THE WEIGHT DISTRIBUTIONS OF SEVERAL CLASSES OF CYCLIC CODES FROM APN MONOMIALS

Chunlei Li * Nian Li† Tor Helleseth*

Cunsheng Ding‡

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 $\mathcal{C}_{(1,e)}$ over $\mathbb{F}_p$, which have parity-check polynomial $m_1(x)m_e(x)$, are presented by examining general conditions on the parameters p, m and e, where $m_i(x)$ is the minimal polynomial of π^{-i} over $\mathbb{F}_p$ for a primitive element π of $\mathbb{F}_{p^m}$. Furthermore, for $p \equiv 3 \pmod 4$ and a positive integer e satisfying $(p^k+1)\cdot e \equiv 2 \pmod{p^m-1}$ for some positive integer k with $\gcd(m,k) = 1$, the value distributions of the exponential sums $T(a,b) = \sum_{x\in\mathbb{F}_{p^m}} \omega^{\mathrm{Tr}(ax+bx^e)}$ and $S(a,b,c) = \sum_{x\in\mathbb{F}_{p^m}} \omega^{\mathrm{Tr}(ax+bx^e+cx^s)}$, 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 $\mathcal{C}_{(1,e,s)}$ with parity-check polynomial $m_1(x)m_e(x)m_s(x)$. In the case of $p = 3$ and even e satisfying the above condition, the dual of the cyclic code $\mathcal{C}_{(1,e,s)}$ has optimal minimum distance.

*Department of Informatics, University of Bergen, PB 7803, N-5020 Bergen, Norway

†Inf. Security and National Computing Grid Lab, Southwest Jiaotong Univ., Chengdu, China

‡Dept. of Computer Sci. and Engineering, Univ. of Sci. and Tech. Hong Kong, China

1 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 $[n, \kappa, \rho]$ code $\mathcal{C}$ over $\mathbb{F}_p$ is a κ-dimensional subspace of $\mathbb{F}_p^n$ with minimum (Hamming) nonzero weight ρ. Let A_i denote the number of codewords in $\mathcal{C}$ with Hamming weight i. The weight distribution $(A_0, A_1, \cdots, A_n)$ 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 $\mathcal{C}$ over $\mathbb{F}_p$ is called *cyclic* if any cyclic shift of a codeword is another codeword of $\mathcal{C}$. 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 $\mathcal{C} = \langle g(x) \rangle$, 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 $\mathcal{C}$. 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, for example, [4, 9, 10, 13, 14, 20, 22, 23]). In this paper, cyclic codes with τ nonzero weights are called τ-weight cyclic codes.

Let Γ_j be the p-cyclotomic coset modular $q-1$ containing j, i.e., $\Gamma_j = \{j \cdot p^i \bmod (q-1) | i = 0, 1, \cdots, l_j - 1\}$, where j is any integer with $0 \le j \le q-2$ and l_j is the smallest positive integer such that $j \equiv j \cdot p^{l_j} \bmod (q-1)$. Let $\mathbb{Z}_{q-1}$ be the set of integers modulo $q-1$ and $m_i(x)$ be the minimal polynomial of π^{-i} over $\mathbb{F}_p$ for a primitive element π in $\mathbb{F}_q$. For integers $i_1, \cdots, i_t \in \mathbb{Z}_{q-1}$, $t \ge 1$ with pairwise disjoint cyclotomic cosets $\Gamma_{i_1}, \cdots, \Gamma_{i_t}$, we denote by $\mathcal{C}_{(i_1, \cdots, i_t)}$ the cyclic code with parity-check polynomial $h(x) = m_{i_1}(x) \cdots m_{i_t}(x)$ and write $\mathcal{C}^{\perp}_{(i_1, \cdots, i_t)}$ for its dual code. By the well-known Delsarte's Theorem [7], one can express the cyclic code $\mathcal{C}_{(i_1, \cdots, i_t)}$ as

$$\mathcal{C}_{(i_1, \cdots, i_t)} = \left\{ \Big(\sum_{s=1}^{t} \mathrm{Tr}(a_s \pi^{j \cdot i_s}) \Big)_{j=0}^{q-2} \,\Big|\, a_1, a_2, \cdots, a_t \in \mathbb{F}_q \right\},$$

where $\mathrm{Tr}(\cdot)$ is the trace mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$. Hence the Hamming weight of the codeword $\mathbf{c} = (c_0, c_1, \cdots, c_{q-2})$ in $\mathcal{C}_{(i_1,\cdots,i_t)}$ satisfies

$$\begin{aligned} w_H(\mathbf{c}) =& \big|\{j \,|\, 0 \le j \le q-2,\, c_j \neq 0\}\big| \\ =& (q-1) - \big|\{j \,|\, 0 \le j \le q-2,\, c_j = 0\}\big| \\ =& (q-1) - \frac{1}{p} \sum_{x\in\mathbb{F}_q^*} \sum_{y\in\mathbb{F}_p} \omega^{y\cdot \mathrm{Tr}(\sum_{s=1}^{t} a_s x^{i_s})} \\ =& \frac{(q-1)(p-1)}{p} - \frac{1}{p} \sum_{y\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}(y\sum_{s=1}^{t} a_s x^{i_s})} \\ =& p^{m-1}(p-1) - \frac{1}{p} \sum_{y\in\mathbb{F}_p^*} S(ya_1, ya_2, \cdots, ya_t), \end{aligned} \tag{1}$$

where $S(a_1, a_2, \cdots, a_t) = \sum_{x\in\mathbb{F}_q} \omega^{\mathrm{Tr}(a_1 x^{i_1} + a_2 x^{i_2} + \cdots + a_t x^{i_t})}$ and ω is a primitive p-th root of unity. In this way, the weight distribution of the cyclic code $\mathcal{C}_{(i_1,\cdots,i_t)}$ can be derived from the value distribution of the multi-set

$$\{S(a_1, a_2, \cdots, a_t) \,|\, a_1, a_2, \cdots, a_t \in \mathbb{F}_q\}.$$

Perfect nonlinear (PN) and almost perfect nonlinear (APN) functions are important research objects in cryptography and coding theory [1, 2, 6]. For $p = 2$, it is shown in [3] that the monomial x^e is APN if and only if the cyclic code $\mathcal{C}^{\perp}_{(1,e)}$ has optimal minimum distance 5. In [23], the Gold and Kasami-Welch APN monomials were utilized to construct a class of cyclic codes $\mathcal{C}^{\perp}_{(1,3,13)}$ having the same weight distribution as the triple-error-correcting BCH code $\mathcal{C}^{\perp}_{(1,3,5)}$. For odd prime p, when x^e is a PN monomial over $\mathbb{F}_q$, the cyclic codes $\mathcal{C}_{(1,e)}$ and $\mathcal{C}_{(0,1,e)}$ and their duals were intensively studied in [4, 12, 17, 21], where the weight distributions of the cyclic codes $\mathcal{C}_{(1,e)}$ and $\mathcal{C}_{(0,1,e)}$ were determined and their dual codes were proved to have optimal minimum distances 4 and 5 respectively. Very recently, for $p = 3$ and some monomials x^e including APN ones, the ternary cyclic codes $\mathcal{C}^{\perp}_{(1,e)}$ and $\mathcal{C}^{\perp}_{(1,e,s)}$, where $s = (3^m - 1)/2$, were shown to have optimal minimum distances 4 and 5 in [8] and [18]. The weight distributions of the proposed cyclic codes and their duals are mostly unknown.

In this paper, for odd integer $m \ge 3$, we will derive general conditions on the parameters p, m and e under which $\mathcal{C}_{(1,e)}$ is a three-weight code.

It turns out that all the three-weight cyclic codes recently found in [5, 11, 25] 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 $p \equiv 3 \pmod 4$ and a positive integer e satisfying $(p^k+1) \cdot e \equiv 2 \pmod{p^m-1}$ for some positive integer k with $\gcd(m,k) = 1$, we will determine the value distributions of the two exponential sums

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

and

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

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 $\mathcal{C}_{(1,e,s)}$. For $p = 3$ and even e satisfying $(p^k+1) \cdot e \equiv 2 \pmod{p^m-1}$, the cyclic codes $\mathcal{C}^{\perp}_{(1,e,s)}$ have optimal minimum distance 5 [18].

The remainder of this paper is organized as follows. Section 2 presents a unified approach to generating three-weight cyclic codes, of which the weight distributions are as well settled. Section 3 deals with the value distributions of the exponential sums $T(a,b)$ and $S(a,b,c)$. Section 4 determines the weight distribution of the cyclic code $\mathcal{C}_{(1,e,s)}$. Section 5 concludes this paper.

2 Three-weight cyclic codes and their weight distributions

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

In [4, 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 $\mathcal{C}_{(1,e)}$ has length $q-1$, dimension $2m$, and the weight distribution in Table 1 if*

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

Table 1: *Weight distribution I*

Hamming weight	Multiplicity
0	1
$(p-1)p^{m-1}-p^{\frac{m-1}{2}}$	$\frac{1}{2}(p-1)(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})$
$(p-1)p^{m-1}+p^{\frac{m-1}{2}}$	$\frac{1}{2}(p-1)(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})$
$(p-1)p^{m-1}$	$(p^m-1)(p^{m-1}+1)$

Table 2: *Weight distribution II*

Hamming weight	Multiplicity
0	1
$(p-1)p^{m-1}-\frac{(p-1)}{2}p^{\frac{m+s-2}{2}}$	$(p^m-1)(p^{m-s}+p^{\frac{m-s}{2}})$
$(p-1)p^{m-1}+\frac{(p-1)}{2}p^{\frac{m+s-2}{2}}$	$(p^m-1)(p^{m-s}-p^{\frac{m-s}{2}})$
$(p-1)p^{m-1}$	$(p^m-1)(p^m-2p^{m-s}+1)$

The second construction in Lemma 1 was extended to any odd prime p and positive integer k, $1 \leq k \leq m-1$, in [20, 26].

