The Weight Distributions of Several Classes of Cyclic Codes From APN Monomials
Chunlei Li, Nian Li, Tor Helleseth, Fellow, IEEE, and Cunsheng Ding, Senior Member, IEEE

Abstract—Let \( m \geq 3 \) be an odd integer and \( p \) be an odd prime. In this paper, a number of classes of three-weight cyclic codes \( C(1,e) \) over \( \mathbb{F}_p \), which have parity-check polynomial \( m_1(x) \), are presented by examining general conditions on the parameters \( p, m, \) and \( e \), where \( m_1(x) \) is the minimal polynomial of \( \pi^{-1} \) over \( \mathbb{F}_p \) for a primitive element \( \pi \) of \( \mathbb{F}_p^m \). Furthermore, for \( p = 3 \) (mod 4) and a positive integer \( e \) satisfying \( (p^k + 1) \cdot e = 2 \) (mod \( p^m - 1 \)) for some positive integer \( k \) with \( \gcd(m, k) = 1 \), the value distributions of the exponential sums \( T(a, b) = \sum_{x \in \mathbb{F}_p} \omega^{Tr(ax + bx^e)} \) and \( S(a, b, c) = \sum_{x \in \mathbb{F}_p} \omega^{Tr(ax + bx^e + cx^e)} \), where \( s = (p^m - 1)/2 \), are determined. As an application, the value distribution of \( S(a, b, c) \) is utilized to derive the weight distribution of the cyclic codes \( C(1,e,\pi) \) with parity-check polynomial \( m_1(x) \). In the case of \( p = 3 \) and even \( e \) satisfying the above condition, the dual of the cyclic code \( C(1,e,\pi) \) has optimal minimum distance.

Index Terms—Almost perfect nonlinear function, cyclic code, weight distribution, exponential sum, quadratic form.

I. INTRODUCTION

Let \( p \) be a prime, \( m \) be a positive integer and \( q = p^m \). Let \( \mathbb{F}_q \) denote the finite field with \( q \) elements and \( \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \). A linear \([n, k, \rho]\) code \( C \) over \( \mathbb{F}_p \) is a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \) with minimum (Hamming) nonzero weight \( \rho \). Let \( A_l \) denote the number of codewords in \( C \) with Hamming weight \( i \). The weight distribution \( (A_0, A_1, \ldots, A_n) \) is an important research object in coding theory because it contains crucial information as to estimate the error correcting capability and allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms [16].

A linear code \( C \) over \( \mathbb{F}_p \) is called cyclic if any cyclic shift of a codeword is another codeword of \( C \). It is well known that any cyclic code of length \( n \) over \( \mathbb{F}_p \) corresponds to an ideal of the polynomial residue class ring \( \mathbb{F}_p[x]/(x^n - 1) \) and can be expressed as \( C = \langle g(x) \rangle \), where \( g(x) \) is monic and has the least degree. This polynomial is called the generator polynomial and \( h(x) = (x^n - 1)/g(x) \) is referred to as the parity-check polynomial of \( C \). Cyclic codes with a few weights are of particular interest in secret sharing schemes and designing frequency hopping sequences. They have been extensively studied in the literature (see [4], [8], [11], [13], [14], [20], [22], [23]). In this paper, cyclic codes with \( r \) nonzero weights are called \( r \)-weight cyclic codes.

Let \( \Gamma_j \) be the \( p \)-cyclotomic coset modulo \( q - 1 \) containing \( j \), i.e., \( \Gamma_j = \{ j \cdot p^t \mod (q - 1) | i = 0, 1, \ldots, l_j - 1 \} \), where \( j \) is any integer with \( 0 \leq j < q - 2 \) and \( l_j \) is the smallest positive integer such that \( j \equiv j \cdot p^l \mod (q - 1) \). Let \( \mathbb{Z}_{q-1} \) be the set of integers modulo \( q - 1 \) and \( m_1(x) \) be the minimal polynomial of \( \pi^{-1} \) over \( \mathbb{F}_p \) for a primitive element \( \pi \) in \( \mathbb{F}_q \). For integers \( i_1, \ldots, i_t \in \mathbb{Z}_{q-1}, t \geq 1 \) with pairwise disjoint cyclotomic cosets \( \Gamma_{i_1}, \ldots, \Gamma_{i_t} \), we denote by \( C_{\{i_1, \ldots, i_t\}} \) the cyclic code with parity-check polynomial \( h(x) = m_1(x) \cdot m_1(x) \) and write \( C_{\{i_1, \ldots, i_t\}} \) for its dual code. By the well-known Delsarte’s Theorem [7], one can express the cyclic code \( C_{\{i_1, \ldots, i_t\}} \) as

\[
C_{\{i_1, \ldots, i_t\}} = \left\{ \left( \sum_{s=1}^{l_j} \text{Tr}(a_s x^{i_s}) \right)^{q-2} a_1, a_2, \ldots, a_t \in \mathbb{F}_q \right\},
\]

where \( \text{Tr}() \) is the trace mapping from \( \mathbb{F}_q \) to \( \mathbb{F}_p \). Hence the Hamming weight of the codeword \( e = (c_0, c_1, \ldots, c_{q-2}) \) in \( C_{\{i_1, \ldots, i_t\}} \) satisfies

\[
w_H(e) = ||\{j | 0 \leq j < q - 2, c_j \neq 0\}|| - (q - 1) - ||\{j | 0 \leq j < q - 2, c_j = 0\}||
\]

\[
= (q - 1) - \frac{1}{p} \sum_{x \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p} y \cdot \text{Tr}(y \sum_{i=1}^{l_j} a_i x^{i_s})
\]

\[
= \frac{(q - 1)(p - 1)}{p} - \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^*} \text{Tr}(y \sum_{i=1}^{l_j} a_i x^{i_s})
\]

\[
= p^{m-1}(p - 1) - \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} S(ya_1, ya_2, \ldots, ya_t),
\]

where \( S(a_1, a_2, \ldots, a_t) = \sum_{x \in \mathbb{F}_p} \omega^{\text{Tr}(a_1 x^{a_1} + a_2 x^{a_2} + \ldots + a_t x^{a_t})} \) and \( \omega \) is a primitive \( p \)-th root of unity. In this way, the weight distribution of the cyclic code \( C_{\{i_1, \ldots, i_t\}} \) can be derived from

the value distribution of the multi-set

\[ \{S(a_1, a_2, \ldots, a_t) \mid a_1, a_2, \ldots, a_t \in \mathbb{F}_q \} \]

Perfect nonlinear (PN) and almost perfect nonlinear (APN) functions are important research objects in cryptography and coding theory [1], [3], [6]. For \( p = 2 \), it is shown in [2] that the monomial \( x^r \) is APN if and only if the cyclic code \( C_{1,e} \) has optimal minimum distance 5. In [23], the Gold and Kasami-Welch APN monomials were utilized to construct a class of cyclic codes \( C_{1,3,13} \) having the same weight distribution as the triple-error-correcting BCH code \( C_{1,3,5} \). For odd prime \( p \), when \( x^e \) is a PN monomial over \( \mathbb{F}_q \), the cyclic codes \( C_{1,e} \) and \( C_{0,1,e} \) and their duals were intensively studied in [4], [12], [19], and [21], where the weight distributions of the cyclic codes \( C_{1,e} \) and \( C_{0,1,e} \) were determined and their dual codes were proved to have optimal minimum distances 4 and 5 respectively \(^1\). Very recently, for \( p = 3 \) and some monomials \( x^r \) including APN ones, the ternary cyclic codes \( C_{1,e} \) and \( C_{1,1,e} \), where \( s = (3^m - 1)/2 \), were shown to have optimal minimum distances 4 and 5 in [10] and [17]. The weight distributions of the proposed cyclic codes and their duals are mostly unknown.

In this paper, for odd integer \( m \geq 3 \), we will derive general conditions on the parameters \( p, m, \) and \( e \) under which \( C_{1,e} \) is a three-weight code. It turns out that all the three-weight cyclic codes recently found in [5], [9], and [26] are special cases of the general construction of this paper and many new three-weight cyclic codes, as demonstrated in Corollaries 1-3, are generated. Furthermore, for \( p \equiv 3 \) (mod 4) and a positive integer \( e \) satisfying \( (p^k + 1) \cdot e \equiv 2 \) (mod \( p^m - 1 \)) for some positive integer \( k \) with \( \gcd(m, k) = 1 \), we will determine the value distributions of the two exponential sums

\[ T(a, b) = \sum_{x \in \mathbb{F}_q} \omega^{Tr(ax+bx^e)} \]

and

\[ S(a, b, c) = \sum_{x \in \mathbb{F}_q} \omega^{Tr(ax+bx^e+cx^r)} \]

where \( s = (q - 1)/2 \). The value distribution of \( S(a, b, c) \) is subsequently used to investigate the weight distribution of the cyclic codes \( C_{1,e} \). For \( p = 3 \) and even \( e \) satisfying \( (p^k + 1) \cdot e \equiv 2 \) (mod \( p^m - 1 \)), the cyclic codes \( C_{1,e} \) have optimal minimum distance 5 [17].

The remainder of this paper is organized as follows. Section II presents a unified approach to generating three-weight cyclic codes, of which the weight distributions are well settled. Section III deals with the value distributions of the exponential sums \( T(a, b) \) and \( S(a, b, c) \). Section IV determines the weight distribution of the cyclic code \( C_{1,e} \). Section V concludes this paper.

---

\(^1\)The cyclic code \( C_{0,1,e} \) is slightly different from the code \( \overline{C}_{11} \) for \( \Pi(x) = x^r \) defined in [4], and the weight distribution of \( C_{0,1,e} \) can be similarly settled as in [19].

