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1997).
15. Rao A., Pinnawala N.: A family of two-weight irreducible cyclic codes. IEEE Trans. Inf. Theory 56(6), 2568–2570 (2010).
16. Vega G.: The weight distribution of an extended class of reducible cyclic codes. IEEE Trans. Inf. Theory 58(7), 4862–4869 (2012).
17. Vega G., Wolfmann J.: New classes of 2-weight cyclic codes. Des. Codes Cryptogr. 42(3), 327–334 (2007).
18. Wang B., Tang C., Qi Y., Yang Y., Xu M.: The weight distributions of cyclic codes and elliptic curves. IEEE Trans. Inf. Theory 58(12), 7253–7259 (2012).
19. Xiong M.: The weight distributions of a class of cyclic codes II. Des. Codes Cryptogr. (2012). doi:10.1007/s10623-012-9785-0.
20. Xiong M.: The weight distributions of a class of cyclic codes. Finite Fields Appl. 18(5), 933–945 (2012).
21. Xiong M.: The weight distributions of a class of cyclic codes III. Finite Fields Appl. 21, 84–96 (2013).
22. Zeng X., Hu L., Jiang W., Yue Q., Cao X.: The weight distribution of a class of \( p \)-ary cyclic codes. Finite Fields Appl. 16(1), 56–73 (2010).
23. Zeng X., Shan J., Hu L.: A triple-error-correcting cyclic code from the Gold and Kasami–Welch APN power functions. Finite Fields Appl. 18(1), 70–92 (2012).
24. Zheng D., Wang X., Zeng X., Hu L.: The weight distribution of a family of \( p \)-ary cyclic codes. Des. Codes Cryptogr. (2013). doi:10.1007/s10623-013-9908-2.
25. Zhou Z., Ding C.: A class of three-weight cyclic codes. Finite Fields Appl. 25, 79–93 (2014).
26. Zhou Z., Ding C., Luo J., Zhang A.: A family of five-weight cyclic codes and their weight enumerators. IEEE Trans. Inf. Theory 59(10), 6674–6682 (2013).