# A FAMILY OF OPTIMAL TERNARY CYCLIC CODES WITH MINIMUM DISTANCE FIVE AND THEIR DUALS

DANDAN WANG, XIWANG CAO

Abstract. As a subclass of linear codes, cyclic codes have important applications in consumer electronics, data storage systems and communication systems. In this paper, a new family of optimal ternary cyclic codes with minimum distance five are obtained from known perfect nonlinear functions over $\mathbb{F}_{3^m}$. Moreover, we investigate the weight distributions of their duals.

## 1. Introduction

Let $\mathbb{F}_p$ denote the finite field with $p$ elements, where $p$ is a prime. An $[n, k, d]$ linear code over $\mathbb{F}_p$ is a $k$-dimensional subspace of $\mathbb{F}_p^n$ with minimum distance $d$. An $[n, k]$ linear code $\mathcal{C}$ is called cyclic code if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. It is well known that any linear code of length $n$ over $\mathbb{F}_p$ corresponds to a subset of the polynomial residue class ring $\mathbb{F}_p[x]/(x^n - 1)$. A linear code is cyclic if and only if the corresponding subset in $\mathbb{F}_p[x]/(x^n - 1)$ is an ideal of ring $\mathbb{F}_p[x]/(x^n - 1)$. So we study cyclic code by identifying any codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_p^n$ with a polynomial

$$c(x) := \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_p[x]/(x^n - 1).$$

Note that every ideal of $\mathbb{F}_p[x]/(x^n - 1)$ is principal. For any cyclic code $\mathcal{C}$ over $\mathbb{F}_p$, there exists a monic polynomial with the smallest degree among all generators of $\mathcal{C}$ such that $\mathcal{C} = \langle g(x) \rangle$. Then $g(x)$ is unique and called the generator polynomial, and $h(x) = (x^n - 1)/g(x)$ is termed as the parity-check polynomial of $\mathcal{C}$. We say the code $\mathcal{C}$ has $\ell$ zeros if the generator polynomial of the dual code of $\mathcal{C}$ of length $n$ over $\mathbb{F}_p$ is a product of $\ell$ distinct irreducible polynomials over $\mathbb{F}_p$. For more information of cyclic codes, the readers can refer to [12].

Let $A_i$ denote the number of codewords with Hamming weight $i$ in a linear code $\mathcal{C}$ of length $n$. The weight enumerator of $\mathcal{C}$ is defined by

$$1 + A_1 z + A_2 z^2 + \cdots + A_n z^n.$$

The weight distribution $(1, A_1, \ldots, A_n)$ is a significant research topic in coding theory, as it contains crucial information about the error correcting capability, the probability of error detection and correction with respect to some algorithms. A code $\mathcal{C}$ is said to be a $t$-weight code if the number of nonzero $A_i$ in the sequence $(A_1, \ldots, A_n)$ is equal to $t$.

Cyclic codes are a special subclass of linear codes. Since cyclic codes have efficient encoding and decoding algorithms, they have wide applications in storage and communication systems [2, 11, 19]. For example, Reed-Solomon codes have found important applications from deep-space communication to consumer electronics. Therefore, cyclic codes have attracted a number of scholars to research over the last few decades[21, 25, 26, 28, 29, 30].

*Date*: September 2, 2020.
2010 *Mathematics Subject Classification.* 94B15, 11T71.
*Key words and phrases.* Cyclic code, Sphere Packing Bound, perfect nonlinear function .
This work was supported by the National Natural Science Foundations of China (Grant Nos. 11771007 and 61572027).

Let $\beta$ be a generator of $\mathbb{F}_{3^m}^*$, where $\mathbb{F}_{3^m}$ is the finite field with $3^m$ elements and $\mathbb{F}_{3^m}^* = \mathbb{F}_{3^m} \setminus \{0\}$. The cyclotomic coset modulo $3^m - 1$ containing $j$ is defined as

$$C_j = \{j \cdot 3^t (\text{mod } 3^m - 1) : t = 0, 1, \cdots, l_j - 1\},$$

where $l_j$ is the smallest integer satisfying $j \cdot 3^{l_j} \equiv j \pmod{3^m - 1}$. It is well known that the minimal polynomial of $\beta^i$ over $\mathbb{F}_3$ is $m_i(x) = \prod_{j \in C_i}(x - \beta^j)$. We denote by $\mathcal{C}_{(i_1, i_2, \ldots, i_t)}$ the cyclic code with generator polynomial $m_{i_1}(x) m_{i_2}(x) \cdots m_{i_t}(x)$.

Carlet et al. constructed some optimal ternary cyclic codes with minimum distance 4 by using perfect nonlinear monomials in [1]. Ding and Helleseth [6] obtained several optimal ternary cyclic codes by utilizing almost perfect nonlinear monomials and some other monomials over $\mathbb{F}_{3^m}$. Moreover, they proposed nine open problems about that optimal ternary cyclic codes, one of which were settled by Li et al.[13, 14] with the help of factorization of a polynomial. Some new optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 2m - 1, 4]$ are also obtained in [13]. Zhou et al.[28] presented a class of three-weight cyclic codes over $\mathbb{F}_p$ whose duals have two zeros, and the duals of a subclass of the cyclic codes are also studied and proved to be optimal. Fan et al.[7] obtained a class of optimal ternary cyclic codes and studied the weight distribution of their duals. Wang et al. [22] constructed several new classes of optimal ternary cyclic codes by analyzing the solutions of certain equations over $\mathbb{F}_{3^m}$. Yan et al.[24] obtained a family of optimal ternary cyclic codes and the weights of their duals were also considered. Very recently, Liu et al.[16] settled one of the nine conjectures proposed in [6]. In addition, they made progress toward other two conjectures. And in [17], four classes of optimal quinary cyclic codes were provided. Based on the result in [6], Zha and Hu [27] presented six new classes of optimal ternary cyclic codes by determining the solutions of certain equations over $\mathbb{F}_{3^m}$.

Especially, by setting $u = \frac{3^m - 1}{2}$ and properly choosing integers $v$, several classes of optimal ternary cyclic codes $\mathcal{C}_{(1,u,v)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ were obtained [13]. Inspired by the work before, we present a new family of ternary codes $\mathcal{C}_{(0,u,v)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ by taking $u = \frac{3^m + 1}{2}$, and $v$ is an integer such that $x^v$ is a known PN function over $\mathbb{F}_{3^m}$, where $m$ is even. It is verified that the ternary code we mentioned is optimal with respect to some certain bound. And the weight distribution of the duals of $\mathcal{C}_{(0,u,v)}$ are also considered.