**II. THREE-WEIGHT CYCLIC CODES AND THEIR WEIGHT DISTRIBUTIONS**

In this section our task is to derive general conditions on \( (p, m, e) \) under which \( C_{1,e} \) is a three-weight code. To this end, we need to introduce earlier results on three-weight cyclic codes \( C_{1,e} \).

In [4] and [21], Carlet et al. employed PN monomials to construct three-weight cyclic codes documented in the following lemma.

**Lemma 1 ([4], [21]):** Let \( p \) be an odd prime and \( m \geq 3 \) be odd. Then the cyclic code \( C_{1,e} \) has length \( q - 1 \), dimension \( 2m \), and the weight distribution in Table I if

(i) \( e = p^k + 1 \) or

(ii) \( e = (p^k + 1)/2 \), where \( p = 3 \) and \( \gcd(2m, k) = 1 \).

The second construction in Lemma II was extended to any odd prime \( p \) and positive integer \( k \), \( 1 \leq k \leq m - 1 \), in [20] and [25].

**Lemma 2 ([20], [25]):** Let \( p \) be an odd prime. Let \( m \) and \( k \) be positive integers such that \( \frac{m}{\gcd(m, k)} \) is odd and no less than 3. Define \( e = (p^k + 1)/2 \). Then the cyclic code \( C_{1,e} \) has length \( q - 1 \), dimension \( 2m \), and the weight distribution in Table II if \( k/s \) is odd and in Table III if \( k/s \) is even, where \( s = \gcd(m, k) \).

The following lemma will be needed in the sequel.

**Lemma 3:** Let \( m \geq 3 \) be odd and \( p \) be an odd prime with \( p - 1 = 2^e h \), where \( h \) is an odd integer. If two integers \( d, e \in \mathbb{Z}_{p^m - 1} \setminus \Gamma_1 \) satisfy \( 2de \equiv 2 \) (mod \( p^m - 1 \)) and \( d + e \equiv 2 \) (mod \( 2^e \)), then the cyclic codes \( C_{1,d} \) and \( C_{1,e} \) have the same weight distribution.

**Proof:** According to (1), the weight distributions of \( C_{1,d} \) and \( C_{1,e} \) are respectively determined by the value distributions of

\[ \Delta_0(a, b) = \sum_{y \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_q} \omega^{Tr(ax+ybx^e)} \]
Thus, for some nonnegative integer $k$, then

$$\omega \equiv \begin{cases} 
\omega_1 & \text{if } e \equiv 0 \mod 2, \\
\omega_2 & \text{if } e \equiv 1 \mod 2
\end{cases}$$

\end{equation}

is a primitive element in $F_{p^k}$. Since $gcd(2d, p^m - 1) = 2$, it follows that $gcd(p^k + 1, p^m - 1) = 2$, $e \in \Gamma_1$ and $|\Gamma_e| = m$. Thus, all the conditions in Lemma II are satisfied. Then it follows from Lemmas II and II that $C_{1,e}$ has the weight distribution of Table I.

(iii) Let $p$ be any odd prime and $m$ be odd. Assume that $e$ is an integer satisfying $(p^k + 1)e \equiv 2 \mod (p^m - 1)$ for some positive integer $k$. Then $gcd((p^k + 1)e, p^m - 1) = 2$, and it follows that $gcd(p^k + 1, p^m - 1) = 2$, $e \in \Gamma_1$ and $|\Gamma_e| = m$.

By assumption, $(p^k + 1)e \equiv 2 \mod (p^m - 1)$, which implies that $2e \equiv 2 \mod (p - 1)$, we deduce that $e \equiv 1 \mod (p - 1)$ or $e \equiv 1 + (p - 1)/2 \mod (p - 1)$.

In the case of $e \equiv 1 \mod (p - 1)$, let $k_0$ be an integer such that $k_0 = k$ if $k$ is even and $k_0 = m - k$ if $k$ is odd. It is clear that $k_0$ is always even since $m$ is odd. Set $d = (p^k + 1)/2$. We have $d \equiv 1 + (p^k - 1)/2 \equiv 1 + k_0(p - 1)/2 \equiv 1 \mod (p - 1)$. Then $d + e \equiv 2 \mod (p - 1)$. In addition, by assumption $(p^k + 1)e \equiv 2 \mod (p^m - 1)$, we have $2de \equiv 2 \mod (p^m - 1)$ if $e$ is even and $2de \equiv 2p^{m-k} \mod (p^m - 1)$ if $k$ is odd. Since $m$ is odd, the integer $s = gcd(m, k_0)$ is odd and $k_0/s$ is even. Note that the cyclic codes $C_{1,e}$ are the same when $e$ runs through the cyclotomic coset $\Gamma_e$. The conclusion thus follows from Lemmas II and II.

Similarly, in the case of $e \equiv 1 + (p - 1)/2 \mod (p - 1)$, we take $k_1 = k$ if $k$ is odd and $k_1 = m - k$ if $k$ is even. Then $k_1$ is odd and $(p^k + 1)/2 \equiv 1 + k_1(p - 1)/2 \equiv 1 + (p - 1)/2 \mod (p - 1)$. Let $d = (p^k + 1)/2$. Then $d + e \equiv 2 \mod (p - 1)$.

In addition, $2de \equiv 2 \mod (p^m - 1)$ if $k$ is odd and $2de \equiv 2p^{m-k} \mod (p^m - 1)$ if $k$ is even. Since the cyclic codes $C_{1,e}$ are the same when $e$ runs through the cyclotomic coset $\Gamma_e$, it follows from Lemmas II and II that $C_{1,e}$ has the weight distribution of Table II since $k_1/s$ is odd. The proof is completed.

Very recently, a total of twelve classes of three-weight $[p^m - 1, 2m]$ cyclic codes over $F_p$ are described in [5], [26], and [9]. It can be verified by hand that all the three-weight cyclic codes found in [5], [26], and [9] are special cases of the codes in Theorem I. Furthermore, a closer look at Theorem I reveals that many new three-weight cyclic codes can be generated in this way.

The following are three corollaries of Theorem I, which give new three-weight codes that are not covered in [5], [9], and [26]. They demonstrate that Theorem I can be applied to generate many new three-weight cyclic codes and settle their weight distributions.

**Corollary 1:** Let $p = 3$ and let $m \equiv 2t - 1 \mod (2^t)$ for any integer $t \geq 2$. For any $h$ with $2 \leq h \leq t$, if $e = (3^{(m+1)/2^h} - 1) \prod_{i=1}^{t-1} (3^{(m+1)/2^i} + 1)$.
then $C_{1,e}$ is a $[3^m - 1, 2m]$ ternary cyclic code with the weight distribution in Table II, where $s = 1$; if $e = (3^{(m+1)/2} - 1) \prod_{i=1}^{t-1} (3^{(m+1)/2} + 1) + (3^m - 1)/2$, then $C_{1,e}$ is a $[3^m - 1, 2m]$ ternary cyclic code with the weight distribution in Table III, where $s = 1$.

Proof: Let $d = (3^{(m+1)/2} + 1)$. Then $de \equiv 2 \pmod {3^m - 1}$. We have clearly that $\text{gcd}(m+1)/2^k, m) = 1$. In addition, $(3^{(m+1)/2} - 1) \prod_{i=1}^{t-1} (3^{(m+1)/2} + 1) \equiv 2 \pmod {p-1}$. The desired conclusion then follows from Theorem 1 (ii). □

Corollaries 2 and 3 below document new three-weight codes that are not covered in [5], [26], and [9] for $p > 3$.

Corollary 2: Let $m \geq 3$ be odd and $p \equiv 3 \pmod{4}$. Let $e = (p^m + 1)/4 + (p^m - 1)/2$ if $p \equiv 3 \pmod{8}$ and $e = (p^m + 1)/4$ if $p \equiv 7 \pmod{8}$. Then $C_{1,e}$ is a $[p^m - 1, 2m]$ cyclic code with the weight distribution in Table I.

Proof: Let $d = 4$. Then $de \equiv 2 \pmod {p^m - 1}$. Since $(p^m + 1)/4 \equiv (p + 1)/4 \pmod {2}$ and $(p^m - 1)/2$ is odd, the conclusion follows from Theorem 1 (i). □

Corollary 3: Let $m \geq 3$ be odd and $p$ be any odd prime. Let the sets $S_0, i = 0, 1$, be defined by $S_i = \left\{ \frac{(p+1)(p^m - 1) - 4(p^{\frac{m+1}{2}} - 1)}{2(p-1)} \right\}$. (i) If $e \in S_0$, then $C_{1,e}$ is a $[p^m - 1, 2m]$ cyclic code with the weight distribution in Table II, where $s = 1$. (ii) If $e \in S_1$, then $C_{1,e}$ is a $[p^m - 1, 2m]$ cyclic code with the weight distribution in Table III, where $s = 1$.

Proof: Since $(p^{\frac{m+1}{2}} + 1)(p + 1) \equiv 4 \pmod {p - 1}$, it is easily verified that

\[
\left( p^{\frac{m+1}{2}} + 1 \right) \cdot \left( p + 1 \right) \left( p^m - 1 \right) - 4 \left( p^{\frac{m+1}{2}} - 1 \right) \equiv 2 \pmod {p^m - 1}.
\]

Similarly, it follows from $(p^{\frac{m+1}{2}} + 1)(p - 3) \equiv -4 \pmod {p - 1}$ that

\[
\left( p^{\frac{m+1}{2}} + 1 \right) \cdot \left( p - 3 \right) \left( p^m - 1 \right) + 4 \left( p^{\frac{m+1}{2}} - 1 \right) \equiv 2 \pmod {p^m - 1}.
\]

Thus, for any integer $e \in S_0 \cup S_1$, there exists an integer $d \in \{ p^{\frac{m+1}{2}} + 1, p^{\frac{m+1}{2}} + 1 \}$ such that $de \equiv 2 \pmod {p^m - 1}$.

