OPTIMAL TERNARY CYCLIC CODES WITH MINIMUM DISTANCE FOUR AND FIVE

Nian Li[*]   Chunlei Li [†]   Tor Helleseth[†]

Cunsheng Ding[‡]   Xiaohu Tang[*]

Cyclic codes are an important subclass of linear codes and have wide applications in data storage systems, communication systems and consumer electronics. In this paper, two families of optimal ternary cyclic codes are presented. The first family of cyclic codes has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ and contains a class of conjectured cyclic codes and several new classes of optimal cyclic codes. The second family of cyclic codes has parameters $[3^m - 1, 3^m - 2 - 2m, 5]$ and contains a number of classes of cyclic codes that are obtained from perfect nonlinear functions over $\mathbb{F}_{3^m}$, where $m > 1$ and is a positive integer.

1 Introduction

Throughout this paper let p and m be a prime and a positive integer respectively, and let $\mathbb{F}_{p^m}$ denote the finite field with p^m elements. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with

[*]Inf. Security and National Computing Grid Lab, Southwest Jiaotong Univ., Chengdu, China

[†]Department of Informatics, University of Bergen, PB 7803, N-5020 Bergen, Norway

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

minimum Hamming distance d, and is called *cyclic* if any cyclic shift of a codeword is another codeword of $\mathcal{C}$. By identifying $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ with

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_p[x]/(x^n - 1),$$

any cyclic code of length n over $\mathbb{F}_p$ corresponds to an ideal of the polynomial residue class ring $\mathbb{F}_p[x]/(x^n - 1)$. Note that every ideal of $\mathbb{F}_p[x]/(x^n - 1)$ is principal. Any cyclic code $\mathcal{C}$ can be expressed as $\mathcal{C} = \langle g(x) \rangle$, where $g(x)$ is monic and has the least degree. This polynomial $g(x)$ 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 are an important subclass of linear codes and have been extensively studied (see for example [1, 6, 7, 9, 10, 12, 14, 16, 17] for some recent developments). Let α be a generator of $\mathbb{F}_{3^m}^* = \mathbb{F}_{3^m} \setminus \{0\}$ and let $m_i(x)$ denote the minimal polynomial of α^i over $\mathbb{F}_3$. A class of cyclic codes $\mathcal{C}_{(1,e)}$ over $\mathbb{F}_3$ with generator polynomial $m_1(x)m_e(x)$, where $1 \leq e \leq 3^m - 1$ and e is not in the 3-cyclotomic coset modulo $3^m - 1$ containing 1, was investigated in [2] and [5]. Carlet, Ding and Yuan proved that the code $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ when x^e are certain perfect nonlinear (PN) monomials [2]. Employing some monomials x^e over $\mathbb{F}_{3^m}$, including almost perfect nonlinear (APN) monomials, Ding and Helleseth [5] obtained several classes of ternary cyclic codes with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ which are optimal according to the Sphere Packing bound. In addition, nine open problems about this kind of optimal ternary cyclic codes were proposed in [5]. Notably, as a class of subcodes of $\mathcal{C}_{(1,e)}$, the cyclic codes with generator polynomial $(x - 1)m_1(x)m_e(x)$, which are denoted by $\mathcal{C}_{(0,1,e)}$, is closely related to the linear code $\overline{\mathcal{C}}_\Pi$ investigated in [2] and [15], and it can be similarly proven as in [2] that $\mathcal{C}_{(0,1,e)}$ has parameters $[3^m - 1, 3^m - 2m - 2, 5]$ if x^e is PN.

In this paper, we will present a number of classes of new optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ and $[3^m - 1, 3^m - 2 - 2m, 5]$. We will first settle an open problem proposed in [5] and then construct several classes of new optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ using some monomials over $\mathbb{F}_{3^m}$. We then derive a number of classes of optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 2 - 2m, 5]$ by considering the subcodes of $\mathcal{C}_{(1,e)}$ with generator polynomial $(x + 1)m_1(x)m_e(x)$ over $\mathbb{F}_3$. Following the notations in [5], we denote by $\mathcal{C}_{(1,e,s)}$ the cyclic code with generator polynomial $(x + 1)m_1(x)m_e(x)$, where $s = \frac{3^m - 1}{2}$. It will be shown in

this paper that the ternary cyclic code $\mathcal{C}_{(1,e,s)}$ has parameters $[3^m - 1, 3^m - 2m - 2, 5]$ and is optimal for several classes of properly chosen integers e. The optimality of $\mathcal{C}_{(1,e,s)}$ is established by virtue of properties of PN functions over $\mathbb{F}_{3^m}$.

2 AUXILIARY RESULTS ABOUT CYCLOTOMIC COSETS, THE CODES $\mathcal{C}_{(1,e)}$ AND POLYNOMIALS

A function f from $\mathbb{F}_{p^m}$ to itself 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

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

In this paper we will need the notions of PN and APN functions [11, 18].

For a prime p, the p-cyclotomic coset modulo $p^m - 1$ containing j is defined as

$$C_j = \{jp^s \bmod (p^m - 1) : s = 0, 1, \cdots, m-1\}.$$

The following lemma will be frequently used in the sequel.

Lemma 1. ([5]) *For any $1 \leq e \leq p^m - 2$ with $\gcd(e, p^m - 1) = 2$, the length of the p-cyclotomic coset C_e is equal to m.*

Ding and Helleseth proved the following fundamental theorem about the ternary codes $\mathcal{C}_{(1,e)}$.

Theorem 1. ([5, Thm. 4.1]) *Let $e \notin C_1$ and $|C_e| = m$. The ternary cyclic code $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ if and only if the following conditions are satisfied:*

  C1: e is even;

  C2: the equation $(x+1)^e + x^e + 1 = 0$ has the only solution $x = 1$ in $\mathbb{F}_{3^m}$; and

  C3: the equation $(x+1)^e - x^e - 1 = 0$ has the only solution $x = 0$ in $\mathbb{F}_{3^m}$.

We shall need the following lemma in the sequel, in addition to Theorem 1.

Lemma 2. ([13, Thm. 2.14]) *Let q be a prime power and let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n. Then $f(x) = 0$ has a root x in $\mathbb{F}_{q^n}$. Furthermore, all the roots of $f(x) = 0$ are simple and are given by the n distinct elements $x, x^q, x^{q^2}, \cdots, x^{q^{n-1}}$ of $\mathbb{F}_{q^n}$.*

Let us take $f(x) = x^3 + x^2 + x - 1 \in \mathbb{F}_3[x]$ as an example to show how Lemma 2 works. Note that $f(0) = f(1) = 2 \neq 0$ and $f(2) = f(-1) = 1 \neq 0$. This means that $f(x) = x^3 + x^2 + x - 1$ is a cubic irreducible polynomial over $\mathbb{F}_3[x]$. Then by Lemma 2, $f(x) = 0$ has no solutions in $\mathbb{F}_{3^m}$ if and only if $m \not\equiv 0 \pmod 3$. This idea will be frequently employed in the sequel to prove some of the main results of this paper.

For any given $f(x) \in \mathbb{F}_3[x]$, if one factorizes $f(x)$ over $\mathbb{F}_3$, then the number of solutions of $f(x) = 0$ in $\mathbb{F}_{3^m}$ can be determined with Lemma 2. However, the factorization of a polynomial is normally a hard problem. In this paper, we mainly consider the cyclic code $\mathcal{C}_{(1,e)}$ for special values of e, where only low-degree polynomials over $\mathbb{F}_3[x]$ should be factorized. In fact, to apply Lemma 2, sometimes one only needs to know the degrees of the irreducible factors of $f(x)$.

The following lemmas are basic results about polynomials over finite fields and will be employed in the sequel.

Lemma 3. ([13]) *Let q be a prime power and $g(x)$ be a polynomial in $\mathbb{F}_q[x]$. Then for any $f(x) \in \mathbb{F}_q[x]$ there exist polynomials $h(x), r(x) \in \mathbb{F}_q[x]$ such that $f(x) = g(x)h(x) + r(x)$, where $\deg(r(x)) < \deg(g(x))$. Moreover, $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$.*

Lemma 4. ([13, Thm. 3.20]) *For every finite field $\mathbb{F}_q$ and every positive integer n, where q is a prime power, the product of all monic irreducible polynomials over $\mathbb{F}_q[x]$ whose degrees divide n is equal to $x^{q^n} - x$.*

For a given $f(x) \in \mathbb{F}_q[x]$ with low degree, Lemmas 3 and 4 can be used to determine the degrees of irreducible factors of $f(x)$. For example, let $f(x) = x^8 + x^7 - x^6 + x^4 - x^3 + x^2 - 1 \in \mathbb{F}_3[x]$. Applying Lemma 3, one gets that $\gcd(f(x), x^{3^3} - x) = 1$ and $\gcd(f(x), x^{3^4} - x) = x^2 + x - 1$. It then follows from Lemma 4 that $f(x)$ has the irreducible factor $x^2 + x - 1$ but no irreducible factor with degree equals to 1, 3 and 4. This implies that $f(x)$ has an irreducible factor with degree 6.

3 SOLVING AN OPEN PROBLEM ABOUT THE TERNARY CYCLIC CODES $\mathcal{C}_{(1,e)}$

With the preparations in Section 2, in this section we settle the following open problem proposed in [5]:

Open 1. ([5]) *Let $e = 2(3^{m-1} - 1)$. Does the ternary cyclic code $\mathcal{C}_{(1,e)}$ have parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ if $m \geq 5$ and m is prime?*

To solve this problem, we need to prove the following lemmas.

Lemma 5. *Let m be odd and $e = 2(3^{m-1} - 1)$. Then $|C_e| = m$ and $C_1 \cap C_e = \emptyset$.*

Proof. It is easily seen that $\gcd(e, 3^m - 1) = 2$. It then follows from Lemma 1 that $|C_e| = m$. Since both e and $3^m - 1$ are even, it is obvious that $C_1 \cap C_e = \emptyset$. This completes the proof. □

After proving Lemma 5, we now consider Conditions C2 and C3 in Theorem 1 for $e = 2(3^{m-1} - 1)$.