This paper is organized as follows. After this introduction, some notations and known results are recalled in Section 2 and the parameters of cyclic codes $\mathcal{C}_{(0,u,v)}$ are presented in Section 3. The weight distributions of the duals of $\mathcal{C}_{(0,u,v)}$ are discussed in Section 4. Section 5 concludes this paper.

## 2. Preliminaries

In this section, we present some basic notations and lemmas over finite fields, which are needed to discuss the parameters of ternary cyclic codes $\mathcal{C}_{(0,u,v)}$ and calculate the weight distributions of their duals. Firstly, we introduce some notations about perfect nonlinear (PN) functions and almost perfect nonlinear functions (APN) on $\mathbb{F}_{p^m}$. Let $f$ be a function from $\mathbb{F}_{p^m}$ to itself, $f$ is called *perfect nonlinear* (PN) or *planar* if

$$\max_{0 \neq a \in \mathbb{F}_{p^m}} \max_{b \in \mathbb{F}_{p^m}} |\{x \in \mathbb{F}_{p^m} : f(x + a) - f(x) = b\}| = 1,$$

and *almost perfect nonlinear* (APN) if

$$\max_{0 \neq a \in \mathbb{F}_{p^m}} \max_{b \in \mathbb{F}_{p^m}} |\{x \in \mathbb{F}_{p^m} : f(x + a) - f(x) = b\}| = 2.$$

PN and APN functions are of interest in cryptography and coding theory. By the definition of PN function, a function $f$ from $\mathbb{F}_{3^m}$ to itself is PN if and only if

$$\begin{cases} x - y = a \\ f(x) - f(y) = b \end{cases}$$

has a unique solution $(x, y) \in \mathbb{F}_{3^m} \times \mathbb{F}_{3^m}$ for each $(a, b) \in \mathbb{F}_{3^m}^* \times \mathbb{F}_{3^m}$. This property of PN functions will be utilized in the proofs of the main results in this paper. The known PN monomials over $\mathbb{F}_{3^m}$ are listed as follows:

- $f(x) = x^{3^\alpha+1}$, where $m/\gcd(m, \alpha)$ is odd;
- $f(x) = x^2$;
- $f(x) = x^{\frac{3^h+1}{2}}$, where $\gcd(m, h) = 1$ and $h$ is odd.

**Lemma 2.1.** [23] *Let $p$ be a prime and $n = p^m - 1$. For any $1 \le i \le n-1$ with $1 \le \gcd(i, n) \le p-1$, the length of the $p$-cyclotomic coset $C_i$ is equal to $m$.*

The following bound on linear codes was given by EI Ronayheb, which will be employed in the analysis of the minimum distance of cyclic codes we constructed.

**Lemma 2.2.** [20] *Let $A_q(n, d)$ be the maximum number of codewords of a $q$-ary code with length $n$ and Hamming distance at least $d$. If $q \ge 3, t = n - d + 1$ and $r = \lfloor min\{\frac{n-t}{2}, \frac{t-1}{q-2}\}\rfloor$, then*

$$A_q(n, d) \le \frac{q^{t+2r}}{\sum_{i=0}^{r} \begin{pmatrix} t+2r \\ i \end{pmatrix} (q-1)^i}.$$

Our calculation of wight distributions of the duals of $\mathcal{C}_{(0,u,v)}$ rely heavily on the following lemmas. Let $\chi$ be an additive and $\psi$ a multiplicative character of $\mathbb{F}_q$. Then the Gaussian sum $G(\psi, \chi)$ is defined by

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x).$$

Let $\eta$ and $\chi_1$ be the quadratic and canonical additive character of $\mathbb{F}_q$, respectively. The explicit value of quadratic Gaussian sum $G(\eta, \chi_1)$ is given as follows.

**Lemma 2.3.** [15] *Let $\mathbb{F}_q$ be a finite field with $q = p^m$, where $p$ is an odd prime. Then*

$$G := G(\eta, \chi_1) = \begin{cases} (-1)^{m-1} q^{\frac{1}{2}} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{m-1} i^m q^{\frac{1}{2}} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

*where $i = \sqrt{-1}$.*

**Lemma 2.4.** [15] *Assume that $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then*

$$\sum_{x \in \mathbb{F}_q} \chi_1(f(x)) = \chi_1(a_0 - a_1^2(4a_2)^{-1})\eta(a_2)G.$$

We take the following definition and properties from [3] and [4]. For $a, b \in \mathbb{F}_{p^m}$ and any integer $\alpha$, define $S_\alpha(a, b)$ by

$$S_\alpha(a, b) = \sum_{x \in \mathbb{F}_{p^m}} \chi_1(ax^{p^\alpha+1} + bx).$$

For the explicit values of $S_\alpha(a, b)$, we have the following useful results.

**Lemma 2.5.** [4] *Let $q = p^m$ and $\alpha$ be any integer such that $m/\gcd(\alpha, m)$ is odd. Assume $a \neq 0$. Then*

$$S_\alpha(a,0) = \begin{cases} (-1)^{m-1}\sqrt{q}\eta(a) & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{m-1} i^m \sqrt{q}\eta(a) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

**Lemma 2.6.** [3] *Let $q = p^m$ and $\alpha$ be any integer such that $m/\gcd(\alpha, m)$ is odd, $f(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax$. Assume $a \neq 0, b \neq 0$. Let $x_{a,b}$ be the unique solution of equation $f(x) = -b^{p^\alpha}$. Then*

$$S_\alpha(a,b) = \begin{cases} (-1)^{m-1}\sqrt{q}\eta(-a)\overline{\chi_1(ax_{a,b}^{p^\alpha+1})} & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{m-1} i^{3m} \sqrt{q}\eta(-a)\overline{\chi_1(ax_{a,b}^{p^\alpha+1})} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

**Remark 2.7.** *It is an easy work to prove that for any $a \neq 0, f(x)$ is a linearized permutation polynomial. Hence the equation $f(x) = -b^{p^\alpha}$ has a unique solution.*

## 3. New optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 2m - 2, 5]$

In this section, let $m > 1$ be an even integer, $u = \frac{3^m+1}{2}$, $v$ an integer such that $x^v$ is a known PN function over $\mathbb{F}_{3^m}$, and $\beta$ a generator of $\mathbb{F}_{3^m}^*$. By considering the cyclic code $\mathcal{C}_{(0,u,v)}$ with the generator polynomial $(x-1)m_u(x)m_v(x)$, where $x-1$ is the minimal polynomial of $\beta^0$ over $\mathbb{F}_3$, we derive a class of optimal ternary cyclic codes with minimum distance 5.