In addition, we observe that

\[
\left( p + 1 \right) \left( p^m - 1 \right) - 4 \left( p^{\frac{m+1}{2}} - 1 \right) \equiv 1 + \frac{(p - 1)}{2} \pmod {p - 1}
\]

and

\[
\left( p - 3 \right) \left( p^m - 1 \right) + 4 \left( p^{\frac{m+1}{2}} - 1 \right) \equiv 1 + \frac{(p - 1)}{2} \pmod {p - 1}.
\]

Then it follows that $e \equiv 1 + (p - 1)/2 \pmod {p - 1}$ for $e \in S_0$ and $e \equiv 1 \pmod {p - 1}$ for $e \in S_1$. The desired conclusion then follows from Theorem 1 (ii). □

III. Value Distributions of the Two Exponential Sums

Throughout what follows, we will always assume that $m \geq 3$ is an odd integer, $p \equiv 3 \pmod{4}$ and $e$ is an integer $e$ satisfying $(p^k + 1)e \equiv 2 \pmod {p^m - 1}$ for some positive integer $k$ with $\text{gcd}(m, k) = 1$. For convenience of presentation, such an integer $e$ is hereafter said to satisfy the Congruence Condition.

In this section, for an integer $e$ satisfying the Congruence Condition, we will study the following multi-sets

\[
\{ T(a, b) = \sum_{x \in \mathbb{F}_q^*} \omega^{Tr(ax + bx^e)} | a, b \in \mathbb{F}_q \} \]  (2)

and

\[
\{ S(a, b, c) = \sum_{x \in \mathbb{F}_q^*} \omega^{Tr(ax + bx^e + cx)} | a, b, c \in \mathbb{F}_q \} \]  (3)

where $s = (q - 1)/2$, $\mathbb{F}_q$ is composed of $p$ elements in $\mathbb{F}_q$ such that $\{ Tr(c) | c \in \mathbb{F}_p \} = \mathbb{F}_p$. (It is clear that we can take $\mathbb{F}_p = \mathbb{F}_q$, if $Tr(1) \neq 0$). The value distribution of $S(a, b, c)$ will be utilized to investigate the weight distribution of the cyclic codes $C_{1,e,s}$ in Section IV.

Define

\[
T_0(a, b) = \sum_{x \in \mathbb{F}_q^*} \omega^{Tr(ax^{k+1} + bx^e)}.
\]

(4)

For odd $m$ and $p \equiv 3 \pmod{4}$, $-1$ is a non-square in $\mathbb{F}_q$. When $x$ runs through $\mathbb{F}_q^*$, $x^{k+1}$ runs twice through the squares in $\mathbb{F}_q^*$ and $-x^{k+1}$ runs twice through all the non-squares in $\mathbb{F}_q^*$. Therefore, for integers $e$ satisfying the Congruence Condition, the exponential sums $T(a, b)$ and $S(a, b, c)$ can be rewritten as

\[
T(a, b) = \frac{1}{2} (T_0(a, b) + T_0(-a, -1^{e+b})),
\]  (5)

and

\[
S(a, b, c) = 1 + \frac{1}{2} (\omega^t + \omega^{-t})
\]

\[
+ \frac{1}{2} (\omega^t T_0(a, b) + \omega^{-t} T_0(-a, -1^{c+b})),
\]  (6)

where $t = Tr(c)$.

The value distribution of the exponential sum $T_0(a, b)$ for odd $m \geq 3$ is given in Table IV [13]. In order to determine the value distribution of $T(a, b)$ and $S(a, b, c)$, we shall study the distribution of $(T_0(a, b), T_0(-a, -1^{c+b}))$ when $(a, b)$ runs through $\mathbb{F}_q^2$. When $e$ is an odd integer, as $T_0(-a, -b)$ is the conjugate of $T_0(a, b)$ for any $(a, b) \in \mathbb{F}_q^2$, the distribution of $(T_0(a, b), T_0(-a, -b))$ can be readily settled from Table IV. When $e$ is an even integer, the calculation of the distribution of $(T_0(a, b), T_0(-a, -b))$ is not trivial and we will focus on it in the sequel.

The following two lemmas characterize all possible $(T_0(a, b), T_0(-a, -b))$ for any $a, b \in \mathbb{F}_q$.

<table>
<thead>
<tr>
<th>Values</th>
<th>Multiplicity (each)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\pm \sqrt[p]{p^{m+1}}$</td>
<td>$p^{3(m-1)}(p^{m-1} - 1)^2(2p^2 - 1)$</td>
</tr>
<tr>
<td>$\pm \sqrt[p]{p^{m+1}}$</td>
<td>$(p^{m-1} - 1)^2(2p^2 - 1)$</td>
</tr>
<tr>
<td>$\pm \sqrt[p]{p^{m+1}}$</td>
<td>$(p^{m-1} - 1)/(2p^2 - 1)$</td>
</tr>
</tbody>
</table>

TABLE IV

THE VALUE DISTRIBUTION OF $T_0(a, b)$ FOR ODD $m \geq 3$
lemma 4 ([13]): Let \( Q(x) \) be a quadratic form in \( m \) variables over \( \mathbb{F}_p \) of rank \( r \), \( \left( \frac{a}{p} \right) \) be the conventional Legendre symbol. Then
\[
\sum_{x \in \mathbb{F}_p} \omega^Q(x) = \begin{cases} \left( \frac{a}{p} \right) p^{m-r}/2 & \text{if } p \equiv 1 \pmod{4} \\ (-1)^{r/2} \left( \frac{a}{p} \right) p^{m-r}/2 & \text{if } p \equiv 3 \pmod{4}, \end{cases}
\]
where \( \Delta \) is the determinant of \( Q(x) \). Furthermore, for any \( y \in \mathbb{F}_p \),
\[
\sum_{x \in \mathbb{F}_p} \omega^yQ(x) = \left( \frac{y}{p} \right) \sum_{x \in \mathbb{F}_p} \omega^Q(x). \tag{7}
\]

lemma 5 ([13], [25]): Let \( m \) and \( k \) be positive integers such that \( \gcd(m, k) = 1 \). Let
\[
Q_{a, b}(x) = \text{Tr}(ax^{p+1} + bx^2)
\]
be a quadratic form in \( m \) variables over \( \mathbb{F}_p \). Then, (i) for \((a, b) \in \mathbb{F}_p^m \setminus \{(0, 0)\}\), the quadratic form \( Q_{a, b}(x) \) has rank no less than \( m - 2 \); (ii) if \( m \) is odd, then for any \( a \in \mathbb{F}_p^m \) and \( b \in \mathbb{F}_p^m \), at least one of \( Q_{a, b}(x) \) and \( -Q_{a, b}(x) \) has rank \( m \).

For \( i = 0, 1, 2 \), let
\[
v_i = \begin{cases} \frac{m+1}{p} & \text{if } i \text{ is odd}, \\ \frac{m+i-1}{p} & \text{if } i \text{ is even}, \end{cases}
\]
where \( p^* = (-1)^{\frac{p-1}{2}} p \). By Lemmas III and III, for any \((a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}\),
\[
(T_0(a, b), T_0(-a, b)) \in \{ (e_1v_1, e_2v_2) \mid 0 \leq i_1, i_2 \leq 2, e_1, e_2 = \pm 1 \}. \tag{9}
\]

Before further studying the value distribution of \((T_0(a, b), T_0(-a, b))\), we define
\[
N_{+,i} = \left\{ (a, b) \in \mathbb{F}_q^2 \mid T_0(a, b) = e_1v_i \right\},
\]
\[
N_{-,i} = \left\{ (a, b) \in \mathbb{F}_q^2 \mid T_0(-a, b) = e_1v_i \right\},
\]
where \( e \in \{1, -1\} \). Some properties of \( N_{+,i} \) and \( N_{-,i} \) are summarized in the following lemma.

Lemma 1: Let \( \lambda \) be a non-square of \( \mathbb{F}_p^* \). For \( e \in \{1, -1\} \) and \( i \in \{0, 1, 2\} \), we have
(i) \((a, b) \in N_{+,i} \) if and only if \((-a, b) \in N_{-,i} \),
(ii) \( \lambda N_{+,0} = N_{+,0} \), \( \lambda N_{-,0} = N_{-,0} \),
(iii) \( \lambda N_{+,1} = N_{+,1} \), \( \lambda N_{-,1} = N_{-,1} \), and
(iv) \( \lambda N_{+,2} = N_{+,2} \), \( \lambda N_{-,2} = N_{-,2} \).

Proof: Property (i) directly follows from the definitions of \( N_{+,i} \) and \( N_{-,i} \) in (9). Properties (ii), (iii) and (iv) are proved together below.