Lemma 2. *([20, 26]) 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 $\mathcal{C}_{(1,e)}$ has length $q-1$, dimension $2m$, and the weight distribution in Table 2 if k/s is odd and in Table 3 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 $p-1=2^r \cdot h$, where h is an odd integer. If two integers d, $e \in \mathbb{Z}_{p^m-1} \setminus \Gamma_1$ satisfy $2de \equiv 2 \pmod{p^m-1}$ and $d+e \equiv 2 \pmod{2^r}$, then the cyclic codes $\mathcal{C}_{(1,d)}$ and $\mathcal{C}_{(1,e)}$ have the same weight distribution.*

Proof. According to (1), the weight distributions of $\mathcal{C}_{(1,d)}$ and $\mathcal{C}_{(1,e)}$ are respectively determined by the value distributions of

$$\Delta_0(a,b)=\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\omega^{\mathrm{Tr}(yax+ybx^d)}$$

Table 3: *Weight distribution III*

Hamming weight	Multiplicity
0	1
$(p-1)p^{m-1}-(p-1)p^{\frac{m+s-2}{2}}$	$\frac{1}{2}(p^m-1)(p^{m-s}+p^{\frac{m-s}{2}})$
$(p-1)p^{m-1}+(p-1)p^{\frac{m+s-2}{2}}$	$\frac{1}{2}(p^m-1)(p^{m-s}-p^{\frac{m-s}{2}})$
$(p-1)p^{m-1}$	$(p^m-1)(p^m-p^{m-s}+1)$

and

$$\Delta_1(a,b)=\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\omega^{\mathrm{Tr}(yax+ybx^e)}.$$

Notice that h and m are odd. The element $\lambda=\pi^{\frac{(p^m-1)h}{p-1}}$, where π is a primitive element in $\mathbb{F}_{p^m}$, is a non-square in $\mathbb{F}_{p^m}$. It then follows from $p-1=2^r\cdot h$ that the order of λ in $\mathbb{F}_p^*$ (the least integer t such that $\lambda^t=1$) equals 2^r .

When x runs through $\mathbb{F}_q^*$, x^2 runs twice through the squares in $\mathbb{F}_q^*$, and λx^2 runs twice through all the non-squares in $\mathbb{F}_q^*$. Thus,

$$\begin{aligned}\Delta_0(a,b)&=\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(\sum_{x\in\mathbb{F}_q}\omega^{\mathrm{Tr}(yax^2+ybx^{2d})}+\sum_{x\in\mathbb{F}_q}\omega^{\mathrm{Tr}(ya\lambda x^2+yb\lambda^d x^{2d})}\Big)\\&=\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(ax^2+bx^{2d})}+\sum_{x\in\mathbb{F}_q}\omega^{y\lambda\mathrm{Tr}(ax^2+\lambda^{d-1}bx^{2d})}\Big)\\&=\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(ax^2+bx^{2d})}+\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(ax^2+\lambda^{d-1}bx^{2d})}\Big).\end{aligned}$$

Note that $2de\equiv 2 \pmod{p^m-1}$ implies $\gcd(2d,p^m-1)=2$. Thus, when x runs through $\mathbb{F}_q^*$, x^{2d} runs twice through the squares in $\mathbb{F}_q^*$, and λx^{2d} runs twice through all the non-squares in $\mathbb{F}_q^*$. Similarly we have

$$\Delta_1(a,b)=\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(ax^{2d}+bx^2)}+\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(ax^{2d}+\lambda^{e-1}bx^2)}\Big).$$

Furthermore, it follows from $d+e \equiv 2 \pmod{2^r}$ and $\lambda^{2^r}=1$ that

$$\begin{aligned}\Delta_0(a,b) &= \frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(ax^2+bx^{2d})}+\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(\lambda^{e+d-2}ax^2+\lambda^{d-1}bx^{2d})}\Big)\\ &= \frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(ax^2+bx^{2d})}+\sum_{x\in\mathbb{F}_q}\omega^{y\lambda^{d-1}\mathrm{Tr}(\lambda^{e-1}ax^2+bx^{2d})}\Big)\\ &= \frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(ax^2+bx^{2d})}+\sum_{x\in\mathbb{F}_q}\omega^{y\mathrm{Tr}(\lambda^{e-1}ax^2+bx^{2d})}\Big)\\ &= \Delta_1(b,a).\end{aligned}$$

Therefore, the multi-sets $\{\Delta_0(a,b) : a,b\in\mathbb{F}_q\}$ and $\{\Delta_1(a,b) : a,b\in\mathbb{F}_q\}$ have the same value distribution. □

Applying Lemmas 1-3, we obtain the following.

Theorem 1. *Let $m\geq 3$ be odd. (i) Let $p\equiv 3 \pmod 4$. If e is an even integer satisfying $2(p^k+1)e\equiv 2 \pmod{p^m-1}$ for some nonnegative integer k, then $\mathcal{C}_{(1,e)}$ is a $[p^m-1,2m]$ cyclic code with the weight distribution in Table 1. (ii) Let p be any odd prime. If e is an integer satisfying $(p^k+1)e\equiv 2 \pmod{p^m-1}$ for some positive integer k with $\gcd(m,k)=s$, then $\mathcal{C}_{(1,e)}$ is a $[p^m-1,2m]$ cyclic code with the weight distribution of*

- *Table 2 when $e\equiv 1+(p-1)/2 \pmod{p-1}$; and*
- *Table 3 when $e\equiv 1 \pmod{p-1}$.*

Proof. (i) When m is odd and $p\equiv 3 \pmod 4$, we have $p-1=2^rh$ with $r=1$ and $h=(p-1)/2$ being odd. Set $d=p^k+1$. By assumption, $2de\equiv 2 \pmod{p^m-1}$. Then $|\Gamma_e|=m$ since $\gcd(2de,p^m-1)=2$ implies $\frac{p^m-1}{2}|p^{le}-1$. In addition, we have $e+d\equiv 2 \pmod{2^r}$ as e is even by assumption and d is obviously even.

Since m is odd and $p\equiv 3 \pmod 4$, $p^m\equiv 3 \pmod 4$. Hence $\gcd(2(p^k+1),p^m-1)=2$. It then follows that $e\notin\Gamma_1$. It is clear that $d\notin\Gamma_1$. Thus, all the conditions in Lemma 3 are satisfied. Then it follows from Lemmas 1 and 3 that $\mathcal{C}_{(1,e)}$ has the weight distribution of Table 1.

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

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

In the case of $e \equiv 1 \pmod{p-1}$, 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 $d = (p^{k_0}+1)/2$. We have $d \equiv 1 + (p^{k_0}-1)/2 \equiv 1 + k_0(p-1)/2 \equiv 1 \pmod{p-1}$. Then $d + e \equiv 2 \pmod{p-1}$. In addition, by assumption $(p^k+1)e \equiv \pmod{p^m-1}$, we have $2de \equiv 2 \pmod{p^m-1}$ if k is even and $2de \equiv 2p^{m-k} \pmod{p^m-1}$ 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 $\mathcal{C}_{(1,e)}$ are the same when e runs through the cyclotomic coset Γ_e. The conclusion thus follows from Lemmas 2 and 3.

Similarly, in the case of $e \equiv 1 + (p-1)/2 \pmod{p-1}$, we take $k_1 = k$ if k is odd and $k_1 = m - k$ if k is even. Then k_1 is odd and $(p^{k_1}+1)/2 \equiv 1 + k_1(p-1)/2 \equiv 1 + (p-1)/2 \pmod{p-1}$. Let $d = (p^{k_1}+1)/2$. Then $d + e \equiv 2 \pmod{p-1}$. In addition, $2de \equiv 2 \pmod{p^m-1}$ if k is odd and $2de \equiv 2p^{m-k} \pmod{p^m-1}$ if k is even. Since the cyclic codes $\mathcal{C}_{(1,e)}$ are the same when e runs through the cyclotomic coset Γ_e, it follows from Lemmas 2 and 3 that $\mathcal{C}_{(1,e)}$ has the weight distribution of Table 2 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 $\mathbb{F}_p$ are described in [5, 11, 25]. It can be verified by hand that all the three-weight cyclic codes found in [5, 11, 25] are special cases of the codes in Theorem 1. Furthermore, a closer look at Theorem 1 reveals that many new three-weight cyclic codes can be generated in this way.

The following are three corollaries of Theorem 1, which give new three-weight codes that are not covered in [5, 25] and [11]. They demonstrate that Theorem 1 can be employed to generate many new three-weight cyclic codes and settle their weight distributions.

Corollary 1 below is an extension of Theorem 6.11 in [25] and Theorem 4.8 in [11], and produces new three-weight codes that are not covered in [5, 25] and [11] when $t > 3$.

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

Proof. Let $d = (3^{(m+1)/2^h} + 1)$. Then $de \equiv 2 \pmod{3^m - 1}$. We have clearly that $\gcd((m+1)/2^h, m) = 1$. In addition, $\left(3^{(m+1)/2^h} - 1\right) \prod_{i=1}^{h-1} \left(3^{(m+1)/2^i} + 1\right) \equiv 2 \pmod{p-1}$. 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, 11, 25] 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 $\mathcal{C}_{(1,e)}$ is a $[p^m - 1, 2m]$ cyclic code with the weight distribution in Table 1.*

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_i be defined by $S_i = \left\{ \frac{(p+1)(p^m-1)-4p(p^{\frac{m-1}{2}}-1)}{2(p-1)} + \frac{i(p^m-1)}{2}, \frac{(p-3)(p^m-1)+4(p^{\frac{m+1}{2}}-1)}{2(p-1)} + \frac{i(p^m-1)}{2} \right\}, i = 0, 1$. (i) If $e \in S_0$, then $\mathcal{C}_{(1,e)}$ is a $[p^m - 1, 2m]$ cyclic code with the weight distribution in Table 2, where $s = 1$. (ii) If $e \in S_1$, then $\mathcal{C}_{(1,e)}$ is a $[p^m - 1, 2m]$ cyclic code with the weight distribution in Table 3, where $s = 1$.*

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

$$(p^{\frac{m-1}{2}} + 1) \cdot \frac{(p+1)(p^m-1) - 4p(p^{\frac{m-1}{2}} - 1)}{2(p-1)} \equiv 2 \pmod{p^m - 1}.$$

