Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 19, Number 2 (2023), pp. 515-522

http://www.ripublication.com/gjpam.htm

A Family of Ternary Cyclic Codes with Minimum Distance Four and Their Duals

Shenghan Lei

College of Mathematics and Information,
China West Normal University, Nanchong,
Sichuan-637000, China.

Abstract

Cyclic codes are an important subclass of linear codes and have signicant applications in data storage systems and communication systems, as they have efficient encoding and decoding algorithms. In this paper, by analyzing the existence of solutions of a class of equations, we get an optimal ternary cyclic code $\mathcal{C}_{(u,v)}$ with a minimum distance 4. Furthermore, based on Magam's experimental results, we find the weight of the dual code of the optimal ternary cyclic code. Further propose a conjecture about the weight distribution of the dual code.

Keywords: Cyclic code; optimal code; dual code; weight distribution.

1. INRTODUCTION

Let p be a prime. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is a linear subspace of $\mathbb{F}_p^n$ with dimension k and minimum Hamming distance d. Moreover, $\mathcal{C}$ is called cyclic if any $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$. Note that a codeword $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ can be identified with a polynomial $c_0 + c_1x + c_2x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_p[x]/(x^n - 1)$ where $F_p[x]/(x^n - 1)$ is the polynomial residue class ring. Note that every ideal of $F_p[x]/(x^n - 1)$ is principal and therefore, one can express any cyclic code $\mathcal{C}$ as ¡$g(x)$¿, i.e., the ideal generated by $g(x)$, where $g(x)$ is a monic polynomial with the least degree. The 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 $\mathcal{C}$.

Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n for 1 i n. The weight enumerator of C is defined by $1 + A_1x + A_2x^2 + \cdots + A_nx^n$,

and the vector $(A_0, A_1, A_2, \cdots, A_n)$ is called the weight distribution of the code $\mathcal{C}$. In coding theory, weight distribution has important theoretical and practical significance. Nowadays, calculating the weight distribution of some codes is still a thorny problem. For more information about the weight distribution of cyclic codes, the readers are referred to [9-11] and the references therein. Denote $\mathbb{F}_{p^m}\backslash\{0\}$ by $\mathbb{F}_{p^m}^*$. Let α be a generator of $\mathbb{F}_{p^m}^*$ and $m_i(x)$ be the minimal polynomial of α^i over $\mathbb{F}_p$, where $0 \leq i \leq p^m - 2$. Let $\mathcal{C}_{(u,v)}$ be the cyclic code over $\mathbb{F}_p$ with generator polynomial $m_u(x)m_v(x)$, where u, v are two integers such that α^u and α^v are non conjugate. The p-cyclotomic coset modulo $p^m - 1$ containing i is defined by

$$\mathcal{C}_i = \{i \cdot p^s (mod\ p^m - 1) \mid s = 0, 1, \ldots m - 1\}.$$

In 2013, Ding and Helleseth [1] obtained some optimal ternary cyclic codes with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ by employing almost perfect nonlinear monomials and some other monomials over $\mathbb{F}_{3^m}$. They also presented nine open problems. In the subsequent years, some of these problems were solved in [2-4]. Recently in [6] [7], several new classes of optimal ternary cyclic codes with parameter $[3^m - 1, 3^m - 1 - 2m, 4]$ have been proposed. The latest development of cyclic codes can be seen [3] [6] [7] [12] and the references therein. Inspired by previous work, a ternary cyclic code with parameter $[3^m - 1, 3^m - 1 - 2m, 4]$ is proposed in this paper.

The rest of this paper is organized as follows. After this introduction, some notations and known results are recalled in Section 2 and the optimal ternary cyclic code $\mathcal{C}_{(u,v)}$ constructed in this paper is proved to be optimal in Section 3. The conjecture of the weight distribution of $\mathcal{C}_{(u,v)}^{\perp}$ is presented in Section 4. Section 5 concludes this paper.

2. PRELIMINARIES

In this section, we first introduce some fixed symbols for convenience, and then give some lemmas needed to prove the main results. In this paper, we always let p is 3, m is even and $Tr(x)$ is the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. When $p = 3$, any ternary cyclic code with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ is optimal [14].