By Lemma III, for any non-square \( \lambda \) of \( \mathbb{F}_p^* \),
\[
T_0(\lambda a, \lambda b) = \sum_{x \in \mathbb{F}_q} \omega^x \text{Tr}(ax^{p+1} + bx^2) = \left( \frac{x^r}{p} \right) T_0(a, b), \tag{10}
\]
where \( r \) is the rank of the quadratic form \( Q_{a, b}(x) = \text{Tr}(ax^{p+1} + bx^2) \). Following from the definitions of \( v_i \) and \( N_{+,i} \), we know that if \((a, b) \in N_{+,i} \), then the corresponding quadratic form \( Q_{a, b}(x) \) has rank \( m - i \). This fact together with (10) implies that \( T_0(\lambda a, \lambda b) = T_0(a, b) \) if \((a, b) \in N_{+,i} \)
and \( T_0(\lambda a, \lambda b) = -T_0(a, b) \) if \((a, b) \in N_{-,i} \) or \((a, b) \in N_{+,2} \).
Therefore, we deduce that
\[
\lambda N_{+,0} = N_{+,0}, \quad \lambda N_{+,1} = N_{+,1}, \quad \lambda N_{+,2} = N_{+,2}.
\]
Then the properties for \( N_{-,i} \) in (ii), (iii) and (iv) directly follow from (i).

The following results are necessary for calculating the distribution of \((T_0(a, b), T_0(-a, b))\).

Proposition 1: Let \( N_4 \) denote the number of tuples \((x, y, z, w) \in \mathbb{F}_4^4 \) satisfying
\[
\begin{cases}
x^2 + y^2 + z^2 + w^2 = 0 \\
x^{p+1} + y^{p+1} + z^{p+1} - w^{p+1} = 0.
\end{cases}
\]
Then for odd \( m \geq 3 \) and positive integer \( k \) with \( \gcd(m, k) = 1 \),
\[
N_4 = 4q^2 - 4q - q + p.
\]

Proof: See the Appendix.

Proposition 2: For odd \( m \geq 3 \) and positive integer \( k \) with \( \gcd(m, k) = 1 \),
(i) \( \sum_{a,b \in \mathbb{F}_q} T_0(a, b) \cdot T_0(-a, b) = q^2 \);
(ii) \( \sum_{a,b \in \mathbb{F}_q} T_0(a, b) \cdot T_0(-a, b) = 2q^2 - 2q + p \).

Proof: (i) By the definition of \( T_0(a, b) \) in (4), one has
\[
\sum_{a,b \in \mathbb{F}_q} T_0(a, b) \cdot T_0(-a, b) = \sum_{x,y \in \mathbb{F}_q} \sum_{a \in \mathbb{F}_q} \omega^x \text{Tr}(ax^{p+1} - y^{p+1} + b(x^2 + y^2))
\]
\[
= \sum_{x,y \in \mathbb{F}_q} \sum_{a \in \mathbb{F}_q} \omega^x \text{Tr}(ax^{p+1} - y^{p+1} + b(x^2 + y^2))
\]
\[
= q^2 N_2,
\]
where \( N_2 \) is the number of the solutions of the following system of equations:
\[
\begin{cases}
x^2 + y^2 = 0 \\
x^{p+1} = -y^{p+1}.
\end{cases}
\]
Since \( x^{p+1} = y^{p+1} \) and \( \gcd(p^m - 1, p^k + 1) = 2, \) one has \( x^2 = y^2 \). This together with \( x^2 + y^2 = 0 \) implies \( x = y = 0 \). Thus, we deduce \( N_2 = 1 \).

(ii) In a similar manner, we deduce that
\[
\sum_{a,b \in \mathbb{F}_q} T_0^2(a, b) \cdot T_0(-a, b) = \sum_{x,y,z,w \in \mathbb{F}_q} \sum_{a \in \mathbb{F}_q} \omega^x \text{Tr}(ax^{p+1} + y^{p+1} + z^{p+1} - w^{p+1})
\]
\[
= q^2 N_4,
\]
where \( N_4 \) is the number of the solutions of the following system of equations:
\[
\begin{cases}
x^2 + y^2 + z^2 + w^2 = 0 \\
x^{p+1} + y^{p+1} + z^{p+1} - w^{p+1} = 0.
\end{cases}
\]
The conclusion immediately follows from Proposition 1. □

With the preparations of Table IV, Lemmas III, 1 and Proposition 2, we are now ready to determine the distribution of $(T_0(a, b), T_0(-a, b))$.

Theorem 2: Let $\nu_i, \ i = 0, 1, 2$, be defined by (8). For odd $m \geq 3$ and positive integer $k$ with gcd$(m, k) = 1$, the distribution of the multi-set

$$\{ (T_0(a, b), T_0(-a, b)) \mid a, b \in \mathbb{F}_q \}$$

is shown in Table V.

Proof: By the definitions of $N_{+,i}^+$ and $N_{-,i}^-$ in (9), for $e_1, e_2 \in \{-1, 1\}$ and $i_1, i_2 \in \{0, 1, 2\}$,

$$N_{+,i_1}^+ \cap N_{-,i_2}^- = \{ (a, b) \in \mathbb{F}_q^2 \mid T_0(a, b), T_0(-a, b) \} = (e_1 \nu_{i_1}, e_2 \nu_{i_2}).$$

Then one needs to calculate the cardinality of $N_{+,i_1}^+ \cap N_{-,i_2}^-$. It follows from Lemma III (ii) that for any $i_1, i_2 \in \{0, 1, 2\}$ with $i_1 \cdot i_2 \neq 0$, $N_{+,i_1}^+ \cap N_{-,i_2}^- = \emptyset$. Thus it suffices to consider the cases where $i_1 \cdot i_2 = 0$, namely,

$$(i_1, i_2) \in \{(0, 0), (0, 1), (0, 2), (1, 0), (2, 0)\}.$$

Furthermore, by Lemma 1 (i), for any $e_1, e_2 \in \{-1, 1\}$ and $i_1, i_2 \in \{0, 1, 2\}$, $(a, b) \in N_{+,i_1}^+ \cap N_{-,i_2}^-$ if and only if $(-a, b) \in N_{-,i_1}^- \cap N_{+,i_2}^+$. Thus,$$
|N_{+,i_1}^+ \cap N_{-,i_2}^-| = |N_{-,i_1}^- \cap N_{+,i_2}^+|.$$ (11)

Hence we in the sequel only need to calculate $|N_{+,i_1}^+ \cap N_{-,i_2}^-|$ for $i_1 = 0$ and $i_2 \in \{0, 1, 2\}$. The cardinality of $N_{+,i_1}^+ \cap N_{-,i_2}^-$ for $i_1 \in \{0, 1, 2\}$ and $i_2 = 0$ can be directly obtained.

Let $\lambda$ be a non-square of $\mathbb{F}_p^*$. Due to Lemma 1 (ii), we get

$$\lambda(N_{+,i_1}^+ \cap N_{-,i_2}^-) = N_{+,i_1}^+ \cap N_{-,i_2}^-,$$

which implies

$$|N_{+,i_1}^+ \cap N_{-,i_2}^-| = |N_{+,i_1}^+ \cap N_{-,i_2}^-|.$$ (12)

Similarly, Lemma 1 (iv) gives

$$|N_{+,i_1}^+ \cap N_{-,i_2}^-| = |N_{+,i_1}^+ \cap N_{-,i_2}^-|.$$ (13)

By Lemma 1 (iii), we can deduce that

$$|N_{+,i_1}^+ \cap N_{-,i_2}^-| = |N_{+,i_1}^+ \cap N_{-,i_2}^-|,$$

and let

$$s_i = |N_{+,i_1}^+ \cap N_{-,i}^|, \bar{s}_i = |N_{+,i_1}^+ \cap N_{-,i}^|.$$ (15)

From (11)-(16), the reader will observe that the quantities $s_0, \bar{s}_0, s_1, \bar{s}_1, s_2, \bar{s}_2$ respectively correspond to the first item to the sixth item of the multiplicities in Table V. Thus our next task is to determine these quantities.

By Lemma 1 (i), the cardinalities of $N_{+,i}^+$ and $N_{-,i}^-$ are the same and they are listed in Table IV. We denote $n_{+,i} = |N_{+,i}^+| = |N_{-,i}^-|$. By Lemma III (ii), for any $(a, b) \in \mathbb{F}_q \setminus \{(0, 0)\}$, only when the quadratic form $Q_{a,b}(x) = ax^{2^i} + bx^2$ has rank $m$, the quadratic form $Q_{a,b}(x)$ could have rank $m - 2, m - 1$. This is equivalent to saying that

$$N_{-,i}^- \subseteq N_{+,i}^+ \cup N_{-,i_0}^-$$

for $e \in \{-1, 1\}$ and $i = 1, 2$. Thus we have

$$|N_{+,i}^+ \cap N_{-,i}^-| + |N_{-,i_0}^- \cap N_{+,i}^-| = |N_{-,i}^-| = n_{+,i}.$$ (17)

This fact combined with (12), (13) and (14) yields the following equations

$$s_0 + \bar{s}_0 + s_1 + \bar{s}_1 + s_2 + \bar{s}_2 = n_{1,0}$$

$$s_1 + s_2 = n_{1,1}$$

$$\bar{s}_1 + \bar{s}_2 = n_{1,1}$$

$$s_2 + \bar{s}_2 = n_{1,2}.$$ (18)

Furthermore, by the correspondences between the first six items of multiplicities in Table V and the quantities $s_0, \bar{s}_0, s_1, \bar{s}_1, s_2, \bar{s}_2$, it is easy to verify that

$$\sum_{a, b \in \mathbb{F}_q} T_0(a, b)T_0(-a, b) = p^{2m} + 2(s_0 - \bar{s}_0)v_0^2 + 4(s_2 - \bar{s}_2)v_0v_2$$

and

$$\sum_{a, b \in \mathbb{F}_q} T_0^2(a, b)T_0(-a, b) = q^4 + 2(s_0 - \bar{s}_0)v_0^4 + 2(s_2 - \bar{s}_2)(v_0^3v_2 + v_0v_2^3).$$ (19)

Then Proposition 2 gives two more equations

$$2(s_0 - \bar{s}_0)v_0^2 + 4(s_2 - \bar{s}_2)v_0v_2 = 0$$

$$2(s_0 - \bar{s}_0)v_0^4 + 2(s_2 - \bar{s}_2)(v_0^3v_2 + v_0v_2^3) = q^2(q - 1)(q - p).$$ (20)

Therefore, one can deduce the values of $s_0, \bar{s}_0, s_1, \bar{s}_1, s_2, \bar{s}_2$ by solving the systems of equations (17) and (18). Then the distribution of $(T_0(a, b), T_0(-a, b))$ is determined and listed in Table V.