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

$$(p^{\frac{m+1}{2}} + 1) \cdot \frac{(p-3)(p^m-1) + 4(p^{\frac{m+1}{2}} - 1)}{2(p-1)} \equiv 2 \pmod{p^m - 1}.$$

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

$$\frac{(p+1)(p^m-1) - 4p(p^{\frac{m-1}{2}} - 1)}{2(p-1)} \equiv 1 + \frac{(p-1)}{2} \pmod{p-1}$$

and

$$\frac{(p-3)(p^m-1) + 4p(p^{\frac{m+1}{2}} - 1)}{2(p-1)} \equiv 1 + \frac{(p-1)}{2} \pmod{p-1}.$$

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). □

3 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 $\gcd(m,k) = 1$. 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

$$\Big\{T(a,b) = \sum_{x \in \mathbb{F}_q} \omega^{\mathrm{Tr}(ax+bx^e)} | a,\, b \in \mathbb{F}_q\Big\} \tag{2}$$

and

$$\Big\{S(a,b,c) = \sum_{x \in \mathbb{F}_q} \omega^{\mathrm{Tr}(ax+bx^e+cx^s)} | a,\, b \in \mathbb{F}_q, c \in \mathbb{F}'_p\Big\}, \tag{3}$$

where $s = (q-1)/2$, $\mathbb{F}'_p$ is composed of p elements in $\mathbb{F}_q$ such that $\{\mathrm{Tr}(c) | c \in \mathbb{F}'_p\} = \mathbb{F}_p$ (It is clear that $\mathbb{F}'_p = \mathbb{F}_p$ if $\mathrm{Tr}(1) \neq 0$). The value distribution of $S(a,b,c)$ will be utilized to investigate the weight distribution of the cyclic codes $\mathcal{C}_{(1,e,s)}$ in Section 4.

Define

$$T_0(a,b) = \sum_{x \in \mathbb{F}_q} \omega^{\mathrm{Tr}(ax^{p^k+1}+bx^2)}. \tag{4}$$

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^{p^k+1} runs twice through the squares in $\mathbb{F}_q^*$ and $-x^{p^k+1}$ 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

$$T(a,b) = \frac{1}{2}\big(T_0(a,b) + T_0(-a,(-1)^e b)\big), \tag{5}$$

and

$$\begin{aligned} S(a,b,c) =& 1 - \frac{1}{2}\big(\omega^t + \omega^{-t}\big) \\ &+ \frac{1}{2}\big(\omega^t T_0(a,b) + \omega^{-t} T_0(-a,(-1)^e b)\big), \end{aligned} \tag{6}$$

Table 4: *The value distribution of $T_0(a,b)$ for odd $m \geq 3$*

Values	Multiplicity (each)
$\pm\sqrt{p^*}p^{\frac{m-1}{2}}$	$p^2(p^m-1)(p^m-p^{m-1}-p^{m-2}+1)/(2(p^2-1))$
$\pm p^{\frac{m+1}{2}}$	$(p^m-1)(p^{m-1}\pm p^{\frac{m-1}{2}})/2$
$\pm\sqrt{p^*}p^{\frac{m+1}{2}}$	$(p^m-1)(p^{m-1}-1)/(2(p^2-1))$
p^m	1

where $t = \mathrm{Tr}(c)$.

The value distribution of the exponential sum $T_0(a,b)$ for odd $m \geq 3$ is given in Table 4 [13]. In order to determine the value distribution of $T(a,b)$ and $S(a,b,c)$, we shall study the distribution of

$$\big(T_0(a,b), T_0(-a,(-1)^e b)\big)$$

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 $\big(T_0(a,b), T_0(-a,-b)\big)$ can be readily settled from Table 4. When e is an even integer, the calculation of the distribution of $\big(T_0(a,b), T_0(-a,b)\big)$ is not trivial and we will focus on it in the sequel.

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

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*

$$\sum_{x\in\mathbb{F}_q} \omega^{Q(x)} = \begin{cases} \left(\frac{\Delta}{p}\right)p^{m-r/2}, & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{r/2}\left(\frac{\Delta}{p}\right)p^{m-r/2}, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where Δ is the determinant of $Q(x)$. Furthermore, for any $y \in \mathbb{F}_p^*$,

$$\sum_{x\in\mathbb{F}_q} \omega^{yQ(x)} = \left(\frac{y^r}{p}\right) \sum_{x\in\mathbb{F}_q} \omega^{Q(x)}. \tag{7}$$

Lemma 5. *([13]) Let m and k be positive integers such that $\gcd(m,k) = 1$. Let*

$$Q_{a,b}(x) = \mathrm{Tr}(ax^{p^k+1} + bx^2)$$

be a quadratic form in m variables over $\mathbb{F}_p$. Then, (i) for $(a,b) \in \mathbb{F}_{p^m}^2 \setminus \{(0,0)\}$, 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

$$\nu_i = \begin{cases} p^{\frac{m+i}{2}}, & \text{if } i \text{ is odd,} \\ \sqrt{p^*}\, p^{\frac{m+i-1}{2}}, & \text{if } i \text{ is even,} \end{cases} \tag{8}$$

where $p^* = (-1)^{\frac{p-1}{2}} p$. By Lemmas 4 and 5, for any $(a,b) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$,

$$\big(T_0(a,b), T_0(-a,b)\big) \in \big\{(\varepsilon_1 \nu_{i_1}, \varepsilon_2 \nu_{i_2}) \,|\, 0 \le i_1, i_2 \le 2, \varepsilon_1, \varepsilon_2 = \pm 1\big\}.$$

Before further studying the value distribution of $\big(T_0(a,b), T_0(-a,b)\big)$, we define

$$\begin{aligned} N_{\varepsilon,i}^+ &= \Big\{(a,b) \in \mathbb{F}_q^2 \,|\, T_0(a,b) = \varepsilon \nu_i\Big\}, \\ N_{\varepsilon,i}^- &= \Big\{(a,b) \in \mathbb{F}_q^2 \,|\, T_0(-a,b) = \varepsilon \nu_i\Big\}, \end{aligned} \tag{9}$$

where $\varepsilon \in \{1, -1\}$. Some properties of $N_{\varepsilon,i}^+$ and $N_{\varepsilon,i}^-$ are summarized in the following lemma.

Lemma 6. *Let λ be a non-square of $\mathbb{F}_p^*$. For $\varepsilon \in \{1,-1\}$ and $i \in \{0,1,2\}$, we have*

(i) $(a,b) \in N_{\varepsilon,i}^+$ *if and only if* $(-a,b) \in N_{\varepsilon,i}^-$;

(ii) $\lambda N_{\varepsilon,0}^+ = N_{-\varepsilon,0}^+$, $\lambda N_{\varepsilon,0}^- = N_{-\varepsilon,0}^-$;

(iii) $\lambda N_{\varepsilon,1}^+ = N_{\varepsilon,1}^+$, $\lambda N_{\varepsilon,1}^- = N_{\varepsilon,1}^-$; *and*

(iv) $\lambda N_{\varepsilon,2}^+ = N_{-\varepsilon,2}^+$, $\lambda N_{\varepsilon,2}^- = N_{-\varepsilon,2}^-$.

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

By Lemma 4, for any non-square λ of $\mathbb{F}_p^*$,

$$T_0(\lambda a, \lambda b) = \sum_{x \in \mathbb{F}_q} \omega^{\lambda \mathrm{Tr}(a x^{p^k+1} + b x^2)} = \Big(\frac{\lambda^r}{p}\Big) T_0(a,b), \tag{10}$$

where r is the rank of the quadratic form $Q_{a,b}(x) = \mathrm{Tr}(a x^{p^k+1} + b x^2)$. Following from the definitions of ν_i and $N_{\varepsilon,i}^+$, we know that if $(a,b) \in$

$N^+_{\varepsilon,i}$, 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 $(a,b) \in N^+_{\varepsilon,1}$ and $T_0(\lambda a, \lambda b) = -T_0(a,b)$ if $(a,b) \in N^+_{\varepsilon,0}$ or $(a,b) \in N^+_{\varepsilon,2}$. Therefore, we deduce that

$$\lambda N^+_{\varepsilon,0} = N^+_{-\varepsilon,0}, \ \ \lambda N^+_{\varepsilon,1} = N^+_{\varepsilon,1}, \ \ \lambda N^+_{\varepsilon,2} = N^+_{-\varepsilon,2}.$$

Then the properties for $N^-_{\varepsilon,i}$ in (ii), (iii) and (iv) directly follow from (i). □

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

Proposition 1. *Let $\mathcal{N}_4$ denote the number of tuples $(x,y,z,w) \in \mathbb{F}_q^4$ satisfying*

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = 0 \\ x^{p^k+1} + y^{p^k+1} + z^{p^k+1} - w^{p^k+1} = 0. \end{cases}$$

Then for odd $m \geq 3$ and positive integer k with $\gcd(m,k) = 1$,

$$\mathcal{N}_4 = 2q^2 - qp - q + p.$$

Proof. See the Appendix. □

Proposition 2. *For odd $m \geq 3$ and positive integer k with $\gcd(m,k) = 1$,*

(i) $\sum\limits_{a,b \in \mathbb{F}_q} T_0(a,b) \cdot T_0(-a,b) = q^2;$

(ii) $\sum\limits_{a,b \in \mathbb{F}_q} T_0^3(a,b) \cdot T_0(-a,b) = q^2 \cdot (2q^2 - qp - q + p).$

Proof. (i) By the definition of $T_0(a,b)$ in (4), one has

$$\begin{aligned} &\sum_{a,\,b \in \mathbb{F}_q} T_0(a,b) \cdot T_0(-a,b) \\ &= \sum_{a,\,b \in \mathbb{F}_q} \sum_{x,\,y \in \mathbb{F}_q} \omega^{\mathrm{Tr}\left(a(x^{p^k+1} - y^{p^k+1}) + b(x^2+y^2)\right)} \\ &= \sum_{x,\,y \in \mathbb{F}_q} \sum_{a \in \mathbb{F}_q} \omega^{\mathrm{Tr}(a(x^{p^k+1} - y^{p^k+1}))} \sum_{b \in \mathbb{F}_q} \omega^{\mathrm{Tr}(b(x^2+y^2))} \\ &= q^2 \mathcal{N}_2, \end{aligned}$$

where $\mathcal{N}_2$ is the number of the solutions of the following system of equations:

$$\begin{cases} x^2 + y^2 = 0 \\ x^{p^k+1} - y^{p^k+1} = 0. \end{cases}$$

Since $x^{p^k+1} = y^{p^k+1}$ 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 $\mathcal{N}_2 = 1$.