Lemma 2.1. [6] Let u be odd and v be even with $gcd(u, v, 3^m - 1) = 1$. Then the minimum distance of the cyclic code $\mathcal{C}_{(u,v)}$ is no less than 3.

Lemma 2.2. [14] Let $\mathbb{F}_q$ be a finite field. Then $\mathbb{F}_q$ has p^n elements, where the prime p is the characteristic of $\mathbb{F}_q$, then $(\alpha + \beta)^p = \alpha^p + \beta^p$ where α, $\beta \in \mathbb{F}_q$.

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

In this section, by determining the existence of solutions of some systems of equations over $\mathbb{F}_{3^m}$, we prove that the code $\mathcal{C}_{(u,v)}$ is an optimal ternary cyclic code with parameters $[3^m-1, 3^m-1-2m, 4]$, where $u = 1+(3^m-1)/4$, $v = 2$.

Theorem 3.1. Let m be even and $(u, v) = (1+(3^m-1)/4, 2)$. Then the code $\mathcal{C}_{(u,v)}$ is an optimal ternary cyclic code with parameters $[3^m-1, 3^m-1-2m, 4]$.

Proof. The length of the cyclic code $\mathcal{C}_{(u,v)}$ is 3^m-1, and its dimension is determined by the sizes of the cyclotomic cosets modulo 3^m-1 containing u and v. Since u is odd and v is even, it can be readily verified that $C_u \cap C_v = \varnothing$. If $|C_u| = |C_v| = m$, then the dimension of $\mathcal{C}_{(u,v)}$ is equal to 3^m-1-2m. Since $gcd(u, v, 3^m-1) = gcd(1+\frac{3^m-1}{4}, 2, 3^m-1) = 1$, where $u = 1+\frac{3^m-1}{4}$ is odd and $v = 2$ is even. Then the minimum weight of the cyclic code $\mathcal{C}_{(u,v)}$ is no less than 3 by utilizing Lemma 2.1. Therefore, we need show that $\mathcal{C}_{(u,v)}$ has no codeword of Hamming weight three.

Assume that the cyclic code $\mathcal{C}_{(u,v)}$ has a codeword of Hamming weight three. Then there exist three elements c_1, c_2 and c_3 in $\mathbb{F}_3^*$ and three distinct elements x_1, x_2 and x_3 in $\mathbb{F}_{3^m}^*$ such that

$$\begin{cases} c_1x_1^{1+\frac{3^m-1}{4}} + c_2x_2^{1+\frac{3^m-1}{4}} + c_3x_3^{1+\frac{3^m-1}{4}} = 0 \\ c_1x_1^2 + c_2x_2^2 + c_3x_3^2 = 0 \end{cases}$$

Putting $y_1 = \frac{x_1}{x_3}$ and $y_2 = \frac{x_2}{x_3}$, then $y_1 \neq y_2$, $y_1, y_2 \neq 0, 1$ and $y_1y_2 \neq 0$. The above equation system becomes

$$\begin{cases} c_1y_1^{1+\frac{3^m-1}{4}} + c_2y_2^{1+\frac{3^m-1}{4}} + c_3 = 0 \\ c_1y_1^2 + c_2y_2^2 + c_3 = 0 \end{cases} \tag{1}$$

Due to symmetry it is sufficient to consider the following two cases.

Case A: $c_1 = c_2 = 1, c_3 = -1$. In this case, (1) turns into

$$\begin{cases} y_1^{1+\frac{3^m-1}{4}} + y_2^{1+\frac{3^m-1}{4}} = 1 & (2) \\ y_1^2 + y_2^2 = 1 & (3) \end{cases}$$

Let $a_1 = y_1^{\frac{3^m-1}{4}}$ and $a_2 = y_2^{\frac{3^m-1}{4}}$. Then $a_1^4 = a_2^4 = 1$, where a_1 and a_2 is 4th root of unity over $\mathbb{F}_{3^m}^*$.

$$\begin{cases} a_1y_1 + a_2y_2 = 1 \\ y_1^2 + y_2^2 = 1 \end{cases}$$

$$(a_1^2-1)y_1+(a_2^2-1)y_2-a_1a_2y_1y_2=0, \tag{4}$$

Let $\frac{y_1}{y_2}=t$, where $t\neq 0,1$. (4) is equivalent to

$$(a_1^2-1)t^2-a_1a_2t+(a_2^2-1)=0. \tag{5}$$

Due to $a_1^2=\pm 1$,$a_2^2=\pm 1$, it is sufficient to consider the following three cases:
(A1) When $a_1^2=a_2^2=1$, In this subcase, (4) becomes

$$-a_1a_2y_1y_2=0,$$

Then $y_1y_2=0$. This is a contradiction to the assumption that $y_1y_2\neq 0$.