By (4)-(6), Tables IV and V, we have the following two theorems.
TABLE VI
THE VALUE DISTRIBUTION OF $\{T(a, b) \mid a, b \in \mathbb{F}_q\}$ FOR ODD $e$

<table>
<thead>
<tr>
<th>Values</th>
<th>Multiplicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$(p^n - 1)(p^n + p - 1)$</td>
</tr>
<tr>
<td>$p^{\frac{n+1}{2}}$</td>
<td>$(p^n - 1)(p^{n+1} + p + 1)/2$</td>
</tr>
<tr>
<td>$-p^{\frac{n+1}{2}}$</td>
<td>$(p^{n+1} - 1)(p^n + p - 1)/2$</td>
</tr>
<tr>
<td>$p^n$</td>
<td>1</td>
</tr>
</tbody>
</table>

TABLE VII
THE VALUE DISTRIBUTION OF $\{T(a, b) \mid a, b \in \mathbb{F}_q\}$ FOR EVEN $e$

<table>
<thead>
<tr>
<th>Values</th>
<th>Multiplicity (each)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$(p - 1)(p^{n+1} - 1)/(2(p + 1))$</td>
</tr>
<tr>
<td>$\pm \sqrt{p^2 + p^{n+1}}$</td>
<td>$(p^n - 1)(p^{n+1} - 3p^n + p + 1)/(4(p - 1))$</td>
</tr>
<tr>
<td>$\frac{1}{2}(\pm \sqrt{p^2 + p^{n+1}} + p^{n+1})$</td>
<td>$(p^n - 1)(p^{n+1} + p^n + 1)/2$</td>
</tr>
<tr>
<td>$\frac{1}{2}(\pm \sqrt{p^2 - p^{n+1}} + p^{n+1})$</td>
<td>$(p^n - 1)(p^{n+1} - p^{n+2})/2$</td>
</tr>
<tr>
<td>$\pm \frac{1}{2}(1 + p)\sqrt{p^2 + p^{n+1}}$</td>
<td>$(p^n - 1)(p^{n+1} - 1)/(p^2 - 1)$</td>
</tr>
<tr>
<td>$p^n$</td>
<td>1</td>
</tr>
</tbody>
</table>

Theorem 3: Let $T(a, b)$ be the exponential sum defined in (2). For $p \equiv 3 \pmod{4}$, odd $m \geq 3$ and an integer $e$ satisfying the Congruence Condition, the value distribution of the multi-set $\{T(a, b) \mid a, b \in \mathbb{F}_q\}$ is shown in Table VI if $e$ is odd and in Table VII if $e$ is even.

Theorem 4: Let $S(a, b, c)$ be the exponential sum defined in (3). For $p \equiv 3 \pmod{4}$, odd $m \geq 3$ and an integer $e$ satisfying the Congruence Condition, the value distribution of the multi-set $\{S(a, b, c)\mid a, b \in \mathbb{F}_q, c \in \mathbb{F}_p\}$ is shown in Table VIII if $e$ is odd and in Table IX if $e$ is even.

IV. WEIGHT DISTRIBUTION OF $C_{1(e,s)}$

In this section, for odd $m \geq 3$ and $p \equiv 3 \pmod{4}$, we study the weight distribution of the cyclic codes $C_{1(e,s)}$ for integers $e$ satisfying the Congruence Condition, i.e., there exist some positive integers $k$ coprime to $m$ such that $(p^k + 1)e \equiv 2 \pmod{p^m - 1}$.

Theorem 5: Let $p \equiv 3 \pmod{4}$, $s = (p^m - 1)/2$, $m \geq 3$ be an odd integer and $e$ be an integer satisfying the Congruence Condition. Then the weight distribution of the $[m^2, 2m + 1]_p$ cyclic code $C_{1(e,s)}$ is given in Table X if $e$ is odd and in Table XI if $e$ is even.

Proof: By (1), the Hamming weight of any nonzero codeword $c = (c_0, c_1, \ldots, c_{q-2}) \in C_{1(e,s)}$ is

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

(19)

where

$$\Delta(a, b, c) = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \omega y^{Tr(ax + bx^2 + cx^3)},$$

It suffices to determine the value distribution of $\Delta(a, b, c)$.

Let $Tr(c) = t$ and $Q_{a,b}(x) = Tr(ax^{p^t + 1} + bx^2)$. The exponential sum $\Delta(a, b, c)$ is investigated according to the parity of the integer $e$ in the following.

When $e$ is an odd integer satisfying the Congruence Condition, one has

$$\Delta(a, b, c) = \frac{1}{2} \sum_{y \in \mathbb{F}_p^*} \left(2 + \sum_{x \in \mathbb{F}_q^*} \omega y^{Tr(ax^{p^t + 1} + bx^2)} + \sum_{x \in \mathbb{F}_q} \omega y^{Tr(-ax^{p^t + 1} - bx^2)}\right),$$

$$= \frac{1}{2} \sum_{y \in \mathbb{F}_p^*} \left(2 + \sum_{x \in \mathbb{F}_q^*} \omega y^{Tr(ax^{p^t + 1} + bx^2 + c)} + \sum_{x \in \mathbb{F}_q} \omega y^{Tr(ax^{p^t + 1} - bx^2 + c)}\right),$$

$$= \sum_{y \in \mathbb{F}_p^*} \left(1 + \sum_{x \in \mathbb{F}_q^*} \omega y^{Tr(ax^{p^t + 1} + bx^2 + c)} + \sum_{x \in \mathbb{F}_q} \omega y^{Tr(ax^{p^t + 1} - bx^2 + c)}\right),$$

$$= \sum_{y \in \mathbb{F}_p^*} \left(1 - \omega y^t + \sum_{x \in \mathbb{F}_q} \omega y^{Q_{a,b}(x) + yt}\right),$$

$$= \sum_{y \in \mathbb{F}_p^*} \left(1 - \omega y^t + \omega y^t \left(\frac{\omega^t}{p}\right) \sum_{x \in \mathbb{F}_q} \omega^t Q_{a,b}(x)\right),$$

where $r$ is the rank of $Q(a, b)$ and the last equality sign comes from Lemma III.

Case I: $t = 0$. In this case, we have

$$\Delta(a, b, c) = \sum_{y \in \mathbb{F}_p^*} \left(\frac{\omega y^t}{p}\right) \sum_{x \in \mathbb{F}_q} \omega y^{Q_{a,b}(x)}.$$  

(20)

Case II: $t \neq 0$. It is easily seen that

$$\sum_{y \in \mathbb{F}_p^*} \omega y^t = -1$$

and

$$\sum_{y \in \mathbb{F}_p^*} \omega y^t \left(\frac{\omega^t}{p}\right) \sum_{x \in \mathbb{F}_q} \omega y^{Q_{a,b}(x)} = \left(\frac{\omega}{p}\right) \sum_{y \in \mathbb{F}_p^*} \omega y^t \left(\frac{\omega^t}{p}\right).$$

Then,

$$\Delta(a, b, c) = p + \sum_{y \in \mathbb{F}_p^*} \omega y^t \left(\frac{\omega^t}{p}\right) \sum_{x \in \mathbb{F}_q} \omega y^{Q_{a,b}(x)}.$$  

(21)

Recall that $T_0(a, b) = \sum_{x \in \mathbb{F}_q} \omega y^{Q_{a,b}(x)}$. According to the value distribution of $T_0(a, b)$ in Table IV, the weight distribution of $C_{1(e,s)}$ for odd $e$ can therefore be derived from (19), (20) and (21) by direct calculations.

When $e$ is an even integer satisfying the Congruence Condition,

$$\Delta(a, b, c) = \frac{1}{2} \sum_{y \in \mathbb{F}_p^*} \left(2 + \sum_{x \in \mathbb{F}_q^*} \omega y^{Q_{a,b}(x) + yt} \right. + \left. \sum_{x \in \mathbb{F}_q} \omega y^{Q_{a,b}(x) - yt}\right),$$

$$= \frac{1}{2} \sum_{y \in \mathbb{F}_p^*} \left(2 - \omega y^t + \omega y^t \right. + \left. \sum_{x \in \mathbb{F}_q} \omega y^{Q_{a,b}(x) + yt} \right. + \left. \sum_{x \in \mathbb{F}_q} \omega y^{Q_{a,b}(x) - yt}\right).$$
TABLE VIII
THE VALUE DISTRIBUTION OF \( \{S(a, b, c) \mid a, b \in \mathbb{F}_q, c \in \mathbb{F}_p' \} \) FOR ODD \( e \)

<table>
<thead>
<tr>
<th>Values</th>
<th>Multiplicity (each)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1 + \frac{1}{p} (a + \omega^{-t}) )</td>
<td>( p^2(p^m - 1)(p^m - p^{m-1} - p^{m-2} + 1)/(2(p^2 - 1)) )</td>
</tr>
<tr>
<td>( 1 - \frac{1}{p} (a + \omega^{-t}) + \frac{1}{p} (a + \omega^{-t}) \sqrt{p^2 p^m} )</td>
<td>( p^m - 1 )</td>
</tr>
<tr>
<td>( 1 - \frac{1}{2} (\omega^t + \omega^{-t}) + \frac{1}{2} (\omega^t + \omega^{-t}) \sqrt{p^2 p^m} )</td>
<td>( (p^m - 1)/2 )</td>
</tr>
<tr>
<td>( 1 + \frac{1}{p} (a + \omega^{-t}) )</td>
<td>( 1 )</td>
</tr>
</tbody>
</table>

where \( t = 0, 1, \ldots, p - 1 \).