(ii) In a similar manner, we deduce that

$$\begin{aligned} &\sum_{a,b\in\mathbb{F}_q} T_0^3(a,b)\cdot T_0(-a,b) \\ &= \sum_{x,y,z,w\in\mathbb{F}_q} \sum_{a\in\mathbb{F}_q} \omega^{\mathrm{Tr}(a(x^{p^k+1}+y^{p^k+1}+z^{p^k+1}-w^{p^k+1}))} \\ &\qquad * \sum_{b\in\mathbb{F}_q} \omega^{\mathrm{Tr}(b(x^2+y^2+z^2+w^2))} \\ &= q^2\mathcal{N}_4, \end{aligned}$$

where $\mathcal{N}_4$ is the number of the solutions of the following system of equations:

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = 0 \\ x^{p^k+1} + y^{p^k+1} + z^{p^k+1} - w^{p^k+1} = 0. \end{cases}$$

The conclusion immediately follows from Proposition 1. □

With the preparations of Table 4, Lemmas 5, 6 and Proposition 2, we are now ready to determine the distribution of $\big(T_0(a,b), T_0(-a,b)\big)$.

Theorem 2. *Let v_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*

$$\Big\{ \big(T_0(a,b), T_0(-a,b)\big) | a, b \in \mathbb{F}_q \Big\}$$

is shown in Table 5.

Proof. By the definitions of $N^+_{\varepsilon,i}$ and $N^-_{\varepsilon,i}$ in (9), for $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$ and $i_1, i_2 \in \{0, 1, 2\}$,

$$N^+_{\varepsilon_1,i_1} \cap N^-_{\varepsilon_2,i_2} = \Big\{ (a,b) \in \mathbb{F}_q^2 \,|\, \big(T_0(a,b), T_0(-a,b)\big) = (\varepsilon_1 v_{i_1}, \varepsilon_2 v_{i_2}) \Big\}.$$

Table 5: *The value distribution of* $\big(T_0(a,b), T_0(-a,b)\big)$ *for odd* $m \geq 3$

Values	Multiplicity (each)
(ν_0, ν_0), $(-\nu_0, -\nu_0)$	$(p^m-1)(p^{m+1}-3p^m+p+1)/(4(p-1))$
$(\nu_0, -\nu_0)$, $(-\nu_0, \nu_0)$	$(p-1)(p^{2m}-1)/(4(p+1))$
(ν_0, ν_1), (ν_1, ν_0) $(-\nu_0, \nu_1)$, $(\nu_1, -\nu_0)$	$(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})/4$
$(\nu_0, -\nu_1)$, $(-\nu_1, \nu_0)$ $(-\nu_0, -\nu_1)$, $(-\nu_1, -\nu_0)$	$(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})/4$
(ν_0, ν_2), (ν_2, ν_0) $(-\nu_0, -\nu_2)$, $(-\nu_2, -\nu_0)$	$(p^m-1)(p^{m-1}-1)/(2(p^2-1))$
$(\nu_0, -\nu_2)$, $(-\nu_2, \nu_0)$ $(-\nu_0, \nu_2)$, $(\nu_2, -\nu_0)$	0
(p^m, p^m)	1

Then one needs to calculate the cardinality of $N^+_{\varepsilon_1,i_1} \cap N^-_{\varepsilon_2,i_2}$.

It follows from Lemma 5 (ii) that for any $i_1, i_2 \in \{0,1,2\}$ with $i_1 \cdot i_2 \neq 0$, $N^+_{\varepsilon_1,i_1} \cap N^-_{\varepsilon_2,i_2} = \emptyset$. 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 6 (i), for any $\varepsilon_1, \varepsilon_2 \in \{1,-1\}$ and $i_1, i_2 \in \{0,1,2\}$, $(a,b) \in N^+_{\varepsilon_1,i_1} \cap N^-_{\varepsilon_2,i_2}$ if and only if $(-a,b) \in N^-_{\varepsilon_1,i_1} \cap N^+_{\varepsilon_2,i_2}$. Thus,

$$|N^+_{\varepsilon_1,i_1} \cap N^-_{\varepsilon_2,i_2}| = |N^+_{\varepsilon_2,i_2} \cap N^-_{\varepsilon_1,i_1}|. \tag{11}$$

Hence we in the sequel only need to calculate $|N^+_{\varepsilon_1,i_1} \cap N^-_{\varepsilon_2,i_2}|$ for $i_1 = 0$ and $i_2 \in \{0,1,2\}$. The cardinality of $N^+_{\varepsilon_1,i_1} \cap N^-_{\varepsilon_2,i_2}$ for $i_1 \in \{0,1,2\}$ and $i_2 = 0$ will be directly obtained.

Let λ be a non-square of $\mathbb{F}_p^*$. Due to Lemma 6 (ii), we get

$$\lambda(N^+_{1,0} \cap N^-_{1,0}) = N^+_{-1,0} \cap N^-_{-1,0},\ \lambda(N^+_{-1,0} \cap N^-_{1,0}) = N^+_{1,0} \cap N^-_{-1,0},$$

which implies

$$|N^+_{1,0} \cap N^-_{1,0}| = |N^+_{-1,0} \cap N^-_{-1,0}|,\ |N^+_{-1,0} \cap N^-_{1,0}| = |N^+_{1,0} \cap N^-_{-1,0}|. \tag{12}$$

Similarly, Lemma 6 (iv) gives

$$|N^+_{1,0} \cap N^-_{1,2}| = |N^+_{-1,0} \cap N^-_{-1,2}|,\ |N^+_{-1,0} \cap N^-_{1,2}| = |N^+_{1,0} \cap N^-_{-1,2}|. \tag{13}$$

By Lemma 6 (iii), we can deduce that

$$|N^+_{1,0} \cap N^-_{1,1}| = |N^+_{-1,0} \cap N^-_{1,1}|,\ |N^+_{-1,0} \cap N^-_{-1,1}| = |N^+_{1,0} \cap N^-_{-1,1}|. \tag{14}$$

For the ease of notations, for $i \in \{0,2\}$, denote

$$s_i = |N^+_{1,0} \cap N^-_{1,i}|,\ \bar{s}_i = |N^+_{-1,0} \cap N^-_{1,i}| \tag{15}$$

and let

$$s_1 = |N^+_{1,0} \cap N^-_{1,1}|,\ \bar{s}_1 = |N^+_{-1,0} \cap N^-_{-1,1}|. \tag{16}$$

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 5. Thus our next task is to determine these quantities.

By Lemma 6 (i), the cardinalities of $N^+_{\varepsilon,i}$ and $N^-_{\varepsilon,i}$ are the same and they are listed in Table 4. We denote $n_{\varepsilon,i} = |N^+_{\varepsilon,i}| = |N^-_{\varepsilon,i}|$. By Lemma

5 (ii), for any $(a,b) \in \mathbb{F}_q \setminus \{(0,0)\}$, only when the quadratic form $Q_{a,b}(x) = ax^{p^k+1} + bx^2$ has rank m, the quadratic form $Q_{-a,b}(x)$ could have rank $m-2$, $m-1$. This is equivalent to saying that

$$N^-_{\varepsilon,i} \subseteq (N^+_{1,0} \cup N^+_{-1,0})$$

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

$$|N^+_{1,0} \cap N^-_{\varepsilon,i}| + |N^+_{-1,0} \cap N^-_{\varepsilon,i}| = |N^-_{\varepsilon,i}| = n_{\varepsilon,i}.$$

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

$$\begin{cases} s_0 + \bar{s}_0 + s_1 + \bar{s_1} + s_2 + \bar{s_2} = n_{1,0} \\ s_1 + s_1 = n_{1,1} \\ \bar{s}_1 + \bar{s}_1 = n_{-1,1} \\ s_2 + \bar{s}_2 = n_{1,2}. \end{cases} \tag{17}$$

Furthermore, by the correspondences between the first six items of multiplicities in Table 5 and the quantities $s_0, \bar{s}_0, s_1, \bar{s}_1, s_2, \bar{s}_2$, it is easy to verify that

$$\sum_{a,b\in\mathbb{F}_q} T_0(a,b)T_0(-a,b) = p^{2m} + 2(s_0 - \bar{s}_0)\nu_0^2 + 4(s_2 - \bar{s}_2)\nu_0\nu_2$$

and

$$\begin{aligned} &\sum_{a,b\in\mathbb{F}_q} T_0^3(a,b)T_0(-a,b) \\ &= \quad q^4 + 2(s_0 - \bar{s}_0)\nu_0^4 + 2(s_2 - \bar{s}_2)(\nu_0^3\nu_2 + \nu_0\nu_2^3). \end{aligned}$$

Then Proposition 2 gives two more equations

$$\begin{cases} 2(s_0 - \bar{s}_0)\nu_0^2 + 4(s_2 - \bar{s}_2)\nu_0\nu_2 = 0 \\ 2(s_0 - \bar{s}_0)\nu_0^4 + 2(s_2 - \bar{s}_2)(\nu_0^3\nu_2 + \nu_0\nu_2^3) = q^2(q-1)(q-p). \end{cases} \tag{18}$$

Therefore, one can deduce the values of $s_0, \bar{s}_0, s_1, \bar{s}_1, s_2, \bar{s}_2$ by solving (17) and (18). Then the distribution of $\big(T_0(a,b), T_0(-a,b)\big)$ is determined and listed in Table 5. □

By (4)-(6), Tables 4 and 5, we have the following two theorems.