**Theorem 3.1.** *Let the symbols be the same as before. Then the cyclic code $\mathcal{C}_{(0,u,v)}$ with the generator polynomial $(x-1)m_u(x)m_v(x)$ is an optimal ternary cyclic code with parameters $[3^m - 1, 3^m - 2m - 2, 5]$.*

*Proof.* The length of the cyclic code $\mathcal{C}_{(0,u,v)}$ is $3^m - 1$. Obviously, the dimension is determined by the sizes of cyclotomic cosets modulo $3^m - 1$ containing $u$ and $v$. Note that $(v, 3^m - 1) = 2$ and $\gcd(u, 3^m - 1) = 1$ as $m$ is even. Then we have $|C_u| = |C_v| = m$ by Lemma 2.1, and $C_u \bigcap C_v = \emptyset$ can be verified easily. Hence, the dimension of the ternary cyclic code $\mathcal{C}_{(0,u,v)}$ is $3^m - 2m - 2$. Next, we will prove the minimum distance of the code $\mathcal{C}_{(0,u,v)}$ is equal to 5.

On one hand, we have the minimum distance of code $\mathcal{C}_{(0,u,v)}$ satisfies $d \leq 6$ by Sphere Packing Bound. Below, we will show that there is no ternary cyclic code with parameters $[3^m - 1, 3^m - 2m - 2, 6]$. Otherwise, applying Lemma 2.2 to this case, $q = 3, n = 3^m - 1, t = 3^m - 6, r = 2$, then $t + 2r = 3^m - 2$, $\sum_{i=0}^{r} \begin{pmatrix} t+2r \\ i \end{pmatrix} (q-1)^i = 1 + 2(3^m - 2)^2$ and

$$3^{3^m - 2m - 2} \leq A_3(n,d) \leq \frac{3^{3^m-2}}{1 + 2(3^m - 2)^2},$$

this indicates that $(3^m - 4)^2 \leq 7$, we get a contradiction since $m > 1$. Hence the minimum distance of the cyclic code $\mathcal{C}_{(0,u,v)}$ satisfies $d \leq 5$. (This indicates that $\mathcal{C}_{(0,u,v)}$ is optimal if $d = 5$.)

On the other hand, we prove $d \geq 5$, i.e., we need to show that code $\mathcal{C}_{(0,u,v)}$ has no codeword with Hamming weights $w \in \{1, 2, 3, 4\}$. By the definition of $\mathcal{C}_{(0,u,v)}$, it has a codeword of Hamming weight $w$ if and only if there exist $w$ nonzero elements $c_1, c_2, \ldots, c_w$ in $\mathbb{F}_3$ and $0 \leq t_1 < t_2 < \cdots < t_w \leq 3^m - 2$ such that

$$\begin{cases} c_1 + c_2 + \cdots + c_w = 0 \\ c_1\beta^{ut_1} + c_2\beta^{ut_2} + \cdots + c_w\beta^{ut_w} = 0 \\ c_1\beta^{vt_1} + c_2\beta^{vt_2} + \cdots + c_w\beta^{vt_w} = 0. \end{cases} \tag{3.1}$$

It's easily seen that $d \geq 2$. If $w = 2$, then one has $c_1 = -c_2$, this implies $c_1(\beta^{ut_1} - \beta^{ut_2}) = 0$, i.e., $\beta^{u(t_2-t_1)} = 1$, then we get a contradiction since the fact that $(u, 3^m - 1) = 1$. We continue to prove

$\mathcal{C}_{(0,u,v)}$ has no codeword of weight 3, which is equivalent to show that (3.1) has no solution over $\mathbb{F}_{3^m}$ for $w=3$. Let $x_i=\beta^{t_i}$ for $i=1,2,3$, which implies that $x_1,x_2,x_3$ are pairwise distinct elements of $\mathbb{F}_{3^m}^*$. And then put $x_1/x_3=y_1, x_2/x_3=y_2$, which indicates that $y_1\neq y_2$ and $y_1,y_2\in\mathbb{F}_{3^m}\backslash\{0,1\}$. Hence (3.1) can be written as

$$\begin{cases} c_1+c_2+c_3=0\\ c_1y_1^u+c_2y_2^u+c_3=0\\ c_1y_1^v+c_2y_2^v+c_3=0. \end{cases} \tag{3.2}$$

We only need to consider the case $c_1=c_2=c_3=1$ from the first equation of (3.2). Recall that $u=\frac{3^m+1}{2}$, hence $y^u=y$ if $y$ is a square in $\mathbb{F}_{3^m}^*$, and $y^u=-y$ otherwise. Then (3.2) becomes

$$\begin{cases} \eta(y_1)y_1+\eta(y_2)y_2+1=0\\ y_1^v+y_2^v+1=0. \end{cases}$$

Utilizing the fact that $v$ is even since $x^v$ is PN over $\mathbb{F}_{3^m}$, the system of equations above becomes

$$\begin{cases} \eta(y_1)y_1-1=1-\eta(y_2)y_2\\ (\eta(y_1)y_1)^v-1=1-(\eta(y_2)y_2)^v. \end{cases} \tag{3.3}$$

Then (3.3) is established if and only if $(\eta(y_1)y_1,1)=(1,\eta(y_2)y_2)$ which follows from the property of PN functions. This contradict with the condition that $y_1,y_2$ are two distinct elements in $\mathbb{F}_{3^m}\setminus\{0,1\}$.

Next, we will show that the code $\mathcal{C}_{(0,u,v)}$ does not have a codeword with weight 4. For $w=4$, using the way which analogous to the case for $w=3$, we have

$$\begin{cases} c_1+c_2+c_3+c_4=0\\ c_1y_1^u+c_2y_2^u+c_3y_3^u+c_4=0\\ c_1y_1^v+c_2y_2^v+c_3y_3^v+c_4=0. \end{cases} \tag{3.4}$$

By the first equation of (3.4), we only need to consider the case that $c_4=1$ due to symmetry, then one of $c_i, i=1,2,3$ is 1, and the others are $-1$. Without loss of generality, set $c_1=1$ and then $c_2=c_3=-1$. Similarly, (3.4) can be written as

$$\begin{cases} \eta(y_1)y_1-\eta(y_2)y_2=\eta(y_3)y_3-1\\ y_1^v-y_2^v=y_3^v-1. \end{cases} \tag{3.5}$$

According to the properties of PN function, the solution $(y_1,y_2,y_3)$ of the system of equations above satisfies

$$(\eta(y_1)y_1,\eta(y_2)y_2)=(\eta(y_3)y_3,1),$$

which implies that $y_2=-1, y_1=-y_3$ since $y_i\neq 0,1, i=1,2,3$ are pairwise distinct. Due to symmetry, we only need to prove that (3.5) has no solution for the case that $y_1$ is a square and $y_3$ is a nonsquare. However, $\eta(y_1)=\eta(-y_3)=\eta(y_3)=1$ since $\eta(-1)=1$ for even $m$, this is contradicts with the assumption that $\eta(y_3)=-1$. Thus the proof is completed. □