Lemma 6. *Let $e = 2(3^{m-1} - 1)$. Then Condition C2 in Theorem 1 is met if and only if $m \not\equiv 0 \pmod{3}$.*

Proof. Note that e is even and $x = 0$ is not a solution of $(-x - 1)^e + x^e + 1 = 0$. Then Condition C2 is satisfied if and only if $(x + 1)^e + x^e + 1 = 0$ has the only solution $x = 1$ in $\mathbb{F}_{3^m}$. Raising both sides of this equation to the power of 3 gives $(x + 1)^{3e} + x^{3e} + 1 = 0$. Note that $x \neq 0$, $x + 1 \neq 0$ and $3e = 2(3^m - 3) = 2(3^m - 1) - 4$. Then the equation $(x + 1)^e + x^e + 1 = 0$ is equivalent to $(x + 1)^{-4} + x^{-4} + 1 = 0$, i.e.,

$$(x + 1)^4 x^4 + (x + 1)^4 + x^4 = 0. \tag{1}$$

Denote $f(x) = (x + 1)^4 x^4 + (x + 1)^4 + x^4 = x^8 + x^7 + x^5 + x^3 + x + 1$. Applying Lemma 3, one gets that $\gcd(f(x), x^3 - x) = x - 1$, $\gcd(f(x), x^{3^2} - x) = x - 1$, and $\gcd(f(x), x^{3^3} - x) = x^7 - x^6 - x^5 + x^2 + x - 1$. It then follows from Lemma 4 and $\deg(f(x)) = 8$ that $f(x)$ has the two cubic irreducible factors $x^3 + x^2 + x + 2$ and $x^3 + 2x^2 + 2x + 2$ over $\mathbb{F}_3$ and the factor $(x - 1)^2$. Thus (1) has the only solution $x = 1$ in $\mathbb{F}_{3^m}$ if and only if $m \not\equiv 0 \pmod{3}$ by Lemma 2. This completes the proof. □

Lemma 7. *Let $e = 2(3^{m-1} - 1)$. Then Condition C3 in Theorem 1 is met if and only if m is odd and $m \not\equiv 0 \pmod{3}$.*

Proof. Let $x \in \mathbb{F}_{3^m}$ be a solution of $(x+1)^e - x^e - 1 = 0$. Then we have $(x+1)^{3e} - x^{3e} - 1 = 0$. Notice that $3e = 2(3^m - 3) = 2(3^m - 1) - 4$. Then $(x+1)^{3e} - x^{3e} - 1 = 0$ has the only solution $x = 0$ if and only if $(x+1)^{-4} - x^{-4} - 1 = 0$ has no solution in $\mathbb{F}_{3^m}^*$. Multiplying both sides of this equation with $x^4(x+1)^4$ gives

$$(x+1)^4 x^4 + (x+1)^4 - x^4 = 0. \tag{2}$$

Therefore Condition C3 is equivalent to showing that (2) has no solutions in $\mathbb{F}_{3^m}$. Denote $g(x) = (x+1)^4 x^4 + (x+1)^4 - x^4 = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$. By Lemma 3, we have $\gcd(g(x), x^3 - x) = 1$, $\gcd(g(x), x^{3^2} - x) = x^2 + 1$, and $\gcd(g(x), x^{3^3} - x) = x^6 + x^5 - x^4 - x^2 + x + 1$. It then follows from Lemma 4 that $g(x)$ has the irreducible factor $x^2 + 1$ and the two cubic irreducible factors $x^3 + 2x + 2$ and $x^3 + x^2 + 2$. Then the desired conclusion follows from Lemma 2. This completes the proof. □

The answer to Open Problem 1 is given in the following theorem.

Theorem 2. *Let m be odd, $m \not\equiv 0 \pmod 3$ and $e = 2(3^{m-1} - 1)$. Then the ternary cyclic code $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$.*

Proof. The conclusions follow from Lemmas 5-7 and Theorem 1. □

Example 1. *Let $m = 5$ and let α be the generator of $\mathbb{F}_{3^m}^*$ with $\alpha^5 + 2\alpha + 1 = 0$. Then the code $\mathcal{C}_{(1,e)}$ of Theorem 2 has parameters $[242, 232, 4]$ and generator polynomial $x^{10} + 2x^9 + x^8 + x^5 + x^4 + x^3 + 2x^2 + 2x + 2$.*

4 NEW OPTIMAL TERNARY CYCLIC CODES WITH PARAMETERS $[3^m - 1, 3^m - 1 - 2m, 4]$

Inspired by the idea for solving Open Problem 1, we construct new optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ using other monomials x^e over $\mathbb{F}_{3^m}$ in this section.

4.1 THE FIRST CLASS OF OPTIMAL TERNARY CYCLIC CODES WITH PARAMETERS $[3^m - 1, 3^m - 1 - 2m, 4]$

In this subsection, we consider the exponents e of the form $e = \frac{3^m - 1}{2} - r$, where r and m have the same parity. Denote the quadratic character of $\mathbb{F}_{3^m}$ by η which is defined by $\eta(0) = 0$, $\eta(x) = 1$ if x is a nonzero square in $\mathbb{F}_{3^m}$ and $\eta(x) = -1$ if x is a nonzero nonsquare in $\mathbb{F}_{3^m}$. Note

that e is even. Then Condition C2 in Theorem 1 is satisfied if and only if $(x+1)^e + x^e + 1 = 0$ has the only solution $x = 1$ in $\mathbb{F}_{3^m}$. With the quadratic character of $\mathbb{F}_{3^m}$, $(x+1)^e + x^e + 1 = 0$ can be written as $\eta(x+1)(x+1)^{-r} + \eta(x)x^{-r} + 1 = 0$. Multiplying with $x^r(x+1)^r$ both sides of this equation yields that

$$(x+1)^r x^r + \eta(x+1)x^r + \eta(x)(x+1)^r = 0. \tag{3}$$

Then C2 is satisfied if and only if (3) has the only solution $x = 1$ with $\eta(x(x+1)) \neq 0$ since neither $x = 0$ nor $x = -1$ are the solutions of $(x+1)^e + x^e + 1 = 0$. Similarly, one can conclude that C3 is satisfied if and only if

$$(x+1)^r x^r + \eta(x)(x+1)^r - \eta(x+1)x^r = 0 \tag{4}$$

has no solution x in $\mathbb{F}_{3^m}$ with $\eta(x(x+1)) \neq 0$.

The following theorem then follows from Theorem 1 and the foregoing discussions.

Theorem 3. *Let* $e = \frac{3^m-1}{2} - r$, $e \notin C_1$ *and* $|C_e| = m$, *where* r *and* m *have the same parity. Then the ternary cyclic code* $\mathcal{C}_{(1,e)}$ *has parameters* $[3^m - 1, 3^m - 1 - 2m, 4]$ *if* (3) *has the only solution* $x = 1$ *and* (4) *has no nonzero solution* x *in* $\mathbb{F}_{3^m}$ *with* $\eta(x(x+1)) \neq 0$.

As in Lemmas 6 and 7, the solutions of (3) and (4) can be similarly discussed for a given r.

Corollary 1. *Let* $m \equiv 2 \pmod 4$ *and* $e = \frac{3^m-1}{2} - 2$. *Then the ternary cyclic code* $\mathcal{C}_{(1,e)}$ *has parameters* $[3^m - 1, 3^m - 1 - 2m, 4]$.

Proof. Notice that $3^m - 1 \equiv 0 \pmod 8$ as m is even. It then follows that $e \equiv 2 \pmod 4$ and $\gcd(e, 3^m - 1) = \gcd(e, 4) = 2$. By Lemma 1 we have $|C_e| = m$. On the other hand, $e \notin C_1$ since e is even. For $r = 2$, we will discuss (3) by distinguishing among the following cases:

1. $(\eta(x), \eta(x+1)) = (1, 1)$: In this case, (3) is reduced to $x^4 - x^3 - x + 1 = (x-1)^4 = 0$, i.e., it has the only solution $x = 1$ since $\eta(1) = 1$ and $\eta(1+1) = \eta(-1) = 1$ for even m.

2. $(\eta(x), \eta(x+1)) = (1, -1)$: In this case, (3) is simplified to $x^4 - x^3 + x^2 - x + 1 = 0$. Applying Lemma 3, one obtains that $\gcd(x^4 - x^3 + x^2 - x + 1, x^{3^2} - x) = 1$, which implies that $x^4 - x^3 + x^2 - x + 1$ has no irreducible factors of degrees 1 and 2 by Lemma 4. Therefore $x^4 - x^3 + x^2 - x + 1$ is irreducible over $\mathbb{F}_3$.

3. $(\eta(x), \eta(x+1)) = (-1, 1)$: Similar as in Case 2), in this case (3) is reduced to $x^4 - x^3 + x^2 + x - 1 = 0$, which is irreducible over $\mathbb{F}_3$.

4. $(\eta(x), \eta(x+1)) = (-1, -1)$: In this case one can similarly prove that $x^4 - x^3 - x^2 + x - 1$ is irreducible over $\mathbb{F}_3$.

Therefore, by Lemma 2, (3) has the only solution $x = 1$ if $m \equiv 2$ (mod 4). It can be similarly proved that (4) has no solution x in $\mathbb{F}_{3^m}$ with $\eta(x(x+1)) \neq 0$. Then the desired conclusions follow from Theorem 3. This completes the proof. $\qquad\square$

Example 2. *Let $m = 6$ and let α be the generator of $\mathbb{F}_{3^m}^*$ with $\alpha^6 + 2\alpha^4 + \alpha^2 + 2\alpha + 2$. Then the code $\mathcal{C}_{(1,e)}$ of Corollary 1 has parameters $[728, 716, 4]$ and generator polynomial $x^{12} + 2x^{10} + x^9 + x^8 + 2x^5 + x^4 + x^3 + 2x^2 + 2$.*

Notice that $e = \frac{3^m - 1}{2} - 1 = \frac{3^m - 3}{2}$ and $e = \frac{3^m - 1}{2} - 3 \equiv 3 \cdot (\frac{3^m - 1}{2} - 1)$ (mod $3^m - 1$), i.e., the two cases that $r = 1$ and $r = 3$ are covered by Theorem 6.1 in [5] since $x^{\frac{3^m - 3}{2}}$ is an almost perfect nonlinear function in $\mathbb{F}_{3^m}$ if $m \geq 5$ and m is odd [11]. In the following, we consider the case that $r = 5$.

Corollary 2. *Let m be odd and $e = \frac{3^m - 1}{2} - 5$. Then the ternary cyclic code $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$.*

Proof. Since $\gcd((3^m - 1)/2, 5) = 1$ for odd m, $\gcd(3^m - 1, e) = \gcd(e, 10) = 2$. It then follows from Lemma 1 that $|C_e| = m$. Since e is even, $e \notin C_1$. For $r = 5$, we below discuss only the solution x of (3) with $\eta(x(x+1)) \neq 0$ since that of (4) can be dealt with in the same manner.

1. $(\eta(x), \eta(x+1)) = (1, 1)$: In this case, (3) is reduced to $f(x) = x^{10} - x^9 + x^8 + x^7 - x^6 - x^4 + x^3 + x^2 - x + 1 = 0$. Applying Lemma 3, one obtains that $\gcd(f(x), x^{3^i} - x) = 1$ for all $i \in \{1, 2, 3, 4, 5\}$. It then follows from Lemma 4 that $f(x)$ is irreducible over $\mathbb{F}_3$.