TABLE IX
THE VALUE DISTRIBUTION OF \( \{S(a, b, c) \mid a, b \in \mathbb{F}_q, c \in \mathbb{F}_p' \} \) FOR EVEN \( e \)

<table>
<thead>
<tr>
<th>Values</th>
<th>Multiplicity (each)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1 + \frac{1}{p} (a + \omega^{-t}) + \frac{1}{p} (a + \omega^{-t}) \sqrt{p^2 p^m} )</td>
<td>( (p^m - 1)(p^m - 1)/(4(p^2 - 1)) )</td>
</tr>
<tr>
<td>( 1 - \frac{1}{2} (\omega^t + \omega^{-t}) + \frac{1}{2} (\omega^t + \omega^{-t}) \sqrt{p^2 p^m} )</td>
<td>( (p^m - 1)(p^m - 1)/(4(p^2 + 1)) )</td>
</tr>
<tr>
<td>( 1 - \frac{1}{2} (\omega^t + \omega^{-t}) + \frac{1}{2} (\omega^t + \omega^{-t}) \sqrt{p^2 p^m} )</td>
<td>( (p^m - 1)(p^m - 1)/(2(p^2 - 1)) )</td>
</tr>
<tr>
<td>( 1 - \frac{1}{2} (\omega^t + \omega^{-t}) + \frac{1}{2} (\omega^t + \omega^{-t}) \sqrt{p^2 p^m} )</td>
<td>( (p^m - 1)(p^m - 1)/(p^2 - 1) )</td>
</tr>
<tr>
<td>( 1 + \frac{1}{p} (a + \omega^{-t}) )</td>
<td>( 1 )</td>
</tr>
</tbody>
</table>

where \( t = 0, 1, \ldots, p - 1 \).

TABLE X
WEIGHT DISTRIBUTION OF \( C_{1,c,s} \) FOR ODD \( e \)

<table>
<thead>
<tr>
<th>Hamming weight</th>
<th>Multiplicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( p^m - 1 )</td>
<td>( p - 1 )</td>
</tr>
<tr>
<td>( p^m - 1 )</td>
<td>( p^m - 1 )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/(4(p^2 - 1)) )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/(4(p^2 + 1)) )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/(2(p^2 - 1)) )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/(p^2 - 1) )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
</tbody>
</table>

TABLE XI
WEIGHT DISTRIBUTION OF \( C_{1,c,s} \) FOR EVEN \( e \)

<table>
<thead>
<tr>
<th>Hamming weight</th>
<th>Multiplicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( p^m - 1 )</td>
<td>( p - 1 )</td>
</tr>
<tr>
<td>( p^m - 1 )</td>
<td>( p^m - 1 )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m + 1)/(4(p^2 - 1)) )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m + 1)/(4(p^2 + 1)) )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/(4(p^2 - 1)) )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/(4(p^2 + 1)) )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/(2(p^2 - 1)) )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/(p^2 - 1) )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) - \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
<tr>
<td>( (p^m - 1) + \frac{1}{p} )</td>
<td>( (p^m - 1)(p^m - 1)/2 )</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\sum_{y \in \mathbb{F}_p} \left( 2 - \frac{1}{p} (\omega y^t + \omega^{-y^t}) + \omega^{-y^t} \left( \frac{y^r}{p} \right) \sum_{x \in \mathbb{F}_q} \omega^{Q_{a,b}(x)} \right) + \omega^{-y^t} \left( \frac{y^r}{p} \right) \sum_{x \in \mathbb{F}_q} \omega^{Q_{-a,b}(x)} \right)
\end{align*}
\]

from Lemma III that \((r, r')\) takes value from the following set \((m, m), (m, m - 1), (m, m - 2), (m - 1, m), (m - 2, m)\).

Case I: \( t = 0 \). In this case,

\[
\Delta(a, b, c) = \frac{1}{2} \left( \sum_{y \in \mathbb{F}_p} \left( \frac{y^r}{p} \right) \sum_{x \in \mathbb{F}_q} \omega^{Q_{a,b}(x)} \right) + \sum_{y \in \mathbb{F}_p} \left( \frac{y^r}{p} \right) \sum_{x \in \mathbb{F}_q} \omega^{Q_{-a,b}(x)}
\]

where \( r, r' \) are the rank of \( Q(a, b) \) and \( Q(-a, b) \) respectively, and the last equality sign comes from Lemma III. It follows
By a similar analysis as in the case of odd $e$, the value distribution of $\Delta(a, b, c)$ is given in (24).

**Case II:** $t \neq 0$. Since $\sum_{y \in F_p^*} \omega^{y^t} = \sum_{y \in F_p} \omega^{-y^t} = -1$, one has

$$
\Delta(a, b, c) = p + \frac{1}{2} \left( \sum_{y \in F_p^*} \omega^{y^t} \left( \frac{y^t}{p} \right) \sum_{x \in F_q} \omega^{Q_{a,b}(x)} 
+ \sum_{y \in F_p^*} \omega^{-y^t} \left( \frac{y^t}{p} \right) \sum_{x \in F_q} \omega^{-Q_{a,b}(x)} \right). 
$$

Furthermore, the fact $\sum_{y \in F_p^*} \omega^{y^t} (\frac{y^t}{p}) = (\frac{1}{p}) \sqrt{p^r}$ and the possible values of $(r, r')$ in (23) imply (25).

Recall that $T_0(a, b) = \sum_{x \in F_q} \omega^{Q_{a,b}(x)}$. Thus, by the distribution of $(T_0(a, b), T_0(-a, b))$ in Table V, the value distribution of $\Delta(a, b, c)$ is given in (26).

By (19), (24) and (26), we deduce the weight distribution of $C_{1(1, e, s)}$ for even $e$.

Theorem 5 settles the weight distribution of $C_{1(1, e, s)}$ for $p \equiv 3 \pmod{4}$ and integers $e$ satisfying the Congruence Condition. For the special case $p = 3$, it is shown in [17] that the APN monomials $x^e$ generate the optimal cyclic codes $C_{1(1, e, s)}$ if

(i) $e = \frac{3^m+1}{2} + \frac{3^m-1}{2}$ [15]; or
(ii) $e = \frac{3^{m+1}}{2} - 1$ [15]; or
(iii) $e = (3^{m+1}/4 - 1)(3^{m+1}/2 + 1)$ for $m \equiv 3 \pmod{4}$ [24].

On the other hand, it is easily verify that the above integers $e$ satisfy the Congruence Condition. We thus have the following corollary.

**Corollary 4:** Let $x^e$ be a monomial over $F_{3^n}$ with

(i) $e = \frac{3^m+1}{2} + \frac{3^m-1}{2}$; or
(ii) $e = \frac{3^{m+1}}{2} - 1$; or
(iii) $e = (3^{m+1}/4 - 1)(3^{m+1}/2 + 1)$ for $m \equiv 3 \pmod{4}$.

Then the weight distribution of the $[3^m - 1, 2m + 1]$ ternary cyclic code $C_{1(1, e, s)}$ is given as in Table XII.

<table>
<thead>
<tr>
<th>Hamming weight</th>
<th>Multiplicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2 \cdot 3^m - 3 \cdot 3^{m-1} - 1$</td>
<td>$3^m - 1 \cdot 2 \cdot 3^m - 3 \cdot 3^{m-1}$</td>
</tr>
<tr>
<td>$2 \cdot 3^m - 3 \cdot 3^{m-1} - 1$</td>
<td>$3^m - 1 \cdot 2 \cdot 3^m - 3 \cdot 3^{m-1}$</td>
</tr>
<tr>
<td>$2 \cdot 3^m - 3 \cdot 3^{m-1} - 1$</td>
<td>$3^m - 1 \cdot 2 \cdot 3^m - 3 \cdot 3^{m-1}$</td>
</tr>
<tr>
<td>$2 \cdot 3^m - 3 \cdot 3^{m-1} - 1$</td>
<td>$3^m - 1 \cdot 2 \cdot 3^m - 3 \cdot 3^{m-1}$</td>
</tr>
<tr>
<td>$2 \cdot 3^m - 1$</td>
<td>$2$</td>
</tr>
</tbody>
</table>

For a linear code $C$ of length $n$ with weight distribution $(A_0, A_1, \ldots, A_n)$, its weight enumerator is defined by $A_0 + A_1x + \cdots + A_nx^n$.