## 4. The weight distributions of the duals of $\mathcal{C}_{(0,u,v)}$

In this section, the Hamming weight distributions of the duals of $\mathcal{C}_{(0,u,v)}$ will be settled. Let $\chi_1'$ and $\chi_1$ be the canonical additive character of $\mathbb{F}_3$ and $\mathbb{F}_{3^m}$, respectively. From Delsarte's Theorem [5], we then deduce that the duals of $\mathcal{C}_{(0,u,v)}$ are given as follows

$$\mathcal{C}_{(0,u,v)}^{\perp}=\{\mathbf{c}(a,b,c): a,b,c\in\mathbb{F}_{3^m}\},$$

where $\mathbf{c}(a,b,c)=(\mathrm{Tr}(a\beta^{-ui}+b\beta^{-vi}+c))_{i=0}^{3^m-2}$, the map Tr denotes the absolute trace from $\mathbb{F}_{3^m}$ to $\mathbb{F}_3$. From the discussion above, the weight of codeword $\mathbf{c}(a,b,c)$ in the duals of $\mathcal{C}_{(0,u,v)}$ is given as follows:

$$\begin{aligned}
wt(\mathbf{c}(a,b,c)) &= \#\{0\le i\le 3^m-2 : c_i\neq 0\}\\
&= 3^m-1-\frac{1}{3}\sum_{y\in\mathbb{F}_3}\sum_{i=0}^{3^m-2}\chi_1'(y(\mathrm{Tr}(a\beta^{-ui}+b\beta^{-vi}+c)))\\
&= 3^m-1-\frac{1}{3}\sum_{y\in\mathbb{F}_3}\sum_{x\in\mathbb{F}_{3^m}^*}\chi_1(ayx^u+byx^v+yc)\\
&= 2\cdot 3^{m-1}-1+\frac{1}{3}\sum_{y\in\mathbb{F}_3}\chi_1(yc)-\frac{1}{3}\sum_{y\in\mathbb{F}_3^*}\sum_{x\in\mathbb{F}_{3^m}}\chi_1(yax^u+ybx^v+yc)\\
&= \begin{cases} 2\cdot 3^{m-1}-\frac{1}{3}\sum\limits_{y\in\mathbb{F}_3^*}\sum\limits_{x\in\mathbb{F}_{3^m}}\chi_1(yax^u+ybx^v) & \text{if } \mathrm{Tr}(c)=0,\\ 2\cdot 3^{m-1}-1-\frac{1}{3}\sum\limits_{y\in\mathbb{F}_3^*}\sum\limits_{x\in\mathbb{F}_{3^m}}\chi_1(yax^u+ybx^v+yc) & \text{if } \mathrm{Tr}(c)\neq 0. \end{cases}
\end{aligned}$$

Review that $v$ is even since $x^v$ is a known PN function over $\mathbb{F}_{3^m}$. Denote by SQ and NSQ the set of all squares and nonsquares in $\mathbb{F}_{3^m}^*$, respectively. If $\mathrm{Tr}(c)=0$, we can deduce that

$$\begin{aligned}
wt(\mathbf{c}(a,b,c)) &= 2\cdot 3^{m-1}-\frac{1}{3}\sum_{y\in\mathbb{F}_3^*}\sum_{x\in\mathbb{F}_{3^m}}\chi_1(yax^u+ybx^v)\\
&= 2\cdot 3^{m-1}-\frac{1}{3}(2+\sum_{x\in SQ}\chi_1(ax+bx^v)+\sum_{x\in NSQ}\chi_1(-ax+bx^v)\\
&\quad+\sum_{x\in SQ}\chi_1(-ax-bx^v)+\sum_{x\in NSQ}\chi_1(ax-bx^v))\\
&= 2\cdot 3^{m-1}-\frac{1}{3}(2+\sum_{x\in SQ}\chi_1(ax+bx^v)+\sum_{x\in NSQ}\chi_1(ax+bx^v)\\
&\quad+\sum_{x\in SQ}\chi_1(-ax-bx^v)+\sum_{x\in NSQ}\chi_1(-ax-bx^v))\\
&= 2\cdot 3^{m-1}-\frac{1}{3}(\sum_{x\in\mathbb{F}_{3^m}}\chi_1(bx^v+ax)+\sum_{x\in\mathbb{F}_{3^m}}\overline{\chi_1}(bx^v+ax)). \qquad (4.1)
\end{aligned}$$

The third equality above follows from the fact $-x$ runs though SQ or NSQ as $x$ runs ranges over SQ or NSQ, respectively. Similarly, if $\mathrm{Tr}(c)\neq 0$, we can obtain that

$$\begin{aligned}
&wt(\mathbf{c}(a,b,c))\\
=\ & 2\cdot 3^{m-1}-1-\frac{1}{3}(\sum_{x\in\mathbb{F}_{3^m}}\chi_1(bx^v+ax+c)+\sum_{x\in\mathbb{F}_{3^m}}\overline{\chi_1}(bx^v+ax+c))\\
=\ & 2\cdot 3^{m-1}-1-\frac{1}{3}(\chi_1(c)\sum_{x\in\mathbb{F}_{3^m}}\chi_1(bx^v+ax)+\overline{\chi_1}(c)\sum_{x\in\mathbb{F}_{3^m}}\overline{\chi_1}(bx^v+ax)). \qquad (4.2)
\end{aligned}$$

It is easily seen that $\mathbf{c}(a_1,b_1,c_1)=\mathbf{c}(a_2,b_2,c_2)$ if and only if $a_1=a_2,b_1=b_2,\mathrm{Tr}(c_1)=\mathrm{Tr}(c_2)$, where $\mathbf{c}(a_1,b_1,c_1),\mathbf{c}(a_2,b_2,c_2)$ are codewords in $\mathcal{C}_{(0,u,v)}^{\perp}$. Hence, we only need to consider $a,b\in\mathbb{F}_{3^m}$ and $\mathrm{Tr}(c)\in\mathbb{F}_3$ when we discuss the weight distributions. For even $m$, the weight distributions of the duals of $\mathcal{C}_{(0,u,v)}$ are obtained and described in the following theorem.