2. $(\eta(x), \eta(x+1)) = (1, -1)$: In this case (3) becomes $f(x) = x^{10} - x^9 + x^8 + x^7 - x^6 + x^5 - x^4 + x^3 + x^2 - x + 1 = 0$. Applying Lemma 3 one gets that $\gcd(f(x), x^3 - x) = x - 1$, $\gcd(f(x), x^{3^2} - x) = x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$ and $\gcd(f(x), x^{3^3} - x) = x - 1$. It then follows from Lemma 4 that $f(x)$ has the factor $(x - 1)^4$ and three quadratic irreducible factors (they are $x^2 + 1$, $x^2 + x + 2$ and $x^2 + 2x + 2$). When m is odd, $\eta(1) = 1$ and $\eta(1 + 1) = \eta(-1) = -1$, i.e., $x = 1$ is indeed a solution of (3).

3. $(\eta(x), \eta(x+1)) = (-1, 1)$: In this case (3) is reduced to $f(x) = x^{10} - x^9 + x^8 + x^7 - x^6 + x^5 + x^4 - x^3 - x^2 + x - 1 = 0$. Similar as in Case 1), one can prove that $f(x)$ is irreducible over $\mathbb{F}_3$.

4. $(\eta(x), \eta(x+1)) = (-1, -1)$: In this case one can similarly prove that $x^{10} - x^9 + x^8 + x^7 - x^6 - x^5 + x^4 - x^3 - x^2 + x - 1$ is irreducible over $\mathbb{F}_3$.

Since m is odd, $m \not\equiv 0 \pmod{10}$. It then follows from Lemma 2 that (3) has the only solution $x = 1$ in $\mathbb{F}_{3^m}$ with $\eta(x(x+1)) \neq 0$. Then the desired conclusions follow from Theorem 3. This completes the proof. □

Example 3. *Let $m = 5$ and let α be the generator of $\mathbb{F}_{3^m}^*$ with $\alpha^5 + 2\alpha + 1 = 0$. Then the code $\mathcal{C}_{(1,e)}$ of Corollary 2 has parameters $[242, 232, 4]$ and generator polynomial $x^{10} + 2x^9 + x^8 + 2x^7 + x^6 + x^5 + x^4 + 2x^3 + 2$.*

Remark 1. *By Lemmas 3 and 4, more new optimal ternary codes can also be obtained from other values of r, for example, $r = 7, 10, 11$. It should be noted that $e = \frac{3^m - 15}{2}$ if $r = 7$, which is equivalent to $e = \frac{3^{m-1} - 5}{2}$. This is a special case of Open Problem 7.10 in [5].*

4.2 THE SECOND CLASS OF OPTIMAL TERNARY CYCLIC CODES WITH PARAMETERS $[3^m - 1, 3^m - 1 - 2m, 4]$

The ternary cyclic code $\mathcal{C}_{(1,e)}$ for $e = \frac{3^m - 1}{2} + r$, where r and m have the same parity, is considered in this subsection. With similar discussions for (3) and (4) conducted in the preceding subsection, one can prove the following theorem with Theorem 1.

Theorem 4. *Let $e = \frac{3^m - 1}{2} + r$, $e \notin C_1$ and $|C_e| = m$, where r and m have the same parity. Then the ternary cyclic code $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ if*

$$\eta(x+1)(x+1)^r + \eta(x)x^r + 1 = 0 \tag{5}$$

has the only solution $x = 1$ in $\mathbb{F}_{3^m}$ and

$$\eta(x+1)(x+1)^r - \eta(x)x^r - 1 = 0 \tag{6}$$

has no nonzero solution in $\mathbb{F}_{3^m}$.

Using Theorem 4, one can verify that $\mathcal{C}_{(1,e)}$ with $e = \frac{3^m - 1}{2} + r$ for $r \in \{1, 2, \cdots, 6\}$ either is not optimal or has been treated in [5]. Thus we start with $r = 7$ below.

Corollary 3. *Let m be odd and* $e = \frac{3^m-1}{2} + 7$. *Then the ternary cyclic code* $\mathcal{C}_{(1,e)}$ *has parameters* $[3^m - 1, 3^m - 1 - 2m, 4]$.

Proof. Since m is odd, e is even. Thus $e \notin C_1$. It is easily verified that $e \equiv 2 \pmod 3$ and $\gcd(\frac{3^m-1}{2}, 7) = 1$. Hence $\gcd(e, 3^m - 1) = \gcd(e, 14) = 2$. It then follows from Lemma 1 that $|C_e| = m$. In what follows, we prove that (5) has the only solution $x = 1$ in $\mathbb{F}_{3^m}$ for $r = 7$. This is done by distinguishing among the following cases:

1. $(\eta(x), \eta(x+1)) = (1, 1)$: In this case, (5) is reduced to $f(x) = 2x^7 + x^6 + 2x^4 + 2x^3 + x + 2 = 0$. It is easily checked that $\gcd(f(x), x^{3^2} - x) = (x + 1)(x^2 + 1)$. By Lemma 4, $f(x)$ has the factor $(x + 1)(x^2 + 1)$ and an irreducible factor of degree 4 (i.e., $x^4 + x^3 + x^2 + x + 1$). Note that $x = -1$ is not a solution of (5).

2. $(\eta(x), \eta(x+1)) = (1, -1)$: In this case (5) is simplified to $f(x) = 2x^6 + x^4 + x^3 + 2x = 0$. It is easily verified that $f(x) = x(x + 1)(x - 1)^4$. Note that $x = 1$ is indeed a solution of (5) since $\eta(1 + 1) = \eta(-1) = -1$ for odd m.

3. $(\eta(x), \eta(x+1)) = (-1, 1)$: In this case, (5) is reduced to $f(x) = x^6 + 2x^4 + 2x^3 + x + 2 = 0$. Similar as in Case 1), one can prove that $f(x)$ has the irreducible factor $x^2 + x + 2$ and the irreducible factor $x^4 + 2x^3 + x^2 + 1$ over $\mathbb{F}_3$.

4. $(\eta(x), \eta(x+1)) = (-1, -1)$: In this case one can also similarly prove that $x^7 + 2x^6 + x^4 + x^3 + 2x = x(x^2 + 2x + 2)(x^4 + x^2 + 2x + 1)$ which is the canonical factorization of $x^7 + 2x^6 + x^4 + x^3 + 2x$ over $\mathbb{F}_3$.

Since m is odd, $m \not\equiv 0 \pmod 4$. By Lemma 2, (5) has the only solution $x = 1$ in $\mathbb{F}_{3^m}$ if m is odd. The statement that (6) has no nonzero solution in $\mathbb{F}_{3^m}$ can be similarly proven for odd m. The desired conclusions then follow from Theorem 4. This completes the proof. $\square$

Example 4. *Let* $m = 5$ *and let* α *be the generator of* $\mathbb{F}_{3^m}^*$ *with* $\alpha^5 + 2\alpha + 1 = 0$. *Then the code* $\mathcal{C}_{(1,e)}$ *of Corollary 3 has parameters* $[242, 232, 4]$ *and generator polynomial* $x^{10} + 2x^8 + 2x^7 + 2x^6 + x^4 + 2x^2 + x + 2$.

As an example for even m, we prove the following corollary.

Corollary 4. *Let* $m \equiv 2 \pmod 4$ *and* $e = \frac{3^m-1}{2} + 10$. *Then the ternary cyclic code* $\mathcal{C}_{(1,e)}$ *has parameters* $[3^m - 1, 3^m - 1 - 2m, 4]$.

Proof. Clearly e is even. Hence $e \notin C_1$. It follows from $m \equiv 2 \pmod 4$ that $3^m - 1 \equiv 0 \pmod 8$ and $\gcd(3^m - 1, 5) = 1$. Therefore $e \equiv 2 \pmod 4$ and $\gcd(3^m - 1, e) = \gcd(e, 20) = \gcd(e, 4) = 2$. This leads to $|C_e| = m$ according to Lemma 1. For $r = 10$, we discuss (5) by considering the following cases:

1. $(\eta(x), \eta(x+1)) = (1, 1)$: In this case, (5) is reduced to $2x^{10} + x^9 + x + 2 = 2(x-1)^{10} = 0$ which has the only solution $x = 1$.

2. $(\eta(x), \eta(x+1)) = (1, -1)$: In this case (5) is simplified to $2x(x^8 + 1) = 0$. It is easily verified that $\gcd(x^8 + 1, x^{3^i} - x) = 1$ for all $i \in \{1, 2, 3\}$. It then follows from Lemma 4 that $x^8 + 1$ has no irreducible factor with degrees 1, 2 and 3. This implies that $x^8 + 1$ either is irreducible or has two irreducible factors of degree 4. In fact, the canonical factorization of $x^8 + 1$ over $\mathbb{F}_3$ is $x^8 + 1 = (x^4 + x^2 + 2)(x^4 + 2x^2 + 2)$. Note that $x = 0$ is not a solution of (5).

3. $(\eta(x), \eta(x+1)) = (-1, 1)$: In this case (5) is reduced to $x^9 + x + 2 = 0$. It is straightforward to verify that $\gcd(x^9 + x - 1, x^{3^i} - x) = x + 1$ for all $i \in \{1, 2, 3\}$. It then follows from Lemma 4 that $\frac{x^9 + x - 1}{x+1}$ either is irreducible or has two irreducible factors of degree 4. In fact, the canonical factorization of $\frac{x^9 + x - 1}{x+1}$ over $\mathbb{F}_3$ is given by $\frac{x^9 + x - 1}{x+1} = (x^4 + x^3 + x^2 + 1)(x^4 + x^3 + 2x^2 + 2x + 2)$. Clearly, $x = -1$ is not a solution of (5).

4. $(\eta(x), \eta(x+1)) = (-1, -1)$: In this case one can similarly prove that $x^{10} + 2x^9 + 2x$ has either two irreducible factors of degree 4 or one irreducible factor of degree 8. In fact, the canonical factorization of $x^{10} + 2x^9 + 2x$ over $\mathbb{F}_3$ is given by $x^{10} + 2x^9 + 2x = x(x+1)(x^4 + x^2 + x + 1)(x^4 + x^3 + x^2 + 2x + 2)$.

It then follows from Lemma 2 that (5) has the unique solution $x = 1$ in $\mathbb{F}_{3^m}$ if $m \equiv 2 \pmod 4$. One can similarly prove that (6) has no solution in $\mathbb{F}_{3^m}^*$ if $m \equiv 2 \pmod 4$. Then the desired conclusions follow from Theorem 4. This completes the proof. $\qquad\square$

With the same technique above, one can derive conditions on m such that the ternary cyclic code $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ for $r \in \{11, 13, 14, \cdots, 20\}$.