Table 6: *The value distribution of* $\{T(a,b) \mid a,b \in \mathbb{F}_q\}$ *for odd* e

Values	Multiplicity
0	$(p^m-1)(p^m-p^{m-1}+1)$
$p^{\frac{m+1}{2}}$	$(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})/2$
$-p^{\frac{m+1}{2}}$	$(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})/2$
p^m	1

Table 7: *The value distribution of* $\{T(a,b) \mid a,b \in \mathbb{F}_q\}$ *for even* e

Values	Multiplicity (each)
0	$(p-1)(p^{2m}-1)/(2(p+1))$
$\pm\sqrt{p^*}p^{\frac{m-1}{2}}$	$(p^m-1)(p^{m+1}-3p^m+p+1)/(4(p-1))$
$\frac{1}{2}(\pm\sqrt{p^*}+p)p^{\frac{m-1}{2}}$	$(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})/2$
$\frac{1}{2}(\pm\sqrt{p^*}-p)p^{\frac{m-1}{2}}$	$(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})/2$
$\pm\frac{1}{2}(1+p)\sqrt{p^*}p^{\frac{m-1}{2}}$	$(p^m-1)(p^{m-1}-1)/(p^2-1)$
p^m	1

Table 8: *The value distribution of* $\{S(a,b,c) \mid a,b \in \mathbb{F}_q, c \in \mathbb{F}_p'\}$ *for odd* e

Values	Multiplicity (each)
$1-\frac{1}{2}(\omega^t+\omega^{-t})\pm\frac{1}{2}(\omega^t-\omega^{-t})\sqrt{p^*}p^{\frac{m-1}{2}}$	$\frac{p^2(p^m-1)(p^m-p^{m-1}-p^{m-2}+1)}{2(p^2-1)}$
$1-\frac{1}{2}(\omega^t+\omega^{-t})\pm\frac{1}{2}(\omega^t+\omega^{-t})p^{\frac{m+1}{2}}$	$\frac{(p^m-1)(p^{m-1}\pm p^{\frac{m-1}{2}})}{2}$
$1-\frac{1}{2}(\omega^t+\omega^{-t})\pm\frac{1}{2}(\omega^t-\omega^{-t})\sqrt{p^*}p^{\frac{m+1}{2}}$	$\frac{(p^m-1)(p^{m-1}-1)}{2(p^2-1)}$
$1+\frac{1}{2}(p^m-1)(\omega^t+\omega^{-t})$	1

where $t = 0, 1, \cdots, p-1$.

Table 9: *The value distribution of* $\{S(a,b,c) \mid a,b \in \mathbb{F}_q, c \in \mathbb{F}_p'\}$ *for even* e

Values	Multiplicity (each)
$1-\frac{1}{2}(\omega^t+\omega^{-t})\pm\frac{1}{2}(\omega^t+\omega^{-t})\sqrt{p^*}p^{\frac{m-1}{2}}$	$\frac{(p^m-1)(p^{m+1}-3p^m+p+1)}{4(p-1)}$
$1-\frac{1}{2}(\omega^t+\omega^{-t})\pm\frac{1}{2}(\omega^t-\omega^{-t})\sqrt{p^*}p^{\frac{m-1}{2}}$	$\frac{(p-1)(p^{2m}-1)}{4(p+1)}$
$1-\frac{1}{2}(\omega^t+\omega^{-t})+\frac{1}{2}(\pm\omega^t\sqrt{p^*}+\omega^{-t}p)p^{\frac{m-1}{2}}$	$\frac{(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})}{2}$
$1-\frac{1}{2}(\omega^t+\omega^{-t})+\frac{1}{2}(\pm\omega^t\sqrt{p^*}-\omega^{-t}p)p^{\frac{m-1}{2}}$	$\frac{(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})}{2}$
$1-\frac{1}{2}(\omega^t+\omega^{-t})\pm\frac{1}{2}(\omega^t+\omega^{-t}p)\sqrt{p^*}p^{\frac{m-1}{2}}$	$\frac{(p^m-1)(p^{m-1}-1)}{p^2-1}$
$1+\frac{1}{2}(p^m-1)(\omega^t+\omega^{-t})$	1

where $t=0,1,\cdots,p-1$.

Table 10: *Weight distribution of* $\mathcal{C}_{(1,e,s)}$ *for odd* e

Hamming weight	Multiplicity
0	1
p^m-1	$p-1$
$p^{m-1}(p-1)-p^{\frac{m-1}{2}}-1$	$\frac{(p^m-1)(p^{m+2}-p^m-p^{m-1}-p^{\frac{m+3}{2}}+p^{\frac{m-1}{2}}+p^2)}{2(p+1)}$
$p^{m-1}(p-1)+p^{\frac{m-1}{2}}-1$	$\frac{(p^m-1)(p^{m+2}-p^m-p^{m-1}+p^{\frac{m+3}{2}}-p^{\frac{m-1}{2}}+p^2)}{2(p+1)}$
$p^{m-1}(p-1)-p^{\frac{m+1}{2}}-1$	$\frac{(p^m-1)(p^{m-1}-1)}{2(p+1)}$
$p^{m-1}(p-1)+p^{\frac{m+1}{2}}-1$	$\frac{(p^m-1)(p^{m-1}-1)}{2(p+1)}$
$p^{m-1}(p-1)-(p-1)p^{\frac{m-1}{2}}$	$\frac{(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})}{2}$
$p^{m-1}(p-1)+(p-1)p^{\frac{m-1}{2}}$	$\frac{(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})}{2}$
$p^{m-1}(p-1)$	$(p^m-1)(p^m-p^{m-1}+1)$

Table 11: *Weight distribution of $\mathcal{C}_{(1,e,s)}$ for even e*

Hamming weight	Multiplicity
0	1
p^m-1	$p-1$
$p^{m-1}(p-1)-p^{\frac{m-1}{2}}-1$	$\frac{(p^m-1)(p^{m+1}+p^m+2p^{m-1}-2p^{\frac{m+1}{2}}-2p^{\frac{m-1}{2}}+p-1)(p-1)}{4(p+1)}$
$p^{m-1}(p-1)+p^{\frac{m-1}{2}}-1$	$\frac{(p^m-1)(p^{m+1}+p^m+2p^{m-1}+2p^{\frac{m+1}{2}}+2p^{\frac{m-1}{2}}+p-1)(p-1)}{4(p+1)}$
$p^{m-1}(p-1)-\frac{1}{2}(p-1)p^{\frac{m-1}{2}}-1$	$\frac{(p^m-1)(p^{m-1}-1)}{p+1}$
$p^{m-1}(p-1)+\frac{1}{2}(p-1)p^{\frac{m-1}{2}}-1$	$\frac{(p^m-1)(p^{m-1}-1)}{p+1}$
$p^{m-1}(p-1)-\frac{1}{2}(p-1)p^{\frac{m-1}{2}}$	$(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})$
$p^{m-1}(p-1)+\frac{1}{2}(p-1)p^{\frac{m-1}{2}}$	$(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})$
$p^{m-1}(p-1)-1$	$(p^m-1)(p^{m+1}-p^m-2p^{m-1}+p+1)/2$
$p^{m-1}(p-1)$	$(p^m-1)(p^m+1-2p^{m-1})$

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 $\{T(a,b)|a,b \in \mathbb{F}_q\}$ is shown in Table 6 if e is odd and in Table 7 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 $\{S(a,b,c)|a,b \in \mathbb{F}_q, c \in \mathbb{F}'_p\}$ is shown in Table 8 if e is odd and in Table 9 if e is even.*

4 Weight distribution of $\mathcal{C}_{(1,e,s)}$

In this section, for odd $m \geq 3$ and $p \equiv 3 \pmod 4$, we study the weight distribution of the cyclic codes $\mathcal{C}_{(1,e,s)}$ 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 $[p^m-1, 2m+1]$ cyclic code $\mathcal{C}_{(1,e,s)}$ is given in Table 10 if e is odd and in Table 11 if e is even.*

Proof. By (1), the Hamming weight of any nonzero codeword $\mathbf{c} = (c_0, c_1, \cdots, c_{q-2}) \in \mathcal{C}_{(1,e,s)}$ is

$$w_H(\mathbf{c}) = p^{m-1}(p-1) - \frac{1}{p}\Delta(a,b,c), \tag{19}$$

where

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

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

Let $\mathrm{Tr}(c) = t$ and $Q_{a,b}(x) = \mathrm{Tr}(ax^{p^k+1} + bx^2)$. 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

$$\begin{aligned}
&\Delta(a,b,c)\\
=&\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(2+\sum_{x\in\mathbb{F}_q^*}\omega^{y\mathrm{Tr}(ax^{p^k+1}+bx^2+c)}+\sum_{x\in\mathbb{F}_q^*}\omega^{y\mathrm{Tr}(-ax^{p^k+1}-bx^2-c)}\Big)\\
=&\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(2+\sum_{x\in\mathbb{F}_q^*}\omega^{y\mathrm{Tr}(ax^{p^k+1}+bx^2+c)}+\sum_{x\in\mathbb{F}_q^*}\omega^{y\mathrm{Tr}(ax^{p^k+1}+bx^2+c)}\Big)\\
=&\sum_{y\in\mathbb{F}_p^*}\Big(1+\sum_{x\in\mathbb{F}_q^*}\omega^{y\mathrm{Tr}(ax^{p^k+1}+bx^2+c)}\Big)\\
=&\sum_{y\in\mathbb{F}_p^*}\Big(1-\omega^{yt}+\sum_{x\in\mathbb{F}_q}\omega^{yQ_{a,b}(x)+yt}\Big)\\
=&\sum_{y\in\mathbb{F}_p^*}\Big(1-\omega^{yt}+\omega^{yt}\big(\frac{y^r}{p}\big)\sum_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}\Big),
\end{aligned}$$

where r is the rank of $Q(a,b)$ and the last equality sign comes from Lemma 4.