**Theorem 4.1.** *Let $m$ be even and $u=\frac{3^m+1}{2}$, $v$ is an integers such that $x^v$ is a known PN function over $\mathbb{F}_{3^m}$. Then the duals of $\mathcal{C}_{(0,u,v)}$ are cyclic codes with parameters $[3^m-1,2m+1,2\cdot 3^{m-1}-1-2\cdot 3^{\frac{m}{2}-1}]$ and we have the following results:*

*(i) $v=3^\alpha+1$, where $m/\gcd(m,\alpha)$ is odd, the weight distribution of $\mathcal{C}_{(0,u,v)}^{\perp}$ is given by Table 1.*

TABLE 1. The weight distribution of $\mathcal{C}^{\perp}_{(0,u,3^{\alpha}+1)}$ and $\mathcal{C}^{\perp}_{(0,u,2)}$

| *Hamming Weight* | *Frequency* |
|---|---|
| $0$ | $1$ |
| $3^m-1$ | $2$ |
| $2\cdot 3^{m-1}$ | $3^m-1$ |
| $2\cdot 3^{m-1}-1$ | $2(3^m-1)$ |
| $2\cdot 3^{m-1}\pm 2\cdot 3^{\frac{m}{2}-1}$ | $\frac{3^m-1}{2}(3^{m-1}\mp 2\cdot 3^{\frac{m}{2}-1})$ |
| $2\cdot 3^{m-1}\pm 3^{\frac{m}{2}-1}$ | $(3^m-1)(3^{m-1}\mp 3^{\frac{m}{2}-1})$ |
| $2\cdot 3^{m-1}-1\pm 2\cdot 3^{\frac{m}{2}-1}$ | $(3^m-1)(3^{m-1}\pm 3^{\frac{m}{2}-1})$ |
| $2\cdot 3^{m-1}-1\pm 3^{\frac{m}{2}-1}$ | $(3^m-1)(2\cdot 3^{m-1}\pm 3^{\frac{m}{2}-1})$ |

TABLE 2. The weight distribution of the dual of $\mathcal{C}^{\perp}_{(0,u,\frac{3^h+1}{2})}$

| Hamming Weight | Frequency |
|---|---|
| $0$ | $1$ |
| $3^m-1$ | $2$ |
| $2\cdot 3^{m-1}$ | $3^m-1$ |
| $2\cdot 3^{m-1}-1$ | $2(3^m-1)$ |
| $2\cdot 3^{m-1}\pm 2\cdot 3^{\frac{m}{2}-1}$ | $\frac{1}{8}(3^m-1)((3^{\frac{m}{2}}\pm 1)(3^{\frac{m}{2}-1}\mp 1)+(3^{\frac{m}{2}}\mp 1)^2)$ |
| $2\cdot 3^{m-1}\pm 3^{\frac{m}{2}-1}$ | $3^{\frac{m}{2}-1}(3^m-1)(3^{\frac{m}{2}}\mp 1)$ |
| $2\cdot 3^{m-1}-1\pm 2\cdot 3^{\frac{m}{2}-1}$ | $3^{\frac{m}{2}-1}(3^m-1)(3^{\frac{m}{2}}\pm 1)$ |
| $2\cdot 3^{m-1}-1\pm 3^{\frac{m}{2}-1}$ | $\frac{1}{4}(3^m-1)((3^{\frac{m}{2}}\pm 1)^2+(3^{\frac{m}{2}}\mp 1)(3^{\frac{m}{2}-1}\pm 1)+4\cdot 3^{\frac{m}{2}-1}(3^{\frac{m}{2}}\mp 1))$ |

*(ii) $v=2$, the weight distribution of $\mathcal{C}^{\perp}_{(0,u,v)}$ is same as the case (i).*

*(iii) $v=\frac{3^h+1}{2}$, where $\gcd(m,h)=1$ and $h$ is odd, the weight distribution of $\mathcal{C}^{\perp}_{(0,u,v)}$ is given by Table 2.*

*Proof.* From the discussion above, the proof is given in three cases based on the value of $v$.

(i) Considering the case when $v=3^{\alpha}+1$, where $m/\gcd(m,\alpha)$ is odd. We further distinguish two subcases according to the values of $\mathrm{Tr}(c)$. If $\mathrm{Tr}(c)=0$, from (4.1) and Lemma 2.5, we have

$$\begin{aligned}\mathbf{c}(a,b,c) &= 2\cdot 3^{m-1}-\frac{1}{3}(\sum_{x\in\mathbb{F}_{3^m}}\chi_1(bx^{3^{\alpha}+1}+ax)+\sum_{x\in\mathbb{F}_{3^m}}\overline{\chi_1}(bx^{3^{\alpha}+1}+ax))\\ &= 2\cdot 3^{m-1}-\frac{1}{3}(S_{\alpha}(b,a)+\overline{S_{\alpha}(b,a)}).\end{aligned}$$

If $\mathrm{Tr}(c)\neq 0$, by (4.2) and Lemma 2.6, then

$$wt(\mathbf{c}(a,b,c))=2\cdot 3^{m-1}-1-\frac{1}{3}\left(\chi_1(c)S_{\alpha}(b,a)+\overline{\chi_1(c)S_{\alpha}(b,a)}\right).$$

Note that the value distributions of the exponential sums $S_{\alpha}(b,a)$ is given as Theorem 1 in [10]. Concluding the two cases above, the weight distribution of $\mathcal{C}_{(0,u,v)}$ is obtained.

(ii) Considering the case when $v=2$. Combing with (4.1), (4.2) and Lemmas 2.3, 2.4, the desired results can be obtained.

(iii) Considering the case when $v=\frac{3^h+1}{2}$, where $h$ is odd, and $\gcd(m,h)=1$. The exponential sums $\sum_{x\in\mathbb{F}_{p^m}}\chi_1(ax^{\frac{p^h+1}{2}}+bx)$ is denoted by $S(a,b)$. The value distribution of the multiset

$$\{S(a,b)=\sum_{x\in\mathbb{F}_{p^m}}\chi_1(ax^{\frac{p^h+1}{2}}+bx)|a,b\in\mathbb{F}_{p^m}\}$$

is given in Theorem 2 of [18]. In this case, $p = 3, \gcd(m, h) = 1$. Note that $\chi_1(c) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ if $\mathrm{Tr}(c) = 1$ and $\chi_1(c) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ if $\mathrm{Tr}(c) = -1$. By (4.1), (4.2) and Theorems 2, 4 in [18], we obtain the weight distribution of $\mathcal{C}^{\perp}_{(0,u,v)}$ when $v = \frac{3^h+1}{2}$. □

**Remark 4.2.** *Note that when $h$ is odd and $\gcd(m, h) = 1$, the function $f(x) = \mathrm{Tr}(ax^{\frac{3^h+1}{2}})$ is weakly regular bent function over $\mathbb{F}_{3^m}$. This is also the well-known Coulter-Mattews bent function. For more information about the dual codes when $v = \frac{3^h+1}{2}$, the readers can refer to references* [8, 9].