Example 5. *Let* $m = 6$ *and let* α *be the generator of* $\mathbb{F}_{3^m}^*$ *with* $\alpha^6 + 2\alpha^4 + \alpha^2 + 2\alpha + 2$. *Then the code* $\mathcal{C}_{(1,e)}$ *of Corollary 4 has parameters* $[728, 716, 4]$ *and generator polynomial* $x^{12} + x^{11} + 2x^{10} + 2x^9 + 2x^8 + x^7 + x^6 + x^5 + 2x^2 + x + 2$.

4.3 THE THIRD CLASS OF OPTIMAL TERNARY CYCLIC CODES WITH PARAMETERS $[3^m - 1, 3^m - 1 - 2m, 4]$

A class of ternary cyclic codes $\mathcal{C}_{(1,e)}$, where $e = 3^m - 1 - 2r \equiv -2r$ (mod $3^m - 1$), is investigated in this subsection. Note that e is in the same 3-cyclotomic class with $r(3^{m-1} - 1)$ since $3r(3^{m-1} - 1) = r(3^m - 3) \equiv -2r$ (mod $3^m - 1$).

Clearly, e is even. Hence $x = 0$ and $x = -1$ are not solutions of $(-x - 1)^e + x^e + 1 = 0$. Thus Condition C2 is satisfied if and only if $(x + 1)^{-2r} + x^{-2r} + 1 = 0$, i.e.,

$$(x + 1)^{2r}x^{2r} + (x + 1)^{2r} + x^{2r} = 0 \tag{7}$$

has the only solution $x = 1$ in $\mathbb{F}_{3^m}$. Similarly, C3 is satisfied if and only if

$$(x + 1)^{2r}x^{2r} + (x + 1)^{2r} - x^{2r} = 0 \tag{8}$$

has no solution x in $\mathbb{F}_{3^m}$.

The following theorem then follows from Theorem 1 and the preceding discussions.

Theorem 5. *Let* $e = r(3^{m-1} - 1)$, $e \notin C_1$ *and* $|C_e| = m$. *Then the ternary cyclic code* $\mathcal{C}_{(1,e)}$ *has parameters* $[3^m - 1, 3^m - 1 - 2m, 4]$ *if (7) has the only solution* $x = 1$ *and (8) has no solution in* $\mathbb{F}_{3^m}$.

The two cases that $r = 1$ and $r = 3$ are covered by Theorem 6.1 in [5] since $x^{3^{m-1}-1}$ is an almost perfect nonlinear function on $\mathbb{F}_{3^m}$ if m is odd. For $r = 2$, this is Open Problem 1, which was settled before. When $r = 4$ it is equivalent to $e = 3^{m-2} - 1$ which was discussed in Theorem 7.6 in [5]. Thus, as another example, we consider the case $r = 5$.

Corollary 5. *Let* m *be odd,* $m \not\equiv 0$ (mod 3) *and* $e = 5(3^{m-1} - 1) \equiv 2(3^{m-1} - 2)$ (mod $3^m - 1$). *Then the ternary cyclic code* $\mathcal{C}_{(1,e)}$ *has parameters* $[3^m - 1, 3^m - 1 - 2m, 4]$.

Proof. Since e is even, $e \notin C_1$. It is easily seen that $\gcd(e, 3^m - 1) = 2$. Then it follows from Lemma 1 that $|C_e| = m$. When $r = 5$, (7) is reduced to $f(x) = (x + 1)^{10}x^{10} + (x + 1)^{10} + x^{10} = x^{20} + x^{19} + x^{11} +$

$x^9 + x + 1$. By Lemma 3, one can derive that $\gcd(f(x), x^3 - x) = x - 1$, $\gcd(f(x), x^{3^3} - x) = x^7 - x^6 - x^5 + x^2 + x - 1$ and $\gcd(f(x), x^{3^5} - x) = x - 1$. This together with Lemma 4 implies that $f(x)$ has two cubic irreducible factors and has no irreducible factor of degree 5. Hence, one can claim that $f(x)$ has no other irreducible factor with odd degree due to the facts $(x - 1)^2 | f(x)$ and $\deg(f(x)) = 20$. In fact, the canonical factorization of $f(x)$ over $\mathbb{F}_3$ is given by $f(x) = (x - 1)^2(x^3 + x^2 + x + 2)(x^3 + 2x^2 + 2x + 2)(x^6 + x^5 + 2x^3 + x^2 + 2x + 1)(x^6 + 2x^5 + x^4 + 2x^3 + x + 1)$. Then by Lemma 2, $f(x) = 0$ has the only solution $x = 1$ in $\mathbb{F}_{3^m}$ if m is odd and $m \not\equiv 0 \pmod 3$.

Similarly, one can prove that (8) has no solution x in $\mathbb{F}_{3^m}$. When $r = 5$, (8) is simplified to $g(x) = x^{20} + x^{19} + x^{11} + x^{10} + x^9 + x + 1 = 0$. It is straightforward to check that

$$\gcd(g(x), x^3 - x) = \gcd(g(x), x^{3^2} - x) = 1,$$
$$\gcd(g(x), x^{3^3} - x) = x^6 + x^5 - x^4 - x^2 + x + 1,$$
$$\gcd(g(x), x^{3^4} - x) = x^8 - x^7 + x^6 + x^5 + x^4 + x^3 + x^2 - x + 1.$$

It then follows from Lemma 4 that $g(x)$ has two cubic irreducible factors and two irreducible factors of degree 4. This implies that $g(x)$ has no other irreducible factors with odd degree. In fact, the canonical factorization of $g(x)$ over $\mathbb{F}_3$ is given by $g(x) = (x^3 + 2x + 2)(x^3 + x^2 + 2)(x^4 + x^3 + x^2 + 2x + 2)(x^4 + x^3 + 2x^2 + 2x + 2)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$. Thus, (8) has no solution x in $\mathbb{F}_{3^m}$ if $m \not\equiv 0 \pmod 3$ and $m \not\equiv 0 \pmod 4$. Then the desired conclusions follow from Theorem 5. This completes the proof. $\square$

Example 6. *Let $m = 5$ and let α be the generator of $\mathbb{F}_{3^m}^*$ with $\alpha^5 + 2\alpha + 1 = 0$. Then the code $\mathcal{C}_{(1,e)}$ of Corollary 5 has parameters $[242, 232, 4]$ and generator polynomial $x^{10} + x^9 + x^7 + x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + 2$.*

4.4 TWO MORE CLASSES OF OPTIMAL TERNARY CYCLIC CODES WITH PARAMETERS $[3^m - 1, 3^m - 1 - 2m, 4]$

In this subsection we treat small integers e such that the ternary cyclic code $\mathcal{C}_{(1,e)}$ is optimal. Specifically, we consider the ternary cyclic codes $\mathcal{C}_{(1,e)}$, where $e = 2r$ and $1 \le r \le 10$. Most of them were studied in [2] and [5]:

1. When $e \in \{2, 6, 18\}$, the code is covered by Theorem 5.2 in [5] since they lie in the same 3-cyclotomic coset and x^2 is a planar function over $\mathbb{F}_{3^m}$.

2. When $e \in \{4, 12\}$, the code is covered by Theorem 5.2 in [5] since 4 and 12 are in the same 3-cyclotomic coset and x^{3^h+1} is a planar function over $\mathbb{F}_{3^m}$ if $m/\gcd(m, h)$ is odd.

3. When $e = 8$, the code is covered by Theorem 7.6 in [5] since e can be written as $e = 3^2 - 1$.

4. When $e = 10$, the code is covered by Theorem 5.2 in [5] since x^{3^h+1} is a planar function over $\mathbb{F}_{3^m}$ if $m/\gcd(m, h)$ is odd.

5. When $e = 14$, the code is covered by Theorem 5.2 in [5] since $x^{\frac{3^h+1}{2}}$ is a planar function over $\mathbb{F}_{3^m}$ if $\gcd(m, h) = 1$ and h is odd.

Thus, the remaining cases are $e = 16$ and $e = 20$. In what follows, we investigate the two codes $\mathcal{C}_{(1,16)}$ and $\mathcal{C}_{(1,20)}$

Corollary 6. *Let m be odd and $m \not\equiv 0 \pmod 3$. Then the ternary cyclic code $\mathcal{C}_{(1,16)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$.*

Proof. Clearly $e = 16 \notin C_1$. Note that $3^m - 1 \equiv 2 \pmod 4$ as m is odd. We have obviously that $\gcd(16, 3^m - 1) = 2$. It then follows from Lemma 1 that $|C_e| = m$. The condition C2 is met for $e = 16$ if and only if $(x+1)^{16} + x^{16} + 1 = 0$ has the only solution $x = 1$ in $\mathbb{F}_{3^m}$. Note that

$$\frac{(x+1)^{16} + x^{16} + 1}{(x-1)^4} = -(x^{12} - x^9 - x^8 - x^7 - x^5 - x^4 - x^3 + 1).$$

It suffices to prove that

$$f(x) := x^{12} - x^9 - x^8 - x^7 - x^5 - x^4 - x^3 + 1 = 0 \qquad (9)$$

has no solution in $\mathbb{F}_{3^m}$. It is straightforward to obtain that $\gcd(f(x), x^3 - x) = 1$, $\gcd(f(x), x^{3^2} - x) = x^6 + x^4 + x^2 + 1$ and $\gcd(f(x), x^{3^3} - x) = x^6 - x^4 - x^3 - x^2 + 1$. It then follows from Lemma 4 that $f(x)$ has three quadratic irreducible factors and two cubic irreducible factors. In fact, the canonical factorization of $f(x)$ over $\mathbb{F}_3$ is given by $f(x) = (x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)(x^3 + x^2 + x + 2)(x^3 + 2x^2 + 2x + 2)$. Hence (9) has no solution in $\mathbb{F}_{3^m}$ if and only if m is odd and $m \not\equiv 0 \pmod 3$.