**Example 1:** Let $p = 7$, $m = 3$ and $k = 2$. The integers $e = 130$ and $e = 301$ satisfy the congruence equation $50e \equiv 2$ (mod 342). If $e = 301$, then $C_{1(1, e, s)}$ is a $[342, 7, 244]$ cyclic code with the weight enumerator $1 + 1026x^{244} + 9576x^{252} + 344736x^{286} + 100890x^{294} + 359100x^{300} + 7182x^{336} + 10332x^{342}$, which agrees with Theorem 5 (i). If $e = 130$, then $C_{1(1, e, s)}$ is a $[342, 7, 272]$ cyclic code with the weight enumerator $1 + 2052x^{272} + 19152x^{273} + 175446x^{286} + 336528x^{293} + 84132x^{294} + 189810x^{300} + 2052x^{314} + 14364x^{315} + 6x^{342}$, which agrees with Theorem 5 (ii).

**Example 2:** Let $p = 3$ and $m = 3$. Then the integer $e$ in Corollary 4 is respectively $20$, $8$ and $20$. For $e = 8$ or $e = 20$, the numerical result indicates that $C_{1(1, e, s)}$ is a $[26, 7, 14]$ cyclic code with the weight enumerator $1 + 390x^{14} + 312x^{15} + 520x^{17} + 260x^{18} + 546x^{20} + 156x^{21} + 2x^{26}$, which agrees with Corollary 4, and the dual $C_{1(1, e, s)}^\perp$ has parameter [26, 19, 5], which agrees with the result in [17].
V. SUMMARY AND CONCLUDING REMARKS

One major contribution of this paper is the development of Theorem 1, which not only unifies the weight distributions of the twelve classes of cyclic codes documented in [5, 9], and [26], but also settles the weight distribution of new three-weight codes $C_{1,e}$ with two zeros such as those described in Corollaries 1, 2 and 3. In many cases, the duals of these three-weight codes $C_{1,e}$ are optimal [9], [10], [26].

Another major contribution of this paper is the settlement of the weight distributions of a class of cyclic codes $C_{1,e,x}$ with three zeros, which is documented in Theorem 5. In many cases the duals of the codes $C_{1,e,x}$ are also optimal [17]. Our technique in proving Theorem 5 is similar to that employed in [27].

APPENDIX

Proof of Proposition 1:

Note that the equation $x^2 + y^2 = \alpha$ is equivalent to $x^{p^m+1} + y^{p^m+1} + z^{p^m+1} - w^{p^m+1} = 0$.

Then, $N_4 = \sum_{\alpha, \beta \in F_{p^m}^2} N(\alpha, \beta)$. (27)

From the above analysis we deduce that when $\alpha \beta = 0$,

$$N(\alpha, \beta) = \begin{cases} 1, & \text{if } (\alpha, \beta) = (0, 0) \\ 0, & \text{otherwise}. \end{cases}$$ (30)

Case II: $\alpha \beta \neq 0$. We first consider the possible values of $N(\alpha, \beta)$.

Let $s, \tau \in F_{p^m}^*$ such that $s^2 = \alpha, \tau^2 = -1$. It is easy to verify that all solutions $x, y \in F_{p^m}$ of $x^2 + y^2 = \alpha$ have the form

$$x = \frac{1}{2} s(\theta + \theta^{-1}), \quad y = \frac{1}{2} s(t(\theta - \theta^{-1}), \quad \theta \in F_{p^m}^*.$$ (31)

The above representations of $x, y$ will be utilized to analyze the solutions of (28) in $F_{p^m}^2$.

For the first equation of (28), by applying the fact $x^{p^m} = x$ to (31), we get $x^{p^m-1}(\theta + \theta^{-1})^{p^m} = (\theta + \theta^{-1})$, which is equivalent to

$$\theta^{p^m+1} - \alpha^{(p^m-1)/2} \theta^{p^m-1} = \alpha^{(p^m-1)/2}.$$ (32)

Similarly, the fact $y^{p^m} = y$ gives

$$\theta^{p^m+1} - \alpha^{(p^m-1)/2} \theta^{p^m-1} + \alpha^{(p^m-1)/2} = 0.$$ (33)

By combining these two equations, we deduce

$$\theta^{p^m+1} = \alpha^{(p^m-1)/2}.$$ (34)

It follows from the second equation of (28) and (31) that

$$\left(\frac{1}{2} s(t(\theta + \theta^{-1}))^{p^m+1} + \left(\frac{1}{2} s(t(\theta - \theta^{-1}))^{p^m+1}\right)\theta^{p^m-1} + \alpha^{(p^m-1)/2}\right) = \beta.$$ (35)

Thus, if we take $\tau_1 = \theta^{p^m-1}$ and $\beta_1 = 2\alpha^{-(p^m+1)/2} \beta$, then $\tau_1, \tau_1^{-1}$ are the two solutions of the following equation

$$\tau^2 - \beta_1 \tau + 1 = 0.$$ (36)

By (32) and (33), we have

$$\theta^{p^m+1} = \alpha^{(p^m-1)/2}, \quad \theta^{p^m-1} = \tau_1$$ (37)

and

$$\theta^{p^m+1} = \alpha^{(p^m-1)/2}, \quad \theta^{p^m-1} = \tau_1^{-1}.$$ (38)

If $\beta_1 = 2$, then $\tau_1 = \tau_1^{-1} = \theta^{p^m-1} = 1$ and (35) is the same as (34). Note that $\gcd(2(p^m + 1), p^k - 1) = 2(p + 1)$ when $k$ is even and $\gcd(m, k) = 1$. Then $\theta^2(p^m+1) = \alpha^{(p^m-1)}$ is $1$ together with $\theta^{p^m-1} = 1$ gives $\theta^2(p^m+1) = 1$. Furthermore, since $m$ is odd and $\alpha^{(p^m-1)/2} = \pm 1$, one gets $\theta^{p^m+1} = \alpha^{(p^m-1)/2}$, which indicates that (34) has exactly $p + 1$ solutions in $F_{p^m}$.

If $\beta_1 = -2$, then $\tau_1 = \tau_1^{-1} = \theta^{p^m-1} = -1$ and (35) is the same as (34). The fact $\theta^2(p^m+1) = \theta^2(p^m-1) = 1$ suggests $\theta^{\gcd(2(p^m+1), 2(p^m-1))} = \theta^{2(p^m+1)} = 1$, which is in contradiction with $\theta^{p^m-1} = -1$ since $2(p + 1)(p^k - 1)$. Thus, (34) has no solution in this case.

If $\beta_1 \neq \pm 2$, then $\tau_1 \neq \tau_1^{-1}$. It is readily seen that $\theta$ is a solution of (34) if and only if $\theta^{-1}$ is a solution of (35).

Suppose $\theta_1$ and $\theta_2$ are two solutions of (34). Then ($\theta_1/\theta_2)^{p^m+1} = (\theta_1/\theta_2)^{p^m-1} = 1$, and this implies ($\theta_1/\theta_2)^{p^m+1} = 1$ since $\gcd(p^m + 1, p^k - 1) = p + 1$. As a result, (34) has a solution $\theta$, all solutions of (34) can be represented as $\mu \theta$,
and all solutions of (35) can be represented as $\mu \theta^{-1}$, where $\mu \in \mathbb{F}_{p^m}$ and $\mu^{p+1} = 1$. Therefore for (34) and (35), either each of them has exactly $p+1$ solutions or none of them has a solution.

In summary, for $\alpha \beta \neq 0$,

$$N_1(\alpha, \beta) = \begin{cases} p + 1, & \text{if } \beta = \alpha(p^{k+1})/2, \\ 0, & \text{if } \beta = -\alpha(p^{k+1})/2, \\ 0 \text{ or } 2(p+1), & \text{otherwise.} \end{cases}$$

(36)

Now we turn to analyze the possible values of $N_2(\alpha, \beta)$. The analysis proceeds in a similar fashion to that for $N_1(\alpha, \beta)$.

Recall that $s, r \in \mathbb{F}_{p^m}$ with $s^2 = \alpha$ and $r^2 = -1$. Thus all solutions of $z^2 + w^2 = -\alpha$ can be represented as $z = \frac{1}{2}s(\theta^2 + \theta^{-1}), \quad w = \frac{1}{2}s(\theta - \theta^{-1}), \quad \theta \in \mathbb{F}_{p^m}$. (37)

For the first equation of (29), the facts $\varphi^{p^m} = z$ and $w^{p^m} = w$ imply

$$\varphi^{p^m+1} = -\alpha(p^{m-1})/2,$$

(38)

and the second equation of (29) together with (37) yields

$$\frac{1}{2}\alpha(p^{k+1}/2(\varphi^{p^k+1} + \varphi^{-(p^k+1)}) = \beta.$$ 

Assume $t_2 = \varphi^{p^m+1}$ and $b_1 = 2\alpha(-p^{k+1}/2)\beta$. Then $t_2, t_2^{-1}$ are the two solutions of

$$r^2 - b_1 r + 1 = 0.$$ 

(39)

This equation is the same as Equation (33). Thus $t_2 \in \{t_1, t_1^{-1}\}$.

By (38) and (39), we get the following equations:

$$\varphi^{p^m+1} = -\alpha(p^{m-1})/2, \quad \varphi^{p^m+1} = t_2$$

(40)

and

$$\varphi^{p^m+1} = -\alpha(p^{m-1})/2, \quad \varphi^{p^m+1} = t_2^{-1}.$$ 

(41)

If $b_1 = 2$, then $t_2 = t_2^{-1} = \varphi^{p^k+1} = 1$ and (41) is the same as (40). Since gcd($2(p^{m+1}), p^{k+1} = 2$), one deduces $\varphi^2 = 1$. Therefore, (40) has exactly 2 solutions $\varphi = \pm 1$ if $\alpha$ is a non-square and has no solution otherwise.