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

$$\Delta(a,b,c) = \sum_{y\in\mathbb{F}_p^*}\big(\frac{y^r}{p}\big)\sum_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}. \tag{20}$$

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

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

and

$$\sum_{y\in\mathbb{F}_p^*}\omega^{yt}\left(\frac{y}{p}\right)=\left(\frac{t}{p}\right)\sum_{y\in\mathbb{F}_p^*}\omega^{ty}\left(\frac{ty}{p}\right)=\left(\frac{t}{p}\right)\sqrt{p^*}.$$

Then,

$$\Delta(a,b,c)=p+\sum_{y\in\mathbb{F}_p^*}\omega^{yt}\left(\frac{y^r}{p}\right)\sum_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}. \tag{21}$$

Recall that $T_0(a,b)=\sum_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}$. According to the value distribution of $T_0(a,b)$ in Table 4, the weight distribution of $\mathcal{C}_{(1,e,s)}$ 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*,

$$\begin{aligned}
&\Delta(a,b,c)\\
=&\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(2+\sum_{x\in\mathbb{F}_q^*}\omega^{y(Q_{a,b}(x)+t)}+\sum_{x\in\mathbb{F}_q^*}\omega^{y(Q_{-a,b}(x)-t)}\Big)\\
=&\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(2-(\omega^{yt}+\omega^{-yt})\\
&+\sum_{x\in\mathbb{F}_q}\omega^{yQ_{a,b}(x)+yt}+\sum_{x\in\mathbb{F}_q}\omega^{yQ_{-a,b}(x)-yt}\Big)\\
=&\frac{1}{2}\sum_{y\in\mathbb{F}_p^*}\Big(2-(\omega^{yt}+\omega^{-yt})\\
&+\omega^{yt}\left(\frac{y^r}{p}\right)\sum_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}+\omega^{-yt}\left(\frac{y^{r'}}{p}\right)\sum_{x\in\mathbb{F}_q}\omega^{Q_{-a,b}(x)}\Big)
\end{aligned} \tag{22}$$

where r,r' are the rank of $Q(a,b)$ and $Q(-a,b)$ respectively, and the last equality sign comes from Lemma 4. It follows from Lemma 5 that (r,r') takes value from the following set

$$\big\{(m,m),(m,m-1),(m,m-2),(m-1,m),(m-2,m)\big\}. \tag{23}$$

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

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

By a similar analysis as in the case of odd e, the value distribution of $\Delta(a,b,c)$ is given in (24).

$$\Delta(a,b,c)=\begin{cases}(p-1)p^m, & \text{once}\\ \frac{1}{2}(p-1)p^{\frac{m-1}{2}}, & \text{for } (p^m-1)(p^{m-1}+p^{\frac{m-1}{2}}) \text{ times}\\ -\frac{1}{2}(p-1)p^{\frac{m-1}{2}}, & \text{for } (p^m-1)(p^{m-1}-p^{\frac{m-1}{2}}) \text{ times}\\ 0, & \text{for } (p^m-1)(p^m-2p^{m-1}+1) \text{ times.}\end{cases} \tag{24}$$

Case II: $t\neq 0$. Since $\sum\limits_{y\in\mathbb{F}_p^*}\omega^{yt}=\sum\limits_{y\in\mathbb{F}_p^*}\omega^{-yt}=-1$, one has

$$\begin{aligned}\Delta(a,b,c) &= p+\frac{1}{2}\Big(\sum_{y\in\mathbb{F}_p^*}\omega^{yt}\big(\frac{y^r}{p}\big)\sum_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}\\ &\quad+\sum_{y\in\mathbb{F}_p^*}\omega^{-yt}\big(\frac{y^{r'}}{p}\big)\sum_{x\in\mathbb{F}_q}\omega^{Q_{-a,b}(x)}\Big).\end{aligned}$$

Furthermore, the fact $\sum\limits_{y\in\mathbb{F}_p^*}\omega^{yt}\big(\frac{y}{p}\big)=\big(\frac{t}{p}\big)\sqrt{p^*}$ and the possible values of (r,r') in (23) imply (25).

$$\Delta(a,b,c)=\begin{cases}p+\frac{1}{2}\Big(\big(\frac{t}{p}\big)\sqrt{p^*}\sum\limits_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}-\sum\limits_{x\in\mathbb{F}_q}\omega^{Q_{-a,b}(x)}\Big), & \text{if } r=r+1=m\\ p+\frac{1}{2}\Big(-\sum\limits_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}-\big(\frac{t}{p}\big)\sqrt{p^*}\sum\limits_{x\in\mathbb{F}_q}\omega^{Q_{-a,b}(x)}\Big), & \text{if } r+1=r'=m\\ p+\frac{1}{2}\big(\frac{t}{p}\big)\sqrt{p^*}\Big(\sum\limits_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}-\sum\limits_{x\in\mathbb{F}_q}\omega^{Q_{-a,b}(x)}\Big), & \text{otherwise.}\end{cases} \tag{25}$$

Recall that $T_0(a,b)=\sum\limits_{x\in\mathbb{F}_q}\omega^{Q_{a,b}(x)}$. Thus, by the distribution of $\big(T_0(a,b),$ $T_0(-a,b)\big)$ in Table 5, the value distribution of $\Delta(a,b,c)$ can be calculated.

From the above analysis, we deduce the weight distribution of $\mathcal{C}_{(1,e,s)}$ for even e. □

Theorem 5 settles the weight distribution of $\mathcal{C}_{(1,e,s)}$ for $p\equiv 3 \pmod 4$ and integers e satisfying the *Congruence Condition*. For the special case $p=3$, it is shown in [18] that the APN monomials x^e generate the optimal cyclic codes $\mathcal{C}_{(1,e,s)}^{\perp}$ if

1) $e=\frac{3^m+1}{4}+\frac{3^m-1}{2}$ [15]; or

Table 12: *The weight distribution of $\mathcal{C}_{(1,e,s)}$ for three APN exponents e and $s = (3^m - 1)/2$*

Hamming weight	Multiplicity
$2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}} - 1$	$(3^m - 1)(2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}})$
$2 \cdot 3^{m-1} + 3^{\frac{m-1}{2}} - 1$	$(3^m - 1)(2 \cdot 3^{m-1} + 3^{\frac{m-1}{2}})$
$2 \cdot 3^{m-1} - 3^{\frac{m-1}{2}}$	$(3^m - 1)(3^{m-1} + 3^{\frac{m-1}{2}})$
$2 \cdot 3^{m-1} + 3^{\frac{m-1}{2}}$	$(3^m - 1)(3^{m-1} - 3^{\frac{m-1}{2}})$
$2 \cdot 3^{m-1} - 1$	$2(3^m - 1)(3^{m-1} + 1)$
$2 \cdot 3^{m-1}$	$(3^m - 1)(3^{m-1} + 1)$
$3^m - 1$	2
0	1

2) $e = 3^{(m+1)/2} - 1$ [15]; or

3) $e = (3^{(m+1)/4} - 1)(3^{(m+1)/2} + 1)$ 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 $\mathbb{F}_{3^n}$ with*

1) $e = \frac{3^m+1}{4} + \frac{3^m-1}{2}$; or

2) $e = 3^{(m+1)/2} - 1$; or

3) $e = (3^{(m+1)/4} - 1)(3^{(m+1)/2} + 1)$ for $m \equiv 3 \pmod 4$.

Then the weight distribution of the $[3^m - 1, 2m + 1]$ ternary cyclic code $\mathcal{C}_{(1,e,s)}$ is given as in Table 12.

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

Example 1. Let $p = 7$, $m = 3$ and $k = 2$. The integers $e = 130$ and $e = 301$ satisfy the congruence equation $50e \equiv 2 \pmod{342}$. If $e = 301$, then $\mathcal{C}_{(1,e,s)}$ is a $[342, 7, 244]$ cyclic code with the weight enumerator $1 + 1026x^{244} + 9576x^{252} + 344736x^{286} + 100890x^{294} + 359100x^{300} +$

$7182x^{336} + 1032x^{342}$, which agrees with Theorem 5 (i). If $e = 130$, then $\mathcal{C}_{(1,e,s)}$ 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 $\mathcal{C}_{(1,e,s)}$ 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 $\mathcal{C}^{\perp}_{(1,e,s)}$ has parameter $[26, 19, 5]$, which agrees with the result in [18].

5 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, 25] and [11], but also settles the weight distribution of new three-weight codes $\mathcal{C}_{(1,e)}$ with two zeros such as those described in Corollaries 1, 2 and 3. In many cases, the duals of these three-weight codes $\mathcal{C}_{(1,e)}$ are optimal [8, 11, 25].

Another major contribution of this paper is the settlement of the weight distributions of a class of cyclic codes $\mathcal{C}_{(1,e,s)}$ with three zeros, which is documented in Theorem 5. In many cases the duals of the codes $\mathcal{C}_{(1,e,s)}$ are also optimal [18]. Our technique in proving Theorem 5 is similar to that employed in [27].

6 The Appendix

Proof of Proposition 1:

Note that the equation $x^{p^k+1} + y^{p^k+1} + z^{p^k+1} - w^{p^k+1} = 0$ is equivalent to $x^{p^{m-k}+1} + y^{p^{m-k}+1} + z^{p^{m-k}+1} - w^{p^{m-k}+1} = 0$. Since m is odd, we may assume k is even in the sequel (otherwise replace k by $m - k$).

For any $(\alpha, \beta) \in \mathbb{F}_{p^m}^2$, let $N(\alpha, \beta)$ denote the number of solutions of the following system of equations

$$\begin{cases} x^2 + y^2 = \alpha \\ x^{p^k+1} + y^{p^k+1} = \beta \\ z^2 + w^2 = -\alpha \\ z^{p^k+1} - w^{p^k+1} = -\beta. \end{cases}$$

Then,

$$\mathcal{N}_4 = \sum_{\alpha,\beta \in \mathbb{F}_{p^m}} N(\alpha, \beta). \tag{26}$$

Given $(\alpha, \beta) \in \mathbb{F}_{p^m}^2$, we will study the following systems of equations:

$$\begin{cases} x^2 + y^2 = \alpha \\ x^{p^k+1} + y^{p^k+1} = \beta \end{cases} \tag{27}$$

and

$$\begin{cases} z^2 + w^2 = -\alpha \\ z^{p^k+1} - w^{p^k+1} = -\beta. \end{cases} \tag{28}$$

Denote by $N_1(\alpha, \beta)$ and $N_2(\alpha, \beta)$ the numbers of solutions of (27) and (28), respectively. Then $N(\alpha, \beta) = N_1(\alpha, \beta) * N_2(\alpha, \beta)$ for any $(\alpha, \beta) \in \mathbb{F}_{p^m}^2$.