**Example 4.3.** *Let $m = 6, \alpha = 2$ and $\beta$ be a generator of $\mathbb{F}_{3^m}$ with the minimal polynomial $x^6 + 2x^4 + x^2 + 2x + 2$, then $u = 365, v = 3^\alpha + 1 = 10$. We have the code $\mathcal{C}_{(0,u,v)}$ is an optimal ternary cyclic code with the generator polynomial $x^{13} + x^{12} + 2x^{10} + x^9 + 2x^7 + x^6 + x^5 + 2x^3 + 1$ and parameters $[728, 715, 5]$. By Theorem 4.1, the weight enumerator of $\mathcal{C}^{\perp}_{(0,u,v)}$ is*

$$1 + 2x^{728} + 728x^{486} + 1456x^{485} + 81900x^{504} + 95004x^{468} + 170352(x^{495} + x^{467}) \\ +183456(x^{477} + x^{503}) + 360360x^{494} + 347256x^{476},$$

*which is checked by Magma.*

**Example 4.4.** *Let $m = 4, v = 2$ and $\beta$ be a generator of $\mathbb{F}_{3^m}$ with the minimal polynomial $x^4 + 2x^3 + 2$, then $u = 41$. We have the code $\mathcal{C}_{(0,u,v)}$ is an optimal ternary cyclic code with the generator polynomial $x^9 + 2x^8 + x^6 + 2x^5 + 2x^4 + x^2 + 2x + 1$ and parameters $[80, 71, 5]$. By Theorem 4.1, the weight enumerator of $\mathcal{C}^{\perp}_{(0,u,v)}$ is*

$$1 + 2x^{80} + 80x^{54} + 160x^{53} + 840x^{60} + 1320x^{48} + 1920(x^{47} + x^{57}) \\ +2400(x^{51} + x^{59}) + 4080x^{50} + 4560x^{56},$$

*which is checked by Magma.*

**Example 4.5.** *Let $m = 4, h = 3$ and $\beta$ be a generator of $\mathbb{F}_{3^m}$ with the minimal polynomial $x^4 + 2x^3 + 2$, then $u = 41, v = \frac{3^h+1}{2} = 14$. We have the code $\mathcal{C}_{(0,u,v)}$ is an optimal ternary cyclic code with the generator polynomial $x^9 + x^8 + 2x^6 + 2x^5 + 2x^3 + x^2 + 2x + 1$ and parameters $[80, 71, 5]$. By Theorem 4.1, the weight enumerator of $\mathcal{C}^{\perp}_{(0,u,v)}$ is*

$$1 + 2x^{80} + 80x^{54} + 160x^{53} + 840x^{60} + 1320x^{48} + 1920(x^{47} + x^{57}) \\ +2400(x^{51} + x^{59}) + 4080x^{50} + 4650x^{56},$$

*which is checked by Magma.*

## 5. Concluding remarks

In this paper, a new family of ternary cyclic codes $\mathcal{C}_{(0,u,v)}$ are obtained from known perfect nonlinear monomials over $\mathbb{F}_{3^m}$, whose minimum distance achieves the certain bound for linear codes which is presented in Lemma 2.2. Moreover, we explore the weight distributions of their duals by Gauss sum and some special exponential sums over finite fields. As a review and comparison, some known classes of optimal ternary cyclic codes are listed in Table 3.

In Table 3, the optimal ternary cyclic codes we list are $\mathcal{C}_{(u',v')}$ with generator polynomial $m_{u'}(x)m_{v'}(x)$ and parameters $[3^m - 1, 3^m - 2m - 1, 4]$. Now, a natural question arise: which $(u', v')$ in Table 3 such that $\mathcal{C}_{(0,u',v')}$ is optimal?

When $u' = 1, v'$ is an integer such that $x^{v'}$ is PN over $\mathbb{F}_{3^m}$, the cyclic codes $\mathcal{C}_{(0,1,e)}$ are optimal, and the proof is similar to that of Theorem 3.1. Moreover, we found that there are other cases may make codes $\mathcal{C}_{(0,u',v')}$ optimal, here $u' = 1, v' = e$. we list them as follows:

(1) Let $m$ be even with $\gcd(m,t)=1$ and $m/\gcd(m,s)$ being odd, $s,t$ be nonnegative integers and $e$ be an even integer defined by $e(3^s+1)\equiv 3^t+1 \pmod{3^m-1}$, and $\gcd(3^m-1,e-1)=\gcd(3^t-e,3^m-1)=1$.
(2) Let $m$ be even and $s$ be an integer such that $\gcd(m,s)=1$, $\gcd(3^s-2,3^m-1)=1$. Let $e$ be defined by $e\equiv\frac{3^m-1}{2}+3^s-1 \pmod{3^m-1}$, and equation $x^{3^s+1}-x^{3^s}+x^2=0$ has no solution in $\mathbb{F}_{3^m}\setminus\{0,\pm 1\}$.
(3) Let $m$ be odd, $e=\frac{3^h-1}{2}$, where $h$ is an even integer satisfies $\gcd(h,m)=\gcd(h-1,m)=1$.
(4) Let $m$ be odd, $e$ be even and $0\le h\le m-1$ satisfying $e(3^h+1)\equiv(3^m+1)/2 \pmod{3^m-1}$.
(5) Let $m,e$ be integers satisfying $5\nmid m, 7e\equiv 2 \pmod{3^m-1}$ and $\gcd(m,6)=1$ or $m\equiv 3 \pmod 6$.
(6) Let $e=3^h+5$, where $2\le h\le m-1$. Let $m\ge 4$ be even, $m\equiv 0 \pmod 4$ and $h=\frac{m}{2}$.

However, more conditions are needed and the proof will be more complicated. Here we present six examples corresponding to the cases above.