Condition C3 can be similarly treated. Condition C3 is satisfied for $e = 16$ if and only if $(x+1)^{16} - x^{16} - 1 = 0$ has the only solution $x = 0$ in $\mathbb{F}_{3^m}$. Note that

$$(x+1)^{16} - x^{16} - 1 = x(x^{14} - x^{12} - x^{11} + x^9 + x^8 + x^6 + x^5 - x^3 - x^2 + 1).$$

We need to prove that

$$g(x) := x^{14} - x^{12} - x^{11} + x^9 + x^8 + x^6 + x^5 - x^3 - x^2 + 1 = 0 \quad (10)$$

has no solution in $\mathbb{F}_{3^m}$. One can verify that $\gcd(g(x), x^3 - x) = 1$, $\gcd(g(x), x^{3^2} - x) = 1$ and $\gcd(g(x), x^{3^3} - x) = x^6 + x^5 - x^4 - x^2 + x + 1$. It then follows from Lemma 4 that $g(x)$ has two cubic irreducible factors and $g(x) / \gcd(g(x), x^{3^3} - x)$ either is irreducible or has two irreducible factors of degree 4. In fact, the canonical factorization of $g(x)$ over $\mathbb{F}_3$ is given by $g(x) = (x^3 + 2x + 2)(x^3 + x^2 + 2)(x^8 + 2x^7 + x^6 + 2x^4 + x^2 + 2x + 1)$. Thus (10) has no solution in $\mathbb{F}_{3^m}$ if m is odd and $m \not\equiv 0 \pmod 3$. Then the desired conclusions follow from Theorem 1. This completes the proof. $\square$

Example 7. *Let $m = 5$ and let α be the generator of $\mathbb{F}_{3^m}^*$ with $\alpha^5 + 2\alpha + 1 = 0$. Then the code $\mathcal{C}_{(1,e)}$ of Corollary 6 has parameters $[242, 232, 4]$ and generator polynomial $x^{10} + 2x^9 + x^8 + x^7 + x^5 + x^4 + 2x + 2$.*

Corollary 7. *Let m be odd. Then the ternary cyclic code $\mathcal{C}_{(1,20)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$.*

Proof. Since $e = 20$ is even, $e \notin C_1$. We have that $\gcd(3^m - 1, 20) = \gcd(3^m - 1, 4) = 2$ as m is odd. It then follows from Lemma 1 that $|C_e| = |C_{20}| = m$. Conditions C2 and C3 are met if and only if both $f(x) = [(x+1)^{20} + x^{20} + 1]/(x-1)^2 = 2(x^{18} + x^{16} - x^{15} + x^{13} - x^{12} + x^{10} + x^8 - x^6 + x^5 - x^3 + x^2 + 1)$ and $g(x) = [(x+1)^{20} - x^{20} - 1]/x = 2(x^{18} - x^{17} + x^{10} - x^9 + x^8 - x + 1)$ have no solution in $\mathbb{F}_{3^m}$. By Lemma 2, it is sufficient to prove that both $f(x)$ and $g(x)$ have no irreducible factors with odd degree.

Applying Lemma 3, one obtains that

$$\gcd(f(x), x^{3^2} - x) = 1, \gcd(f(x), x^{3^4} - x) = 1, \gcd(f(x), x^{3^6} - x) = 2f(x),$$

i.e., $f(x)$ has three irreducible factors of degree 6. Then $f(x) = 0$ has no solution in $\mathbb{F}_{3^m}$ if and only if $m \not\equiv 0 \pmod 6$ due to Lemma 2. For $g(x)$, one has that $\gcd(g(x), x^{3^2} - x) = x^2 + 1$ and $\gcd(g(x), x^{3^4} - x) = $

$x^6 + x^5 - x^4 - x^3 - x^2 + x + 1$. It then follows from Lemma 2 that $g(x)$ has the irreducible factor $x^2 + 1$ and an irreducible factor of degree 4. Moreover, Lemma 4 implies that $g(x) / \gcd(g(x), x^{3^4} - x)$ whose degree equals to 12 has no irreducible factors with odd degree since $\gcd(g(x), x^{3^3} - x) = 1$ and $\gcd(g(x), x^{3^5} - x) = 1$. Thus, by Lemma 2, $g(x) = 0$ has no solution in $\mathbb{F}_{3^m}$ if m is odd. Then the desired conclusions follow from Theorem 1. This completes the proof. □

Remark 2. *The value $e = 20$ is a special case of Open Problem 7.5 in [5].*

Example 8. *Let $m = 5$ and let α be the generator of $\mathbb{F}_{3^m}^*$ with $\alpha^5 + 2\alpha + 1 = 0$. Then the code $\mathcal{C}_{(1,e)}$ of Corollary 7 has parameters $[242, 232, 4]$ and generator polynomial $x^{10} + 2x^8 + x^7 + x^4 + x^3 + 2x + 2$.*

It should be noticed that some larger values of r for $e = \frac{3^m - 1}{2} \pm r$, $e = r(3^{m-1} - 1)$ and $e = 2r$ such that $\mathcal{C}_{(1,e)}$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ can also be obtained with the same techniques by virtue of the division algorithm given in Lemma 3. Moreover, in each of the eight remaining open problems in [5], the cases of $h = 0, 1, 2, 3$ and $h = m - 1, m - 2, m - 3$ can also be settled. For the general case, new techniques are required.

5 NEW OPTIMAL TERNARY CYCLIC CODES WITH PARAMETERS $[3^m - 1, 3^m - 2m - 2, 5]$

Throughout this section, let $m > 1$ be an integer, $s = \frac{3^m - 1}{2}$, α be a generator of $\mathbb{F}_{3^m}^*$ and $\mathcal{C}_{(1,e,s)}$ be the cyclic code with generator polynomial $(x + 1)m_1(x)m_e(x)$, where $m_i(x)$ denotes the minimal polynomial of α^i over $\mathbb{F}_3$.

The code $\mathcal{C}_{(1,e,s)}$ is a $[3^m - 1, 3^m - 2m - 2]$ cyclic code if the size of C_e is equal to m, i.e., $|C_e| = m$. A tight upper bound on the minimum distance of $\mathcal{C}_{(1,e,s)}$ can be derived from the following bound on linear codes.

Lemma 8. *([8, Lemma 6]) 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 $q \geq 3$, $t = n - d + 1$ and $r = \lfloor \min\{\frac{n-t}{2}, \frac{t-1}{q-2}\} \rfloor$, then*

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

Theorem 6. *For any given e with $|C_e| = m$, the minimum distance of $\mathcal{C}_{(1,e,s)}$ satisfies $d \leq 5$.*

Proof. Clearly, $\mathcal{C}_{(1,e,s)}$ has length $3^m - 1$ and dimension $3^m - 2m - 2$ if $|C_e| = m$. It follows from the Sphere Packing bound that the minimum distance d of $\mathcal{C}_{(1,e,s)}$ satisfies $d \leq 6$. It then suffices to show there is no ternary code with parameters $[3^m - 1, 3^m - 2m - 2, 6]$.

Assume that there exists a ternary code with parameters $[3^m - 2m - 2, 6]$. Then applying Lemma 8 to this code, we have $q = 3$, $n = 3^m - 1$, $t = n - d + 1 = 3^m - 6$, $r = 2$, $t + 2r = 3^m - 2$, $\sum_{i=0}^{r} \binom{t+2r}{i}(q - 1)^i = 1 + 2(3^m - 2)^2$, and

$$3^{3^m - 2m - 2} \leq A_3(3^m - 1, 6) \leq \frac{3^{3^m - 2}}{1 + 2(3^m - 2)^2}$$

which implies $1 + 2(3^m - 2)^2 \leq 3^{2m}$, i.e., $(3^m - 4)^2 \leq 7$, a contradiction is obtained if $m > 1$. This completes the proof. $\qquad \square$

Theorem 6 indicates that $\mathcal{C}_{(1,e,s)}$ is optimal if it has parameters $[3^m - 1, 3^m - 2m - 2, 5]$. Thus, for any given e, in order to obtain optimal ternary cyclic code $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$, we need to show that $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weights $\omega \in \{1, 2, 3, 4\}$. By the definition of $\mathcal{C}_{(1,e,s)}$, it has a codeword of Hamming weight ω if and only if there exist ω nonzero elements $c_1, c_2, \cdots, c_\omega$ in $\mathbb{F}_3$ and ω nonzero distinct elements $x_1, x_2, \cdots, x_\omega$ in $\mathbb{F}_{3^m}$ such that

$$\begin{cases} c_1 x_1 + c_2 x_2 + \cdots + c_\omega x_\omega = 0 \\ c_1 x_1^e + c_2 x_2^e + \cdots + c_\omega x_\omega^e = 0 \\ c_1 x_1^s + c_2 x_2^s + \cdots + c_\omega x_\omega^s = 0. \end{cases} \tag{11}$$

Clearly, (11) cannot hold for $\omega = 1$. If $\omega = 2$, then one has $c_1 = c_2$ since $x_1 \neq x_2$. This implies $0 = c_1 x_1^e + c_2 x_2^e = c_1(x_1^e + (-x_1)^e)$ and $0 = c_1 x_1^s + c_2 x_2^s = c_1(x_1^s + (-x_1)^s)$, i.e., $\omega \neq 2$ if and only if either e is even or s is even. Note that $s = \frac{3^m - 1}{2}$ is even only if m is even.

To consider the codewords in $\mathcal{C}_{(1,e,s)}$ with Hamming weights $\omega = 3$ and $\omega = 4$, it is more convenient to write (11) as

$$\begin{cases} 1 + \frac{c_2 x_2}{c_1 x_1} + \cdots + \frac{c_\omega x_\omega}{c_1 x_1} = 0 \\ 1 + \frac{c_2 x_2^e}{c_1 x_1^e} + \cdots + \frac{c_\omega x_\omega^e}{c_1 x_1^e} = 0 \\ 1 + \frac{c_2 x_2^s}{c_1 x_1^s} + \cdots + \frac{c_\omega x_\omega^s}{c_1 x_1^s} = 0. \end{cases} \tag{12}$$

In the subsequent subsections, by discussing the solutions of (12) for $\omega = 3$ and $\omega = 4$ for a given e, new optimal ternary cyclic codes $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ will be obtained.

5.1 NEW OPTIMAL DOUBLE-ERROR-CORRECTING TERNARY CYCLIC CODES FOR EVEN m

In this subsection, new optimal ternary cyclic codes $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ will be obtained from the exponent e of the form

$$e = \frac{3^m - 1}{2} + r, \quad 1 \leq r \leq 3^m - 2, \tag{13}$$

where x^r is PN over $\mathbb{F}_{3^m}$.

By definition, a function from $\mathbb{F}_{3^m}$ to itself is PN if and only if

$$\begin{cases} x - y = a \\ f(x) - f(y) = b \end{cases} \tag{14}$$

has a unique solution $(x, y) \in \mathbb{F}_{3^m} \times \mathbb{F}_{3^m}$ for each $(a, b) \in \mathbb{F}_{3^m}^* \times \mathbb{F}_{3^m}$.

The following is a list of known PN monomials over $\mathbb{F}_{3^m}$:

- $f(x) = x^2$;

- $f(x) = x^{3^h + 1}$, where $m / \gcd(m, h)$ is odd [4];

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

It is known that r must be even if x^r is PN over $\mathbb{F}_{3^m}$. This fact will be frequently used in subsequent proofs. If m is odd and x^r is PN over $\mathbb{F}_{3^m}$, then the integer e of (13) must be odd as $\frac{3^m - 1}{2}$ is odd. In this case the minimum distance d of $\mathcal{C}_{(1,e,s)}$ is 2. Hence throughout this section we assume that m is even and x^r is PN over $\mathbb{F}_{3^m}$. Let $e = \frac{3^m - 1}{2} + r$. Under these assumptions we will prove that $\mathcal{C}_{(1,e,s)}$ is optimal and has parameters $[3^m - 1, 3^m - 2m - 2, 5]$. To this end, we need to prove that $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weights 3 and 4.