If $b_1 = -2$, then $t_2 = t_2^{-1} = \varphi^{p^k+1} = -1$ and (41) is the same as (40). The fact gcd($2(p^{m+1}), 2(p^k+1) = 4$) suggests $\varphi^4 = 1$, and then $\varphi^2 = -1$. Thus, (40) has exactly 2 solutions $\varphi = \pm t \theta$ if $\alpha$ is a non-square, where $t^2 = -1$, and has no solution otherwise.

If $b_1 \neq \pm 2$, then $t_2 \neq t_2^{-1}$. Note that $\varphi$ is a solution of (40) if and only if $\varphi^{-1}$ is a solution of (41). Suppose $\varphi_1$ and $\varphi_2$ are the two solutions of (40). Then $\varphi_1/\varphi_2 = \varphi^{p^{m+1}} = (\varphi_1/\varphi_2)^{p^{m+1}+1} = 1$, and this implies $(\varphi_1/\varphi_2)^2 = 1$. Consequently, for (40) and (41), either they respectively have solutions $\pm \varphi$ and $\pm \varphi^{-1}$, or none of them has a solution.

Summarizing up, for $\alpha \beta \neq 0$, we have

$$N_2(\alpha, \beta) = \begin{cases} 2, & \text{if } \beta = \pm\alpha(p^{k+1})/2, \quad \alpha \in \mathcal{N}, \\ 0, & \text{if } \beta = \pm\alpha(p^{k+1})/2, \quad \alpha \in \mathcal{Q}, \\ 0 \text{ or } 4, & \text{otherwise.} \end{cases}$$ 

(42)

(43)

To complete the proof, the next task is to consider the possible values of $N(\alpha, \beta)$ for $\alpha \in \mathbb{F}_{p^m}^*$ and $\beta \in \mathbb{F}_{p^m}^* \setminus \{\pm\alpha(p^{k+1})/2\}$. Thus we turn back to Equations (34), (35), (40) and (41) and gather them together as below

$$\begin{aligned}
\theta^{p^{m+1}} &= \alpha(p^{m-1})/2, \\
\varphi^{p^{m+1}} &= \alpha(p^{m-1})/2,
\end{aligned}$$

(44)

since $t_2 \in \{t_1, t_1^{-1}\}$. For a fixed $\alpha \in \mathbb{F}_{p^m}^*$, let $\mathcal{T} = \mathbb{F}_{p^m}^* \setminus \{\pm\alpha(p^{k+1})/2\}$ and define

$$S_1(\alpha) = \begin{cases} \beta \in \mathcal{T} | (34), (35) \text{ have } p+1 \text{ solutions}, \\ S_2(\alpha) = \beta \in \mathcal{T} | (40), (41) \text{ have } 2 \text{ solutions}. \end{cases}$$

Then (36) and (42) suggest that $N(\alpha, \beta) = 8(p+1)$ if $\beta \in S_1(\alpha) \cap S_2(\alpha)$ and $N(\alpha, \beta) = 0$ otherwise. In what follows, we shall show that if $\alpha$ is a square, then $S_1(\alpha) \cap S_2(\alpha) = \emptyset$; and if $\alpha$ is a non-square, then $S_1(\alpha) \subseteq S_2(\alpha)$.

When $\alpha$ is a square, i.e., $\alpha(p^{m-1})/2 = 1$, the equations in the first row of (44) yield

$$t_1^{p^{m+1}/2} = (\varphi^{p^{m+1}/2})(\varphi^{p^{m+1}/2}) = (\varphi^{p^{m+1}})^{\pm(p^{k+1}/2)} = 1,$$

while the equations in the second row of (44) imply

$$t_1^{p^{m+1}/2} = (\varphi^{p^{m+1}/2})(\varphi^{p^{m+1}/2}) = (\varphi^{p^{m+1}})^{\pm(p^{k+1}/2)} = (-1)^{\pm(p^{k+1}/2)} = -1.$$

This is a contradiction. Thus, there do not exist $\theta, \varphi \in \mathbb{F}_{p^m}^*$ satisfying (44), which is equivalent to $S_1(\alpha) \cap S_2(\alpha) = \emptyset$.

When $\alpha$ is a non-square, i.e., $\alpha(p^{m-1})/2 = -1$, one has $\theta^{p^{m+1}+1} = -1$ and $\varphi^{p^{m+1}+1} = 1$. Let $\zeta$ be a primitive element of $\mathbb{F}_{p^{2m}}$. Then $\theta$ and $\varphi$ can be respectively represented as $\theta = \zeta^{(p^{m+1})/2}$ and $\varphi = \zeta^{(p^{m-1})/2}$, where $i, j \in \{0, 1, \ldots, p^m-1\}$. Assume $t_1 = \zeta^i$, then the equation $\theta^{p^{m+1}} = t_1$ is equivalent to $(2i+1)(p^m-1)(p^k-1)/2 \equiv r \pmod{p^{2m}-1}$. For any $\beta \in S_1(\alpha)$, by the definition of $S_2(\alpha)$, this linear congruence equation with variable $i$ has $p+1$ solutions. Thus, gcd($2(p^{m+1}-1)(p^{k+1}-1)/2$, $p^{2m}-1$) divides $p+1$, and gcd($2(p^{m+1}-1)/2$, $p^{2m}-1$) divides $p+1$, one has
gcd($2(p^{m+1}-1)(p^{k+1}-1)/2$, $p^{2m}-1$) divides $p+1$.

This implies the congruence equation $(p^{m+1}-1)(p^{k+1}+1) \equiv r \pmod{p^{2m}-1}$ with variable $j$ has solutions. Thus, the equations $\theta^{p^{m+1}} = 1$ and $\varphi^{p^{m+1}} = t_1$, $t_1^{-1}$ have 4 solutions. This implies that $\beta$ is also contained in $S_2(\alpha)$. Then $S_1(\alpha)$ is a subset of $S_2(\alpha)$.

Therefore, for $\alpha \in \mathbb{F}_{p^m}^*$ and $\beta \in \mathbb{F}_{p^m}^* \setminus \{\pm\alpha(p^{k+1})/2\}$, we have

$$N(\alpha, \beta) = \begin{cases} 8(p+1), & \text{if } \alpha \text{ is a non-square, } \beta \in S_1(\alpha), \\ 0, & \text{otherwise}. \end{cases}$$

(46)
Combining (27), (30), (43) and (46) gives

\[ N_4 = 1 + ((p + 1) + 4(p + 1)|S_1(a))(p^m - 1). \]

Thus, to determine the value of \( N_4 \), we only need to calculate the cardinality of the set \( S_1(a) \). Given \( a \in \mathbb{F}_{p^m}^* \), by [18, Lemma 6.24], the equation \( x^2 + y^2 = \alpha \) has \( p^m + 1 \) solutions in \( \mathbb{F}_{p^m}^* \). Among all these solutions, by (36), if \( \beta = \alpha^{(p^m+1)/2} \), there are exactly \( p + 1 \) solutions satisfying \( x^{p^k+1} + y^{p^k+1} = \beta \), and for any \( \beta \in S_1(a) \), there are exactly \( 2(p + 1) \) solutions satisfying \( x^{p^k+1} + y^{p^k+1} = \beta \). Thus, \( (p + 1) + 2(p + 1)|S_1(a)| = p^m + 1 \), which implies \( |S_1(a)| = (p^m - p)/2(p + 1) \).

Therefore, for \( p \equiv 3 \) (mod 4)

\[ N_4 = 1 + ((p + 1) + 2(p^m - p))(p^m - 1) = 2p^{2m} - p^{m+1} - p^m + p. \]

The analysis on the value of \( N_4 \) for \( p \equiv 1 \) (mod 4) is similar in spirit to that for \( p \equiv 3 \) (mod 4) and is thus omitted. The proof is completed. \( \square \)

REFERENCES


Chunlei Li received the B.S. and M.S. degrees in mathematics from Hubei University, Wuhan, China, in 2005 and 2008, respectively. He is currently working toward the Ph.D. degree at the Department of Informatics, University of Bergen, Norway. His research interests include cryptography, sequence design and coding theory.

Nian Li received the B.S. and M.S. degrees in mathematics from Hubei University, Wuhan, China, in 2006 and 2009, respectively, and he received the Ph.D. degree at the Southwest Jiaotong University, Chengdu, China, in 2013. From Sept. 2011 to Aug. 2013, he was a visiting Ph.D. student in the Department of Informatics, University of Bergen, Norway. Currently, he is working as a postdoc in the Department of Mathematics, the Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. His research interests include sequence design and coding theory.

Tor Helleseth (M’89–SM’96–F’97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively. From 1973-1980, he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981-1984, he was at the Chief Head quarters of Defense in Norway. Since 1984, he has been a Professor in the Department of Informatics, University of Bergen. During the academic years 1977-1978 and 1992-1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979-1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, the Netherlands. His research interests include coding theory and cryptography. Prof. Helleseth served as an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 1991 to 1993. He was Program Chairman for Eurocrypt 1993 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He was a Program Co-Chairman for SETA in 1998, 2001, 2004, 2006 and 2012. He was also a Program Co-Chairman for the IEEE Information Theory Workshop in Delftland, Norway in 2007. During 2007-2009 he served on the Board of Governors for the IEEE Information Theory Society. In 2004 he was elected as a member of Det Norske Videnskaps-Akademii.

Cunsheng Ding (M’98–SM’05) was born in 1962 in Shaannxi, China. He received the M.S. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland. From 1988 to 1992 he was a Lecturer of Mathematics at Xiian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a professor at Department of Computer Science and Engineering, he was an assistant professor of Computer Science at the National University of Singapore. His research fields are cryptography and coding theory. He has coauthored four research monographs, and served as a guest editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.