**Example 5.1.** *Let $m=4$ and $(s,t)=(0,3)$, since $\gcd(3^s+1,3^m-1)=2$, then $e=14$ or $54$. It can be easily seen that $\gcd(e-1,3^m-1)=\gcd(e-3^t,3^m-1)=1$ hold for both $e=14$ and $e=54$. Let $\beta$ be a generator of $\mathbb{F}_{3^m}$ with $\beta^4+2\beta^3+2=0$. Then $\mathcal{C}_{(0,1,e)}$ is an optimal ternary cyclic code with parameters $[80,71,5]$ and generator polynomial $x^9+2x^8+2x^6+x^5+x^4+x^3+x^2+2x+1(e=14)$ or $x^9+x^7+x^5+2x^3+x^2+2x+1(e=54)$. The weight enumerator of $\mathcal{C}^{\perp}_{(0,1,e)}$ for both $e=14$ and $e=54$ is*

$$1+2x^{80}+80x^2+4560x^{56}+1920(x^{47}+x^{57})+2400(x^{51}+x^{59})+$$
$$1320x^{48}+840x^{60}+4080x^{50}+160x^{53}.$$

**Example 5.2.** *Let $m=6$, $s=1$, then $e=\frac{3^m-1}{2}+3^s-1=366$. Let $\beta$ be a generator of $\mathbb{F}_{3^m}$ with $\beta^6+2\beta^4+\beta^2+2\beta+2=0$. Then $\mathcal{C}_{(0,1,e)}$ is an optimal ternary cyclic code with parameters $[728,715,5]$ and generator polynomial $x^{13}+x^{12}+2x^9+2x^8+x^7+x^6+2x^5+x^4+2x^3+x^2+1$. The weight enumerator of $\mathcal{C}^{\perp}_{(0,1,e)}$ is*

$$1+2x^{728}+1456x^{485}+728x^{486}+170352(x^{495}+x^{467})+347256x^{476}+81900x^{504}+$$
$$183456(x^{477}+x^{503})+95504x^{468}+360360x^{494}.$$

**Example 5.3.** *Let $m=5,h=2$, then $e=\frac{3^h-1}{2}=4$. Let $\beta$ be a generator of $\mathbb{F}_{3^m}$ with $\beta^5+2\beta+1=0$. Then $\mathcal{C}_{(0,1,e)}$ is an optimal ternary cyclic code with parameters $[242,231,5]$ and generator polynomial $x^{11}+x^{10}+x^9+2x^8+x^7+x^6+x^5+2x^4+x^2+1$. The weight enumerator of $\mathcal{C}^{\perp}_{(0,1,e)}$ is*

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

**Example 5.4.** *Let $m=3,h=2$, since $e(3^h+1)\equiv(3^m+1)/2 \pmod{3^m-1}$ and $e$ is even, we have $e=4$. Let $\beta$ be a generator of $\mathbb{F}_{3^m}$ with $\beta^3+2\beta+1=0$. Then $\mathcal{C}_{(0,1,e)}$ is an optimal ternary cyclic code with parameters $[26,19,5]$ and generator polynomial $x^7+x^5+2x^3+x+1$. The weight enumerator of $\mathcal{C}^{\perp}_{(0,1,e)}$ is*

$$1+2x^{26}+390x^{14}+312x^{15}+520x^{17}+260x^{18}+546x^{20}+156x^{21}.$$

**Example 5.5.** *Let $m=3$, since $7e\equiv 2 \pmod{3^m-1}$, then $e=4$. Let $\beta$ be a generator of $\mathbb{F}_{3^m}$ with $\beta^3+2\beta+1=0$. Then $\mathcal{C}_{(0,1,e)}$ is an optimal ternary cyclic code with parameters $[26,19,5]$ and generator polynomial $x^7+x^5+2x^3+x+1$. The weight enumerator of $\mathcal{C}^{\perp}_{(0,1,e)}$ is the same as that in Example 5.4.*

**Example 5.6.** *Let $m=4$, then $h=2$ and $e=3^h+5=14$. Let $\beta$ be a generator of $\mathbb{F}_{3^m}$ with $\beta^4+2\beta^3+2=0$. Then $\mathcal{C}_{(0,1,e)}$ is an optimal ternary cyclic code with parameters $[80,71,5]$ and*

*generator polynomial* $x^9+2x^8+2x^6+x^5+x^4+x^3+x^2+2x+1$. *The weight enumerator of* $\mathcal{C}_{(0,1,e)}^{\perp}$ *is the same as that in Example 5.1.*

TABLE 3. Known optimal ternary cyclic codes $\mathcal{C}_{(u',v')}$

| $u'$ | $v'$ | Conditions | Reference |
|---|---|---|---|
| 1 | $e$ | $e(3^s+1)\equiv 3^t+1 \pmod{3^m-1}$, $0\le s,t\le m-1$, $\gcd(3^m-1,e-1)=\gcd(3^m-1,3^t-e)=1$, $e$ is even, $m$ is either odd or even with $\gcd(m,t)=1$ and $m/\gcd(m,s)$ is odd. | [22] |
| | | $e(3^s-1)\equiv 3^t-1 \pmod{3^m-1}$, $1\le s,t\le m-1$, $m$ is odd, $e$ is even, $\gcd(3^m-1,e-1)=\gcd(m,s)=\gcd(m,t)=1$. | |
| | | $e\equiv \frac{3^m-1}{2}+3^s+1 \pmod{3^m-1}$, $0\le s\le m-1$, $m$ is even, $m/\gcd(m,s)$ is odd. | |
| | | $e\equiv \frac{3^m-1}{2}+3^s-1 \pmod{3^m-1}$, $0\le s\le m-1$, $m$ is even, $\gcd(m,s)=\gcd(3^s-2,3^m-1)=1$, $x^{3^s+1}-x^{3^s}+x^2=0$ has no solution in $\mathbb{F}_{3^m}^*\backslash\{\pm 1\}$. | |
| 1 | $e$ | $m$ is odd, $e$ is even and $0\le h<m$ and $e(3^h+1)\equiv(3^m+1)/2 \pmod{3^m-1}$. | [27] |
| | | $3\nmid m, 5e\equiv 2 \pmod{3^m-1}$ | |
| | | $5\nmid m, 7e\equiv 2 \pmod{3^m-1}$ $\gcd(m,6)=1$ or $m\equiv 3 \pmod 6$. | |
| | | $3\nmid m$, and $5\nmid m$, $5e\equiv 4 \pmod{3^m-1}$. | |
| 1 | $e$ | $x^e$ is planar or APN over $\mathbb{F}_{3^m}$. | [6] |
| | $\frac{3^h-1}{2}$ | $2\le h\le m-1$, $m$ is odd, $h$ is even, $\gcd(m,h)=1$ and $\gcd(m,h-1)=1$. | |
| | $3^h-1$ | $\gcd(m,h)=\gcd(3^m-1,3^h-2)=1$, $1\le h\le m-1$, | |
| 1 | $3^h+5$ | $m$ is even, $2\le h\le m-1$, satisfy $m\equiv 0 \pmod 4$, $h=m/2$ or $m\equiv 2 \pmod 4$, $h=(m+2)/2$. | [16] |
| | $3^h+5$ | $m\ge 5$ is prime, $0\le h\le m-1$,$2h\equiv 1 \pmod m$. | |
| | $3^h+13$ | $m\ge 5$ is prime, $3\le h\le m-1$,$2h\equiv 1 \pmod m$ | |
| 1 | $2(3^{m-1}-1),5(3^{m-1}-1)$ | $m$ is odd, $m\not\equiv 0 \pmod 3$. | [13] |
| | $\frac{3^m-1}{2}-2,\frac{3^m-1}{2}+10$ | $m\equiv 2 \pmod 4$. | |
| | $\frac{3^m-1}{2}+7$ | $m$ is odd. | |
| 1 | $2(3^s+1)$ | $m>1$ is odd and $0\le s\le m-1$. | [14] |
| $\frac{3^m+1}{2}$ | $\frac{3^s+1}{2}$ | $s$ is even and $\gcd(m,s)=1$. | [28] |
| | $2\cdot 3^{\frac{m-1}{2}}+1$ | $m$ is odd. | [7] |
| | $3^s+2$ | $m$ is odd, such that $9\nmid m$ and $4s\equiv 1 \pmod m$. | [24] |