For simplicity, from now on, let η denote the quadratic character on $\mathbb{F}_{3^m}$ which is defined by $\eta(x) = 1$ if x is a nonzero square in $\mathbb{F}_{3^m}$ and $\eta(x) = -1$ if x is a nonzero nonsquare in $\mathbb{F}_{3^m}$.

Lemma 9. *Let m be even, $s = \frac{3^m-1}{2}$ and $e = \frac{3^m-1}{2} + r$, where $1 \le r \le 3^m - 2$. Then $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weight 3 if $f(x) = x^r$ is PN over $\mathbb{F}_{3^m}$.*

Proof. $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weight $\omega = 3$ if and only if (12) has no solution over $\mathbb{F}_{3^m}$ for $\omega = 3$. Let $x = x_2/x_1$ and $y = x_3/x_1$, then $x, y \ne 0, 1$, $x \ne y$ and (12) becomes

$$
\begin{cases}
1 + \frac{c_2}{c_1}x + \frac{c_3}{c_1}y = 0 \\
1 + \frac{c_2}{c_1}\eta(x)x^r + \frac{c_3}{c_1}\eta(y)y^r = 0 \\
1 + \frac{c_2}{c_1}\eta(x) + \frac{c_3}{c_1}\eta(y) = 0
\end{cases}
\tag{15}
$$

since $x^e = \eta(x)x^r$ and $y^e = \eta(y)y^r$. Due to symmetry, we only need to consider (15) for the following two cases:

1. $c_1 = c_2 = c_3 = 1$: In this case, by the third equation in (15), one has $1 + \eta(x) + \eta(y) = 0$. This leads to $\eta(x) = \eta(y) = 1$. Then (15) is reduced to $1 + x + y = 0$ and $1 + x^r + y^r = 0$.

2. $c_1 = c_2 = 1$, $c_3 = -1$: Similarly, by (15), one has $1 + \eta(x) - \eta(y) = 0$, i.e., $\eta(x) = 1$ and $\eta(y) = -1$. Thus (15) is reduced to $1 + x - y = 0$ and $1 + x^r + y^r = 0$.

Assume that (x, y) is a solution of (15) with $x, y \ne 0, 1$ and $x \ne y$. Then 1) and 2) imply that

$$
x - 1 = 1 - (\pm y), \ x^r - 1^r = 1^r - (\pm y)^r
$$

where we used the fact that r is even (because x^r is PN over $\mathbb{F}_{3^m}$). Furthermore, since $f(x) = x^r$ is PN over $\mathbb{F}_{3^m}$, by (14), the equations above hold if and only if $(x, 1) = (1, \pm y)$, a contradiction with $x \ne 1$. Thus, (12) has no solution for $\omega = 3$. This completes the proof. □

With the same techniques, we can also prove $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weight 4 if $e = \frac{3^m-1}{2} + r$ and $f(x) = x^r$ is PN over $\mathbb{F}_{3^m}$.

Lemma 10. *Let m be even, $s = \frac{3^m-1}{2}$ and $e = \frac{3^m-1}{2} + r$, where $1 \le r \le 3^m - 2$. Then $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weight 4 if $f(x) = x^r$ is PN over $\mathbb{F}_{3^m}$.*

Proof. $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weight $\omega = 4$ if and only if (12) has no solution over $\mathbb{F}_{3^m}$ for $\omega = 4$. Let $x = x_2/x_1$, $y = x_3/x_1$ and $z = x_4/x_1$, then $x, y, z \neq 0, 1$ are pairwise distinct and (12) becomes

$$
\begin{cases}
1 + \frac{c_2}{c_1}x + \frac{c_3}{c_1}y + \frac{c_4}{c_1}z = 0 \\
1 + \frac{c_2}{c_1}\eta(x)x^r + \frac{c_3}{c_1}\eta(y)y^r + \frac{c_4}{c_1}\eta(z)z^r = 0 \\
1 + \frac{c_2}{c_1}\eta(x) + \frac{c_3}{c_1}\eta(y) + \frac{c_4}{c_1}\eta(z) = 0
\end{cases}
\tag{16}
$$

since $x^e = \eta(x)x^r$, $y^e = \eta(y)y^r$ and $z^e = \eta(z)z^r$ if $e = \frac{3^m - 1}{2} + r$. Due to symmetry, we only need to consider (16) for the following three cases:

1. $c_1 = c_2 = c_3 = c_4 = 1$: By the third equation in (16), i.e., $1 + \eta(x) + \eta(y) + \eta(z) = 0$, without loss of generality, one can assume $\eta(x) = 1$ and $\eta(y) = \eta(z) = -1$. Then (16) is reduced to $1 + x + y + z = 0$ and $1 + x^r - y^r - z^r = 0$.

2. $c_1 = c_2 = c_3 = 1$, $c_4 = -1$: In this case, one has $1 + \eta(x) + \eta(y) - \eta(z) = 0$ according to (16). Then there are two cases to be considered: (I) If $\eta(z) = -1$, then $\eta(x) + \eta(y) = 1$ which implies $\eta(x) = \eta(y) = -1$; (II) If $\eta(z) = 1$, then $\eta(x) + \eta(y) = 0$ and one can assume $\eta(x) = 1$ and $\eta(y) = -1$ due to the symmetry of x and y. Then, (16) can be reduced to $1 + x + y - z = 0$ and $1 - x^r - y^r + z^r = 0$ or $1 + x + y - z = 0$ and $1 + x^r - y^r - z^r = 0$.

3. $c_1 = c_2 = 1$, $c_3 = c_4 = -1$: Similar as case 2), by (16) one has $1 + \eta(x) - \eta(y) - \eta(z) = 0$. (I) If $\eta(x) = 1$, then $\eta(x) + \eta(y) = -1$. This leads to $\eta(y) = \eta(z) = 1$; (II) If $\eta(x) = -1$, then $\eta(y) + \eta(z) = 0$ and one can assume $\eta(y) = 1$ and $\eta(z) = -1$ due to the symmetry of y and z. Therefore, (16) can be reduced to $1 + x - y - z = 0$ and $1 + x^r - y^r - z^r = 0$ or $1 + x - y - z = 0$ and $1 - x^r - y^r + z^r = 0$.

Thus there are totally five cases to be considered. However, it should be noticed that there are exactly two "-1" and two "1" in the multi-set $\{1, \frac{c_2}{c_1}\eta(x), \frac{c_3}{c_1}\eta(y), \frac{c_4}{c_1}\eta(z)\}$ for each of the five cases. This makes the proof for each case quite similar by using properties of PN functions. Hence we only prove that (16) has no solution over $\mathbb{F}_{3^m}$ for the first case. Assume that (x, y, z) is a solution over $\mathbb{F}_{3^m}$ of (16) with the conditions $c_1 = c_2 = c_3 = c_4 = 1$, $\eta(x) = 1$ and $\eta(y) = \eta(z) = -1$. Then (16) can be rewritten as

$$
x - (-y) = (-z) - 1, \quad x^r - (-y)^r = (-z)^r - 1^r
$$

since r is even. However the above equalities hold if and only if $(x, -y) = (-z, 1)$ according to (14) since x^r is PN over $\mathbb{F}_{3^m}$. This contradicts with $\eta(y) = -1$ for the first case since $\eta(-1) = 1$ for even m. This completes the proof. $\qquad\square$

For even m, new classes of optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ can be obtained from the known PN monomials over $\mathbb{F}_{3^m}$ and are described in the following theorem.

Theorem 7. *Let m be even and $s = \frac{3^m - 1}{2}$. Then the ternary cyclic code $\mathcal{C}_{(1,e,s)}$ is optimal and has parameters $[3^m - 1, 3^m - 2m - 2, 5]$ if*

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

- $e = \frac{3^m - 1}{2} + 3^h + 1$, *where $m / \gcd(m, h)$ is odd; or*

- $e = \frac{3^m - 1}{2} + \frac{3^h + 1}{2}$, *where $\gcd(m, h) = 1$ and h is odd.*

Proof. For each class of e, one can derive that $\gcd(e, 3^m - 1) = 2$. By Lemma 1, we have that $|C_e| = m$. It can be easily verified that $C_1 \cap C_e = \varnothing$. Then the desired conclusions follow from Lemmas 9–10, Theorem 6 and the fact that the three monomials x^2, $x^{3^h + 1}$ and $x^{(3^h + 1)/2}$ are PN over $\mathbb{F}_{3^m}$ under the conditions described in this theorem. This completes the proof. $\qquad\square$

Example 9. *Two examples of the codes of Theorem 7 are the following:*

1. *Let $m = 4$, $s = \frac{3^m - 1}{2} = 40$ and α be a generator of $\mathbb{F}_{3^m}^*$ with $\alpha^4 + 2\alpha^3 + 2 = 0$. If $e = \frac{3^m - 1}{2} + 2 = 42$, then the generator polynomial of $\mathcal{C}_{(1,42,40)}$ is $x^9 + x^8 + 2x^6 + 2x^5 + x^4 + 2x^2 + 2x + 2$ and $\mathcal{C}_{(1,42,40)}$ has parameters $[80, 71, 5]$.*

2. *Let $m = 6$, $s = \frac{3^m - 1}{2} = 364$ and α be a generator of $\mathbb{F}_{3^m}^*$ with $\alpha^6 + 2\alpha^4 + \alpha^2 + 2\alpha + 2 = 0$. If $e = \frac{3^m - 1}{2} + 3^2 + 1 = 374$, then the generator polynomial of $\mathcal{C}_{(1,374,364)}$ is $x^{13} + 2x^{12} + x^{10} + x^9 + 2x^7 + 2x^6 + x^5 + 2x^3 + 2$ and $\mathcal{C}_{(1,374,364)}$ has parameters $[728, 715, 5]$.*

According to Theorem 7, both $\mathcal{C}_{(1,42,40)}$ and $\mathcal{C}_{(1,374,364)}$ are optimal.

Another class of optimal ternary cyclic code $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ for even m are described in the following theorem.