We first investigate the possible values of $N_1(\alpha, \beta)$ for $p \equiv 3 \pmod 4$. The investigation is divided into two subcases: $\alpha\beta = 0$ and $\alpha\beta \neq 0$.

Case I: $\alpha\beta = 0$. For (27), if $\alpha = 0$, then $x = y = 0$ since -1 is a non-square in $\mathbb{F}_{p^m}$. Thus (27) has a solution if and only if $\beta = 0$. If $\beta = 0$, $x^{2(p^k+1)} = y^{2(p^k+1)}$ together with $\gcd(2(p^k + 1), p^m - 1) = 2$ implies $x^2 = y^2$, then $x = y = 0$ since $x^{p^k+1} = -y^{p^k+1}$. Thus (27) has a solution if and only if $\alpha = 0$. Therefore, (27) has only one solution for $(\alpha, \beta) = (0, 0)$ and has no solution in other cases. In addition, for $(\alpha, \beta) = (0, 0)$, (28) becomes $z^2 + w^2 = 0$ and $z^2 - w^2 = 0$. Thus it has exactly one solution $(0, 0)$ as well.

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

$$N(\alpha, \beta) = \begin{cases} 1, & \text{if } (\alpha, \beta) = (0, 0) \\ 0, & \text{otherwise.} \end{cases} \tag{29}$$

Case II: $\alpha\beta \neq 0$. We first consider the possible values of $N_1(\alpha, \beta)$.

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

$$x = \frac{1}{2}s(\theta + \theta^{-1}), \quad y = \frac{1}{2}st(\theta - \theta^{-1}), \quad \theta \in \mathbb{F}_{p^{2m}}^*. \tag{30}$$

The above representations of x, y will be utilized to analyze the solutions of (27) in $\mathbb{F}_{p^m}$.

For the first equation of (27), by applying the fact $x^{p^m} = x$ to (30), we get $s^{p^m-1}(\theta + \theta^{-1})^{p^m} = (\theta + \theta^{-1})$, which is equivalent to

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

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

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

By combining these two equations, we deduce

$$\theta^{p^m+1} = \alpha^{(p^m-1)/2}. \tag{31}$$

It follows from the second equation of (27) and (30) that

$$\begin{aligned}&\left(\tfrac{1}{2}s(\theta + \theta^{-1})\right)^{p^k+1} + \left(\tfrac{1}{2}st(\theta - \theta^{-1})\right)^{p^k+1}\\ &= \tfrac{1}{2}\alpha^{(p^k+1)/2}(\theta^{p^k-1} + \theta^{1-p^k}) = \beta.\end{aligned}$$

Thus, if we take $\tau_1 = \theta^{p^k-1}$ and $\beta_1 = 2\alpha^{-(p^k+1)/2}\beta$, then τ_1, τ_1^{-1} are the two solutions of the following equation

$$\tau^2 - \beta_1\tau + 1 = 0. \tag{32}$$

By (31) and (32), we have

$$\theta^{p^m+1} = \alpha^{(p^m-1)/2}, \quad \theta^{p^k-1} = \tau_1 \tag{33}$$

and

$$\theta^{p^m+1} = \alpha^{(p^m-1)/2}, \quad \theta^{p^k-1} = \tau_1^{-1}. \tag{34}$$

If $\beta_1 = 2$, then $\tau_1 = \tau_1^{-1} = \theta^{p^k-1} = 1$ and (34) is the same as (33). Note that $\gcd(2(p^m+1), p^k-1) = 2(p+1)$ when k is even and $\gcd(m, k) = 1$. Then $\theta^{2(p^m+1)} = \alpha^{(p^m-1)} = 1$ together with $\theta^{p^k-1} = 1$

gives $\theta^{2(p+1)} = 1$. Furthermore, since m is odd and $\alpha^{(p^m-1)/2} = \pm 1$, one gets $\theta^{p+1} = \alpha^{(p^m-1)/2}$, which indicates that (33) has exactly $p+1$ solutions in $\mathbb{F}_{p^{2m}}$.

If $\beta_1 = -2$, then $\tau_1 = \tau_1^{-1} = \theta^{p^k-1} = -1$ and (34) is the same as (33). The fact $\theta^{2(p^m+1)} = \theta^{2(p^k-1)} = 1$ suggests $\theta^{\gcd(2(p^m+1),2(p^k-1))} = \theta^{2(p+1)} = 1$, which is in contradiction with $\theta^{p^k-1} = -1$ since $2(p+1)|(p^k-1)$. Thus, (33) has no solution in this case.

If $\beta_1 \neq \pm 2$, then $\tau_1 \neq \tau_1^{-1}$. It is readily seen that θ is a solution of (33) if and only if θ^{-1} is a solution of (34). Suppose θ_1 and θ_2 are two solutions of (33). Then $(\theta_1/\theta_2)^{p^m+1} = (\theta_1/\theta_2)^{p^k-1} = 1$, and this implies $(\theta_1/\theta_2)^{p+1} = 1$ since $\gcd(p^m+1, p^k-1) = p+1$. As a result, if (33) has a solution θ, all solutions of (33) can be represented as $\mu\theta$, and all solutions of (34) can be represented as $\mu\theta^{-1}$, where $\mu \in \mathbb{F}_{p^{2m}}$ and $\mu^{p+1} = 1$. Therefore for (33) and (34), either each of them has exactly $p+1$ solutions or none of them has a solution.

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

$$N_1(\alpha,\beta) = \begin{cases} p+1, & \text{if } \beta = \alpha^{(p^k+1)/2}, \\ 0, & \text{if } \beta = -\alpha^{(p^k+1)/2}, \\ 0 \text{ or } 2(p+1), & \text{otherwise.} \end{cases} \tag{35}$$

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 $s, t \in \mathbb{F}_{p^{2m}}^*$ with $s^2 = \alpha$ and $t^2 = -1$. Thus all solutions of $z^2 + w^2 = -\alpha$ can be represented as

$$z = \frac{1}{2}st(\vartheta + \vartheta^{-1}), \quad w = \frac{1}{2}s(\vartheta - \vartheta^{-1}), \quad \vartheta \in \mathbb{F}_{p^{2m}}^*. \tag{36}$$

For the first equation of (28), the facts $z^{p^m} = z$ and $w^{p^m} = w$ imply

$$\vartheta^{p^m+1} = -\alpha^{(p^m-1)/2}, \tag{37}$$

and the second equation of (28) together with (36) yields

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

Assume $\tau_2 = \vartheta^{p^k+1}$ and $\beta_1 = 2\alpha^{-(p^k+1)/2}\beta$. Then τ_2, τ_2^{-1} are the two solutions of

$$\tau^2 - \beta_1\tau + 1 = 0. \tag{38}$$

This equation is the same as Equation (32). Thus $\tau_2 \in \{\tau_1, \tau_1^{-1}\}$.

By (37) and (38), we get the following equations:

$$\vartheta^{p^m+1} = -\alpha^{(p^m-1)/2}, \quad \vartheta^{p^k+1} = \tau_2 \tag{39}$$

and

$$\vartheta^{p^m+1} = -\alpha^{(p^m-1)/2}, \quad \vartheta^{p^k+1} = \tau_2^{-1}. \tag{40}$$

If $\beta_1 = 2$, then $\tau_2 = \tau_2^{-1} = \vartheta^{p^k+1} = 1$ and (40) is the same as (39). Since $\gcd(2(p^m+1), p^k+1) = 2$, one deduces $\vartheta^2 = 1$. Therefore, (39) has exactly 2 solutions $\vartheta = \pm 1$ if α is a non-square and has no solution otherwise.

If $\beta_1 = -2$, then $\tau_2 = \tau_2^{-1} = \vartheta^{p^k+1} = -1$ and (40) is the same as (39). The fact $\gcd(2(p^m+1), 2(p^k+1)) = 4$ suggests $\vartheta^4 = 1$, and then $\vartheta^2 = -1$. Thus, (39) has exactly 2 solutions $\vartheta = \pm t$ if α is a non-square, where $t^2 = -1$, and has no solution otherwise.

If $\beta_1 \neq \pm 2$, then $\tau_2 \neq \tau_2^{-1}$. Note that ϑ is a solution of (39) if and only if ϑ^{-1} is a solution of (40). Suppose ϑ_1 and ϑ_2 are two solutions of (39). Then $(\vartheta_1/\vartheta_2)^{p^m+1} = (\vartheta_1/\vartheta_2)^{p^k+1} = 1$, and this implies $(\vartheta_1/\vartheta_2)^2 = 1$. Consequently, for (39) and (40), either they respectively have solutions $\pm\vartheta$ and $\pm\vartheta^{-1}$, or none of them has a solution.

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

$$N_2(\alpha,\beta) = \begin{cases} 2, & \text{if } \beta = \pm\alpha^{(p^k+1)/2},\ \alpha \in NQR, \\ 0, & \text{if } \beta = \pm\alpha^{(p^k+1)/2},\ \alpha \in QR, \\ 0 \text{ or } 4, & \text{otherwise}, \end{cases} \tag{41}$$

where and whereafter QR (resp. NQR) is the set consisting of all squares (resp. nonsquares) in $\mathbb{F}_{p^m}^*$.