## REFERENCES


[1] Carlet, C., Ding, C., Yuan, J.: Linear codes from prefect nonlinear functions and their secret sharing schemes. IEEE Trans. Inf. Theory. **51** (6) 2089-2102, (2005)

[2] Chien, R. T.: Cyclic decoding procedure for Bose-Chaudhuri-Hocquenghem codes. IEEE Trans. Inf. Theory. **10** (4), 357-363, (1964)

[3] Coulter, R. S.: The number of rational points of a class of Artin-Schreier curves. Finite Fields Appl. **8** (4), 397-413, (2002)

[4] Coulter, R. S.: Explicit evaluations of some Weil sums. Acta Arithmetica. **83**, 241-251, (1998)

[5] Delsarte, P.: On subfield subcodes of modified Reed-Solomon codes. IEEE Trans. Inf. Theory. **21** (5), 575-576, (1975)

[6] Ding, C., Helleseth, T.: Optimal ternary cyclic codes from monomials. IEEE Trans. Inf. Theory. **59** (9), 5898-5904, (2013)

[7] Fan, C., Li, N., Zhou, Z.: A class of optimal ternary cyclic codes and their duals. Finite Fields Appl. **37**, 193-202, (2016)

[8] Hu H., Zhang Q., Shao S.: On the Dual of the Coulter-Matthews Bent Functions. IEEE Trans. Inf. Theory **63**(4): 2454-2463 (2017)

[9] Hu H., Yang X., Tang S.: New Classes of Ternary Bent Functions from the Coulter-Matthews Bent Functions. IEEE Trans. Inf. Theory, **64**6, 4653-4663, (2018)

[10] Feng K., Luo J.: Value distributions of exponential sums from perfect nonlinear functions and their applications. IEEE Trans. Inf. Theory, **53**(9), 3035-3041, (2007)

[11] Forney, G. D.: On decoding BCH codes. IEEE Trans. Inf. Theory. **11** (4), 549-337, (1995)

[12] Huffman, W. C., Pless, V.: Fundamentals of Error-Correcting codes. Cambrige, U. K. Cambridge Univ. Press, (2003)

[13] Li, N., Li, C., Helleseth, T., Ding, C., Tang. X.: Optimal ternary cyclic codes with minimum distance four and five. Finite Fields Appl. **30**, 100-120, (2014)

[14] Li, N., Zhou, Z., Helleseth, T.: On a conjecture about a class of optimal ternary cyclic codes. Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA), DOI: 10.1109/IWSDA.2015.7458415, (2015)

[15] Lidl, R., Niederreiter, H.: Finite field. Cambridge university press, (1997)

[16] Liu Y.,Cao X., Lu W. On some conjectures about optimal ternary cyclic codes. Des. Codes Crypt. **88**, 297-309, (2020)

[17] Liu Y., Cao X. Four classes of optimal quinary cyclic codes. IEEE Comm. Letters. DOI 10.1109/LCOM-M.2020.2983373 (2020)

[18] Luo, J., Feng, K.: Cyclic codes and sequences from generalized Coulter-Matthews function. IEEE Trans. Inf. Theory. **54** (12), 5345-5353, (2008)

[19] Prange, E.: Some cyclic error-correcting codes with simple decoding algorithms Cambridge. MA, USA, Air Force Cambridge Research Center-TN-58-156, (1958)

[20] Rouayheb, S. Y. EI, Georghiaheds, C. N., Soljanin, E., Sprintson, A.: Bounds on codes based on graph theory. IEEE Int. Symp. on Information Theory. 1876-1879, (2007)

[21] Schmidt, B., White, C.: All two-weight irreducible cyclic codes. Finite Fields Appl. **8** (1), 1-17, (2002)

[22] Wang, L., Wu, G.: Several classes of optimal ternary cyclic codes with minimal distance four. Finite Fields Appl. **40**, 126-137, (2016)

[23] Xu, G., Cao, X., Xu, S.: Optimal $p$-ary cyclic codes with minimum distance four from monomials. Cryptography and Communications. **8** (4), 541-554, (2016)

[24] Yan, H., Zhou, Z., Du, X.: A family of optimal ternary cyclic codes from Niho-type exponent. Finite Fiels Appl. **54**, 101-112, (2018)

[25] Zheng, D., Wang, X., Hu, L., Zeng., X.: The weight distributions of two classes of $p$-ary cyclic codes. Finite Fields Appl. **29**, 202-224, (2014)

[26] Zheng, D., Wang, X., Zeng, X., Hu, L.: The weight distribution of a family of $p$-ary cyclic codes. Designs, Codes and Cryptography. **75** (2), 263-275, (2015)

[27] Zha Z., Hu L. New classes of optimal ternary cyclic codes with minimum distance four. Finite Fields Appl. **64**, 101671, (2020)

[28] Zhou, Z., Ding, C.: A class of three-weight cyclic codes. Finite Fields and Applications. **25** (10), 79-93, (2013)

[29] Zhou, Z., Ding, C.: Seven classes of three-weight cyclic codes. IEEE Trans. Inf. Theory. **61** (10), 4120-4126, (2013)

[30] Zhou, Z., Ding, C., Luo, J., Zhang, A.: A family of five-weight cyclic codes and their weight enumerators. IEEE Trans. Inf. Theory. **59** (10), 6674-6682, (2013)

Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, P. R. China
*E-mail address*: wangdan244567@163.com

Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, P. R. China, State Key Laboratory of Information Security Institute of Information Engineering, Chinese Academy of Sciences,, Beijing 100093, China
*E-mail address*: xwcao@nuaa.edu.cn