Theorem 8. *Let m be even and let $s = \frac{3^m-1}{2}$. Then the ternary cyclic code $\mathcal{C}_{(1,2,s)}$ is optimal and has parameters $[3^m - 1, 3^m - 2m - 2, 5]$.*

Proof. It follows from Lemma 1 that $|C_2| = m$. Clearly, we have that $C_1 \cap C_2 = \emptyset$. Hence the dimension of $\mathcal{C}_{(1,2,s)}$ is equal to $3^m - 2m - 2$. By the BCH bound, the minimum distance of $\mathcal{C}_{(1,2)}$ is at least 4. Then to prove this theorem, we need only to prove that (12) has no solution over $\mathbb{F}_{3^m}$ for $e = 2$ and $\omega = 4$ due to the fact that $\mathcal{C}_{(1,2,s)} \subset \mathcal{C}_{(1,2)}$ and Theorem 6. Because of symmetry, we discuss (12) by distinguishing among the following cases:

1. $c_1 = c_2 = c_3 = c_4 = 1$: Without loss of generality, we can assume $\eta(x) = 1$ and $\eta(y) = \eta(z) = -1$ by the third equation in (12). On the other hand, the first two equations in (12) imply that $1 + x^2 + y^2 + (-1 - x - y)^2 = 0$, i.e., $x^2 + (y+1)x + y^2 + y + 1 = 0$. For any fixed y, the discriminant of this quadratic equation with unknown x is given by $\Delta = (y+1)^2 - 4(y^2 + y + 1) = y$ which is a nonsquare since $\eta(y) = -1$. Hence, (12) has no solution over $\mathbb{F}_{3^m}$ for this case.

2. $c_1 = c_2 = c_3 = 1, c_4 = -1$: In this case, by the first two equations in (12) one has $1 + x^2 + y^2 - (1 + x + y)^2 = 0$, i.e., $x + y + xy = 0$. This implies $y = -\frac{x}{x+1}$ and $\frac{1}{x+1} = -\frac{y}{x}$. Then $\eta(z) = \eta(1 + x + y) = \eta(\frac{(x-1)^2}{x+1}) = \eta(\frac{1}{x+1}) = \eta(-\frac{y}{x}) = \eta(-xy) = \eta(xy)$ since $\eta(-1) = 1$ if m is even. This leads to $0 = 1 + \eta(x) + \eta(y) - \eta(z) = 1 + \eta(x) + \eta(y) - \eta(xy) = (\eta(x) - 1)(1 - \eta(y)) - 1 \in \{1, -1\}$ since $\eta(x), \eta(y) \in \{1, -1\}$, a contradiction. Thus, (12) has no solution over $\mathbb{F}_{3^m}$.

3. $c_1 = c_2 = 1, c_3 = c_4 = -1$: The first two equations in (12) imply that $1 + x^2 - y^2 - (1 + x - y)^2 = 0$ for this case, i.e, $y^2 - y - xy + x = (y - x)(y - 1) = 0$ which is impossible since $x \neq y$ and $y \neq 1$.

Thus, (12) has no solution over $\mathbb{F}_{3^m}$ for $e = 2$ and $\omega = 4$. This completes the proof. $\square$

It should be noted that the codes of Theorem 8 are not BCH codes.

Example 10. *The following are two examples of the codes of Theorem 8.*

1. *Let $m = 4$, $s = \frac{3^m-1}{2} = 40$ and α be a generator of $\mathbb{F}_{3^m}^*$ with $\alpha^4 + 2\alpha^3 + 2 = 0$. Then the generator polynomial of $\mathcal{C}_{(1,2,40)}$ is $x^9 + 2x^8 + x^6 + 2x^5 + 2x^3 + 2x^2 + 2x + 2$ and $\mathcal{C}_{(1,2,40)}$ has parameters $[80, 71, 5]$.*

2. *Let $m = 6$, $s = \frac{3^m - 1}{2} = 364$ and α be a generator of $\mathbb{F}_{3^m}^*$ with $\alpha^6 + 2\alpha^4 + \alpha^2 + 2\alpha + 2 = 0$. Then the generator polynomial of $\mathcal{C}_{(1,2,364)}$ is $x^{13} + 2x^{12} + 2x^9 + 2x^8 + x^5 + x^4 + 2x^3 + x + 2$ and $\mathcal{C}_{(1,2,364)}$ has parameters $[728, 715, 5]$.*

According to Theorem 8, both $\mathcal{C}_{(1,2,40)}$ and $\mathcal{C}_{(1,2,364)}$ are optimal.

5.2 New optimal double-error-correcting ternary cyclic codes for odd m

In this subsection, new optimal ternary cyclic codes $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ for odd m are investigated, where e is even and satisfies

$$e \cdot r \equiv 2 \cdot 3^\tau \pmod{3^m - 1} \tag{17}$$

for some $1 \leq r \leq 3^m - 2$ and $0 \leq \tau \leq m - 1$.

To prove that $\mathcal{C}_{(1,e,s)}$ has minimum distance $d = 5$, we need to show that $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weights 3 and 4.

Lemma 11. *Let m be odd and let $s = \frac{3^m - 1}{2}$. Let e and r be even positive integers satisfying (17) and $\gcd(r, 3^m - 1) = 2$. Then $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weight 3 if $f(x) = x^{r/2}$ is PN over $\mathbb{F}_{3^m}$.*

Proof. We now prove that (12) has no solution for $\omega = 3$. Notice that $\frac{c_i x_i^e}{c_1 x_1^e} = \frac{c_i}{c_1} \left(\frac{c_i x_i}{c_1 x_1} \right)^e$ since e is even and $c_i / c_1 \in \{1, -1\}$ for $i = 2, 3$. On the other hand, by $\eta(-1) = -1$, one has $\frac{c_i}{c_1} \eta \left(\frac{x_i}{x_1} \right) = \eta \left(\frac{c_i x_i}{c_1 x_1} \right)$. Thus, let $x = c_2 x_2 / c_1 x_1$ and $y = c_3 x_3 / c_1 x_1$, then (12) can be written as

$$\begin{cases} 1 + x + y = 0 \\ 1 + \frac{c_2}{c_1} x^e + \frac{c_3}{c_1} y^e = 0 \\ 1 + \eta(x) + \eta(y) = 0. \end{cases} \tag{18}$$

Assume that (x, y) is a solution of (18), then by $1 + \eta(x) + \eta(y) = 0$, one has $\eta(x) = \eta(y) = 1$. It then follows from $\gcd(r, 3^m - 1) = 2$ that there exist $u, v \in \mathbb{F}_{3^m}$ such that $x = u^r$ and $y = v^r$. Then, according to (17), one gets $x^e = u^{er} = u^{2 \cdot 3^\tau}$ and $y^e = v^{er} = v^{2 \cdot 3^\tau}$. Therefore, (18) is equivalent to

$$\begin{cases} 1 + u^r + v^r = 0 \\ 1 + \frac{c_2}{c_1} u^2 + \frac{c_3}{c_1} v^2 = 0. \end{cases} \tag{19}$$

Notice that $r/2$ is even since $f(x) = x^{r/2}$ is PN over $\mathbb{F}_{3^m}$. This leads to $u^r = (\frac{c_2}{c_1}u^2)^{r/2}$ and $v^r = (\frac{c_3}{c_1}v^2)^{r/2}$. Let $\mu = \frac{c_2}{c_1}u^2$ and $\nu = \frac{c_3}{c_1}v^2$. Then (19) can be written as

$$f(\mu) - f(1) = f(1) - f(\nu), \quad \mu - 1 = 1 - \nu$$

which hold if and only if $(\mu, 1) = (1, \nu)$ according to (14) since $f(x) = x^{r/2}$ is PN over $\mathbb{F}_{3^m}$. However, $\mu = \nu = 1$ implies $x = y = 1$. This leads to $c_1 x_1 = c_2 x_2 = c_3 x_3$ which is impossible since $c_1, c_2, c_3 \in \{1, -1\}$ and x_1, x_2, x_3 are pairwise distinct. Therefore, (18) has no solution $(x, y) \in \mathbb{F}_{3^m}^* \times \mathbb{F}_{3^m}^*$. This completes the proof. $\square$

We also need the following lemma in the sequel.

Lemma 12. *Let m be odd and let $s = \frac{3^m - 1}{2}$. Let e and r be even positive integers satisfying (17) and $\gcd(r, 3^m - 1) = 2$. Then $\mathcal{C}_{(1,e,s)}$ has no codeword of Hamming weight 4 if $f(x) = x^{r/2}$ is PN over $\mathbb{F}_{3^m}$.*

Proof. We now show that (12) has no solution for $\omega = 4$. Similar as in (18), let $x = c_2 x_2 / c_1 x_1$, $y = c_3 x_3 / c_1 x_1$ and $z = c_4 x_4 / c_1 x_1$, then (12) can be written as

$$\begin{cases} 1 + x + y + z = 0 \\ 1 + \frac{c_2}{c_1}x^e + \frac{c_3}{c_1}y^e + \frac{c_4}{c_1}z^e = 0 \\ 1 + \eta(x) + \eta(y) + \eta(z) = 0. \end{cases} \tag{20}$$

Assume that (x, y, z) is a solution of (20). Since $1 + \eta(x) + \eta(y) + \eta(z) = 0$, we need consider the following three cases: 1) $\eta(x) = 1, \eta(y) = \eta(z) = -1$; 2) $\eta(x) = \eta(y) = -1, \eta(z) = 1$; and 3) $\eta(x) = \eta(z) = -1, \eta(y) = 1$. In the following, we give only the proof for case 1) since the other two cases can be completely proven in the same manner due to symmetry.