By (35) and (41), for $\alpha \in \mathbb{F}_{p^m}^*$ and $\beta \in \{\alpha^{(p^k+1)/2}, -\alpha^{(p^k+1)/2}\}$,

$$N(\alpha,\beta) = \begin{cases} 2(p+1), & \text{if } \alpha \in NQR,\ \beta = \alpha^{(p^k+1)/2}, \\ 0, & \text{otherwise}. \end{cases} \tag{42}$$

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 (33), (34), (39) and (40) and gather them together as below

$$\begin{cases} \theta^{p^m+1} = \alpha^{(p^m-1)/2}, & \theta^{(p^k-1)} = \tau_1, \text{ or } \tau_1^{-1}, \\ \vartheta^{p^m+1} = -\alpha^{(p^m-1)/2}, & \vartheta^{(p^k+1)} = \tau_1, \text{ or } \tau_1^{-1} \end{cases} \tag{43}$$

since $\tau_2 \in \{\tau_1, \tau_1^{-1}\}$. For a fixed $\alpha \in \mathbb{F}_{p^m}^*$, let $\mathbb{T} = \mathbb{F}_{p^m}^* \setminus \{\pm\alpha^{(p^k+1)/2}\}$ and define

$$\begin{aligned} \mathbb{S}_1(\alpha) &= \Big\{\beta \in \mathbb{T} \mid \text{(33), (34) have } p+1 \text{ solutions}\Big\}, \\ \mathbb{S}_2(\alpha) &= \Big\{\beta \in \mathbb{T} \mid \text{(39), (40) have 2 solutions}\Big\}. \end{aligned} \tag{44}$$

Then (35) and (41) suggest that $N(\alpha, \beta) = 8(p+1)$ if $\beta \in \mathbb{S}_1(\alpha) \cap \mathbb{S}_2(\alpha)$ and $N(\alpha, \beta) = 0$ otherwise. In what follows, we shall show that if α is a square, then $\mathbb{S}_1(\alpha) \cap \mathbb{S}_2(\alpha) = \emptyset$; and if α is a non-square, then $\mathbb{S}_1(\alpha) \subseteq \mathbb{S}_2(\alpha)$.

When α is a square, i.e., $\alpha^{(p^m-1)/2} = 1$, the equations in the first row of (43) yield

$$\tau_1^{(p^m+1)/2} = (\theta^{\pm(p^k-1)})^{(p^m+1)/2} = (\theta^{p^m+1})^{\pm(p^k-1)/2} = 1,$$

while the equations in the second row of (43) imply

$$\begin{aligned} \tau_1^{(p^m+1)/2} &= (\vartheta^{\pm(p^k+1)})^{(p^m+1)/2} = (\vartheta^{p^m+1})^{\pm(p^k+1)/2} \\ &= (-1)^{\pm(p^k+1)/2} = -1. \end{aligned}$$

This is a contradiction. Thus, there do not exist $\theta, \vartheta \in \mathbb{F}_{p^{2m}}^*$ satisfying (43), which is equivalent to $\mathbb{S}_1(\alpha) \cap \mathbb{S}_2(\alpha) = \emptyset$.

When α is a non-square, i.e., $\alpha^{(p^m-1)/2} = -1$, one has $\theta^{p^m+1} = -1$ and $\vartheta^{p^m+1} = 1$. Let ξ be a primitive element of $\mathbb{F}_{p^{2m}}$. Then θ and ϑ can be respectively represented as $\theta = \xi^{(2i+1)(p^m-1)/2}$ and $\vartheta = \xi^{j(p^m-1)}$, where $i, j = 0, 1, \cdots, p^m$. Assume $\tau_1 = \xi^r$, then the equation $\theta^{p^k-1} = \tau_1$ is equivalent to $(2i+1)(p^m-1)(p^k-1)/2 \equiv r \pmod{p^{2m}-1}$. For any $\beta \in \mathbb{S}_1(\alpha)$, by the definition of $\mathbb{S}_1(\alpha)$, this linear congruence equation with variable i has $p+1$ solutions. Thus, $\gcd((p^m-1)(p^k-1)/2, p^{2m}-1) | r$. Since $\gcd(p^k+1, p^m+1) = 2$ and $\gcd((p^k-1)/2, p^m+1) = (p+1)$, one has

$$\gcd((p^m-1)(p^k+1), p^{2m}-1) | r.$$

This implies the congruence equation $j(p^m-1)(p^k+1) \equiv r \pmod{p^{2m}-1}$ with variable j has solutions. Thus, the equations $\vartheta^{p^m+1} = 1$ and $\vartheta^{p^k+1} = \tau_1, \tau^{-1}$ have 4 solutions. This implies that β is also contained in $\mathbb{S}_2(\alpha)$. Then $\mathbb{S}_1(\alpha)$ is a subset of $\mathbb{S}_2(\alpha)$.

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

$$N(\alpha,\beta) = \begin{cases} 8(p+1), & \text{if } \alpha \text{ is a non-square, } \beta \in \mathrm{S}_1(\alpha), \\ 0, & \text{otherwise.} \end{cases} \tag{45}$$

Combining (26), (29), (42) and (45) gives

$$\mathcal{N}_4 = 1 + ((p+1) + 4(p+1)|\mathrm{S}_1(\alpha)|)(p^m-1).$$

Thus, to determine the value of $\mathcal{N}_4$, we only need to calculate the cardinality of the set $\mathrm{S}_1(\alpha)$. Given $\alpha \in \mathbb{F}_{p^m}^*$, by [19, 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 (35), if $\beta = \alpha^{(p^k+1)/2}$, there are exactly $p+1$ solutions satisfying $x^{p^k+1}+y^{p^k+1}=\beta$, and for any $\beta \in \mathrm{S}_1(\alpha)$, there are exactly $2(p+1)$ solutions satisfying $x^{p^k+1}+y^{p^k+1}=\beta$. Thus, $(p+1)+2(p+1)|\mathrm{S}_1(\alpha)| = p^m+1$, which implies $|\mathrm{S}_1(\alpha)| = (p^m-p)/2(p+1)$.

Therefore, for $p \equiv 3 \pmod 4$

$$\mathcal{N}_4 = 1 + ((p+1) + 2(p^m-p))(p^m-1) = 2p^{2m} - p^{m+1} - p^m + p.$$

The analysis on the value of $\mathcal{N}_4$ for $p \equiv 1 \pmod 4$ is similar in spirit to that for $p \equiv 3 \pmod 4$ and is thus omitted. The proof is completed. □

REFERENCES

[1] C. Carlet. *"Boolean functions for cryptography and error correcting codes", in: Crama Y. and Hammer P.L. ed., Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010.

[2] C. Carlet and C. Ding. Highly nonlinear mappings. *Journal of Complexity*, 20(3):205 – 244, 2004.

[3] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[4] C. Carlet, C. Ding, and J. Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Transactions on Information Theory*, 51(6):2089–2102, 2005.

[5] S. T. Choi, J. Y. Kim, J. S. No, and H. Chung. Weight distribution of some cyclic codes. In *IEEE International Symposium on Information Theory Proceedings, ISIT 2012*, 2012.

[6] R. S. Coulter and R. W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Designs, Codes and Cryptography*, 10(2): 167–184, 1997.

[7] P. Delsarte. On subfield subcodes of modified reed-solomon codes (corresp.). *IEEE Transactions on Information Theory*, 1975.

[8] C. Ding and T. Helleseth. Optimal ternary cyclic codes from monomials. *IEEE Transactions on Information Theory*, 59(9):5898–5904, 2013.

[9] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, and M. Mishima. Sets of frequency hopping sequences: Bounds and optimal constructions. *IEEE Transactions on Information Theory*, 2009.

[10] C. Ding, Y. Liu, C. Ma, and L. Zeng. The weight distributions of the duals of cyclic codes with two zeros. *IEEE Transactions on Information Theory*, 2011.

[11] C. Ding, Y. Gao, and Z. Zhou. Five families of three-weight ternary cyclic codes and their duals. *IEEE Transactions on Information Theory*, 2013.

[12] K. Feng and J. Luo. Value distributions of exponential sums from perfect nonlinear functions and their applications. *IEEE Transaction on Information Theory*, 53(9):3035–3041, 2007.

[13] K. Feng and J. Luo. Weight distribution of some reducible cyclic codes. *Finite Fields and Their Applications*, 14(2):390 – 409, 2008.

[14] T. Feng. On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights. *Designs, Codes and Cryptography*, 62 (3):253–258, 2012.

[15] T. Helleseth, C. Rong, and D. Sandberg. New families of almost perfect nonlinear power mappings. *IEEE Transaction on Information Theory*, 45(2):475–485, 1999.

[16] T. Kløve. *Codes for Error Detection*. Series on coding theory and cryptology. World Scientific, 2007.

[17] C. Li, L. Qu, and S. Ling. On the covering structures of two classes of linear codes from perfect nonlinear functions. *IEEE Transaction on Information Theory*, 55(1):70–82, 2009.

[18] N. Li, C. Li, T. Helleseth, C. Ding, and X. Tang. Optimal ternary cyclic codes with minimum distance four and five. *[Online]. Available: http://arxiv.org/pdf/1309.1218v1.pdf*, 2013.

[19] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, Cambridge, 2nd edition, 1997.

[20] J. Luo and K. Feng. On the weight distributions of two classes of cyclic codes. *IEEE Transactions on Information Theory*, 2008.

[21] J. Yuan, C. Carlet, and C. Ding. The weight distribution of a class of linear codes from perfect nonlinear functions. *IEEE Transactions on Information Theory*, 52(2):712–717, 2006.

[22] X. Zeng, L. Hu, W. Jiang, Q. Yue, and X. Cao. The weight distribution of a class of p-ary cyclic codes. *Finite Fields and Their Applications*, 16(1):56–73, 2010.

[23] X. Zeng, J. Shan, and L. Hu. A triple-error-correcting cyclic code from the Gold and Kasami-Welch APN power functions. *Finite Fields and Their Applications*, 18(1):70 – 92, 2012.

[24] Z. Zha and X. Wang. Almost perfect nonlinear power functions in odd characteristic. *IEEE Transaction on Information Theory*, 57(7): 4826–4832, 2011.

[25] Z. Zhou and C. Ding. Seven classes of three-weight cyclic codes. *IEEE Transactions on Communications*, 2013.

[26] Z. Zhou and C. Ding. A class of three-weight cyclic codes. *Finite Fields and Their Applications*, 25(0):79 – 93, 2014.

[27] Z. Zhou, C. Ding, J. Luo, and A. Zhang. A family of five-weight cyclic codes and their weight enumerators. *IEEE Transactions on Information Theory*, 2013.