Note that $\eta(-1) = -1$ and $\gcd(r, 3^m - 1) = 2$. Every square (resp. nonsquare) in $\mathbb{F}_{3^m}$ can be expressed as u^r (resp. $-u^r$) for some $u \in \mathbb{F}_{3^m}$. Thus, for x, y, z with $\eta(x) = 1$ and $\eta(y) = \eta(z) = -1$, there exist $u, v, w \in \mathbb{F}_{3^m}$ such that $x = u^r, y = -v^r$ and $z = -w^r$. Then, according to (17) and the fact that e is even, one gets $x^e = u^{er} = u^{2 \cdot 3^\tau}$, $y^e = v^{er} = v^{2 \cdot 3^\tau}$ and $z^e = w^{er} = w^{2 \cdot 3^\tau}$. Therefore, (20) is equivalent to

$$\begin{cases} 1 + u^r - v^r - w^r = 0 \\ 1 + \frac{c_2}{c_1}u^2 + \frac{c_3}{c_1}v^2 + \frac{c_4}{c_1}w^2 = 0. \end{cases} \tag{21}$$

Let $\mu = \frac{c_2}{c_1}u^2$, $\nu = \frac{c_3}{c_1}v^2$ and $\lambda = \frac{c_4}{c_1}w^2$. Since $f(x) = x^{r/2}$ is PN over $\mathbb{F}_{3^m}$, $r/2$ must be even. This implies that $f(\pm\mu) = \mu^{r/2} = (\frac{c_2}{c_1}u^2)^{r/2} = u^r$, $f(\pm\nu) = \nu^{r/2} = v^r$ and $f(\pm\lambda) = \lambda^{r/2} = w^r$. Thus, (21) can be rewritten as

$$\begin{cases} f(\mu) - f(-\nu) &= f(-\lambda) - f(1) \\ \mu - (-\nu) &= (-\lambda) - 1. \end{cases} \tag{22}$$

Since $f(x) = x^{r/2}$ is PN over $\mathbb{F}_{3^m}$, then by (14) one has that (22) holds if and only if $(\mu, -\nu) = (-\lambda, 1)$, i.e., $\mu + \lambda = 0$ and $\nu = -1$. This leads to $x + z = 0$ and $y = -1$, i.e., $c_2x_2 + c_4x_4 = 0$ and $c_3x_3 = -c_1x_1$ which imply that $c_2 = c_4$ and $c_1 = c_3$ since $x_2 \neq x_4$ and $x_1 \neq x_3$. Thus, one then has that $x_2 = -x_4$, $x_1 = -x_3$, and the second equation in (12) can be reduced to $2c_1x_1^e + 2c_2x_2^e = 0$ which implies that $(2c_1x_1^e)^r = (-2c_2x_2^e)^r$, i.e., $x_1^2 = x_2^2$ due to (17) and the fact that r is even. This is impossible since $x_1 \neq x_2$ and $x_1 = -x_2$ implies $x_2 = x_3$, a contradiction. Therefore, (20) has no solution over $\mathbb{F}_{3^m}$. This completes the proof. □

We are now ready to document the main result of this section with the following theorem.

Theorem 9. *Let m be odd, e be even and $s = \frac{3^m-1}{2}$. Let r, τ be nonnegative integers such that $\gcd(r, 3^m - 1) = 2$ and $e \cdot r \equiv 2 \cdot 3^\tau \pmod{3^m - 1}$. Then the ternary cyclic code $\mathcal{C}_{(1,e,s)}$ is optimal and has parameters $[3^m - 1, 3^m - 2m - 2, 5]$ if $f(x) = x^{r/2}$ is PN over $\mathbb{F}_{3^m}$.*

Proof. Since e is even and $e \cdot r \equiv 2 \cdot 3^\tau \pmod{3^m - 1}$, we have $\gcd(e, 3^m - 1) = 2$. It then follows from Lemma 1 that $|C_e| = m$. In addition, it is easily verified that $C_1 \cap C_e = \emptyset$. Hence the dimension of the code is equal to $3^m - 2m - 2$. The desired conclusion on the minimum distance of this code follows from Lemmas 11, 12 and Theorem 6. This completes the proof. □

With Theorem 9, new classes of optimal ternary cyclic codes $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2 - 2m, 5]$ for odd m can be obtained.

Corollary 8. *Let m be odd and $s = \frac{3^m-1}{2}$. Then the ternary cyclic code $\mathcal{C}_{(1,e,s)}$ is optimal and has parameters $[3^m - 1, 3^m - 2m - 2, 5]$ if*

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

2. $e = \frac{3^{m+1}-1}{8}$ *for $m \equiv 3 \pmod 4$; and $e = \frac{3^{m+1}-1}{8} + \frac{3^m-1}{2}$ for $m \equiv 1 \pmod 4$; or*

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

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

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

Proof. To prove this corollary with Theorem 9, for each e it is sufficient to find a suitable r such that e and r satisfy the conditions given in Theorem 9. Thus for the given e in each case, we can define the r respectively by

1. $r = 4$;

2. $r = 8$;

3. $r = 3^h + 1$, where $h = (m+1)/2$ if $m \equiv 1 \pmod 4$, and $h = (m-1)/2$ if $m \equiv 3 \pmod 4$;

4. $r = 2(3^h + 1)$, where $h = (m+1)/2$;

5. $r = 3^h + 1$, where $h = (m+1)/4$ if $m \equiv 3 \pmod 8$, and $h = (3m-1)/4$ if $m \equiv 7 \pmod 8$.

Then, for each pair (e, r), one can verify that the conditions in Theorem 9 are met according to the known three classes of PN monomials. This completes the proof. $\square$

Note that all the exponents e given in Corollary 8 are APN exponents [18].

Example 11. *Let $m = 3$, $s = \frac{3^m-1}{2} = 13$ and α be a generator of $\mathbb{F}_{3^m}^*$ with $\alpha^3 + 2\alpha + 1 = 0$.*

1. *If $e = 3^{(m+1)/2} - 1 = 8$, then the generator polynomial of $\mathcal{C}_{(1,8,13)}$ is $x^7 + 2x^4 + x^3 + 2x + 2$ and $\mathcal{C}_{(1,8,13)}$ has parameters $[26, 19, 5]$.*

2. *If $e = \frac{3^{m+1}-1}{8} = 10$, then the generator polynomial of $\mathcal{C}_{(1,10,13)}$ is $x^7 + 2x^6 + x^4 + 2x^2 + 2$ and $\mathcal{C}_{(1,10,13)}$ has parameters $[26, 19, 5]$.*

Both $\mathcal{C}_{(1,8,13)}$ and $\mathcal{C}_{(1,10,13)}$ are optimal according to Corollary 8.

Example 12. *Let $m = 5$, $s = \frac{3^m-1}{2} = 121$ and α be a generator of $\mathbb{F}_{3^m}^*$ with $\alpha^5 + 2\alpha + 1 = 0$.*

1. If $e = \frac{3^m+1}{4} + \frac{3^m-1}{2} = 182$, then the generator polynomial of $\mathcal{C}_{(1,182,121)}$ is $x^{11} + x^9 + x^5 + x^4 + 2x^3 + 2x^2 + 2$ and $\mathcal{C}_{(1,182,121)}$ has parameters $[242, 231, 5]$.

2. If $e = \frac{3^{(m+1)/2}-1}{2} + \frac{3^m-1}{2} = 134$, then the generator polynomial of $\mathcal{C}_{(1,134,121)}$ is $x^{11} + x^8 + x^6 + 2x^5 + 2x^4 + x^2 + x + 2$ and $\mathcal{C}_{(1,134,121)}$ has parameters $[242, 231, 5]$.

Both $\mathcal{C}_{(1,182,121)}$ and $\mathcal{C}_{(1,134,121)}$ are optimal according to Corollary 8.

According to Theorem 9, optimal ternary cyclic code $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2 - 2m, 5]$ can also be obtained from e which is not in the list of known APN exponents [18]. The following Corollary is such an example.

Corollary 9. *Let $m \equiv 3 \pmod 4$, $s = \frac{3^m-1}{2}$ and $e = \frac{3^m+2\cdot 3^t-1}{20}$ with $t \equiv 3$ (mod 4). Then the ternary cyclic code $\mathcal{C}_{(1,e,s)}$ is optimal and has parameters $[3^m - 1, 3^m - 2m - 2, 5]$.*

Proof. By a direct calculation, one has that $\frac{3^m-1}{2} \equiv 13 \pmod{20}$ and $3^t \equiv 7 \pmod{20}$ if $m \equiv 3 \pmod 4$ and $t \equiv 3 \pmod 4$. Hence e is an even integer. If $r = 20$, then $\gcd(r, 3^m - 1) = 2$, $e \cdot r \equiv 2 \cdot 3^t \pmod{3^m - 1}$ and $x^{r/2}$ is PN over $\mathbb{F}_{3^m}$ as m is odd. Then the desired result follows from Theorem 9. This completes the proof. $\square$

Example 13. *Let $m = 7$, $s = \frac{3^m-1}{2} = 1093$ and α be a generator of $\mathbb{F}_{3^m}^*$ with $\alpha^7 + 2\alpha + 1 = 0$. If $t = 3$ and $e = \frac{3^m+2\cdot 3^t-1}{20} = 112$ which is not an APN exponent, then the generator polynomial of $\mathcal{C}_{(1,112,1093)}$ is $x^{15} + 2x^{14} + 2x^{13} + 2x^{11} + x^{10} + x^9 + 2x^8 + x^7 + x^5 + 2x^4 + 2x^3 + x^2 + 2$ and $\mathcal{C}_{(1,112,1093)}$ has parameters $[2186, 2171, 5]$ which is optimal according to Corollary 9.*

It should be noticed that Corollary 9 in fact indicates a general method for deriving new exponent e such that $\mathcal{C}_{(1,e,s)}$ is optimal and has parameters $[3^m - 1, 3^m - 2m - 2, 5]$. In general, with the known PN monomials, one can select an integer r such that $x^{r/2}$ is PN over $\mathbb{F}_{3^m}$ and $\gcd(r, 3^m - 1) = 2$. Then, for such a fixed r, by solving congruence equation (17) which has exactly two solutions since $\gcd(r, 3^m - 1) = 2$, one can get a desired e. Hence, through direct calculations, more new optimal ternary cyclic codes $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ can be obtained from this approach.

6 CONCLUSIONS

Optimal ternary cyclic codes $\mathcal{C}_{(1,e)}$ with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ and $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2 - 2m, 5]$ were investigated respectively in this paper. By analyzing irreducible factors of certain polynomials with low degrees over finite fields, an open problem about $\mathcal{C}_{(1,e)}$ for $e = 2(3^{m-1} - 1)$ proposed by Ding and Helleseth in [5] was solved and new optimal ternary codes $\mathcal{C}_{(1,e)}$ with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ were also obtained with the same techniques. Moreover, inspired by the work of [2] and [5], a number of classes of optimal ternary cyclic codes $\mathcal{C}_{(1,e,s)}$ with parameters $[3^m - 1, 3^m - 2m - 2, 5]$ were also presented. The construction and properties of these optimal codes $\mathcal{C}_{(1,e,s)}$ are based on known PN and APN monomials.

REFERENCES

[1] E. Betti and M. Sala. A new bound for the minimum distance of a cyclic code from its defining set. *IEEE Transactions on Information Theory*, 2006.

[2] 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.

[3] 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.

[4] P. Dembowski and T. Ostrom. Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, 103(3):239–258, 1968.

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

[6] C. Ding and S. Ling. A q-polynomial approach to cyclic codes. *Finite Fields and Their Applications*, 20(0):1 – 14, 2013.

[7] C. Ding and J. Yang. Hamming weights in irreducible cyclic codes. *Discrete Mathematics*, 313(4):434 – 446, 2013.

[8] S. El-Rouayheb, C. Georghiades, E. Soljanin, and A. Sprintson. Bounds on codes based on graph theory. In *IEEE International*

Symposium on Information Theory, ISIT 2007, 2007.

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

[10] 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.

[11] 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.

[12] Y. Jia, S. Ling, and C. Xing. On self-dual cyclic codes over finite fields. *IEEE Transactions on Information Theory*, 2011.

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

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

[15] 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.

[16] 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.

[17] 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.

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