(A2) When $a_1^2=a_2^2=-1$, In this subcase, (5) becomes

$$t^2-a_1a_2t+1=0,$$

Due to $a_1a_2=\pm 1$, it is sufficient to consider the following two cases:

A2.1) When $a_1a_2=-1$, then

$$t^2+t+1=0.$$

It leads to $t^3-1=(t-1)^3=0$. Hence $t=\frac{y_1}{y_2}=1$. This is a contradiction to the assumption that $y_1\neq y_2$.

A2.2) When $a_1a_2=1$, then

$$t^2-t+1=0.$$

It leads to $t^3+1=(t+1)^3=0$. Hence $t=\frac{y_1}{y_2}=-1$, i.e., $y_1=-y_2$. since $1+\frac{1+3^m}{4}$ is odd, then

$$y_1^{1+\frac{3^m-1}{4}}+y_2^{1+\frac{3^m-1}{4}}=(-y_2)^{1+\frac{3^m-1}{4}}+y_2^{1+\frac{3^m-1}{4}}=0,$$

This is a contradiction to the fact that (2).

(A3) When $a_1^2=1$, $a_2^2=-1$. In this subcase, (4) becomes

$$y_2^2-a_1a_2y_1y_2=0,$$

It follows that $y_2(y_2-a_1a_2y_1)=0$. Since $y_2\neq 0$, we get $y_2=a_1a_2y_1$. This leads to $y_1^2+y_2^2=0$. This is a contradiction to the fact that (3).

Case B: $c_1=c_2=c_3=1$. In this case, (1) turns into

$$\begin{cases} y_1^{1+\frac{3^m-1}{4}}+y_2^{1+\frac{3^m-1}{4}}=-1 & (6)\\ y_1^2+y_2^2=-1 & (7)\end{cases}$$

Let $a_1 = y_1^{\frac{3^m-1}{4}}$ and $a_2 = y_2^{\frac{3^m-1}{4}}$. Then $a_1^4 = a_2^4 = 1$, where a_1 and a_2 is 4th root of unity over $\mathbb{F}_{3^m}^*$.

$$\begin{cases} a_1y_1 + a_2y_2 = -1 \\ y_1^2 + y_2^2 = -1 \end{cases}$$

$$(a_1^2 + 1)y_1 + (a_2^2 + 1)y_2 - a_1a_2y_1y_2 = 0, \tag{8}$$

Let $\frac{y_1}{y_2} = t$, where $t \neq 0, 1$, Then (8) is equivalent to

$$(a_1^2 + 1)t^2 - a_1a_2t + (a_2^2 + 1) = 0. \tag{9}$$

Due to $a_1^2 = \pm 1$, $a_2^2 = \pm 1$, it is sufficient to consider the following three cases:

(B1) When $a_1^2 = a_2^2 = -1$, In this subcase, (8) becomes

$$-a_1a_2y_1y_2 = 0,$$

Then we have $y_1y_2 = 0$. This is a contradiction to the assumption that $y_1y_2 \neq 0$.

(B2) When $a_1^2 = a_2^2 = 1$, In this subcase, (9) becomes

$$t^2 + a_1a_2t + 1 = 0,$$

Due to $a_1a_2 = \pm 1$, it is sufficient to consider the following two cases:

B2.1) When $a_1a_2 = 1$, then

$$t^2 + t + 1 = 0.$$

It leads to $t^3 - 1 = (t - 1)^3 = 0$. Hence $t = \frac{y_1}{y_2} = 1$. This is a contradiction to the assumption that $y_1 \neq y_2$.

B2.2) When $a_1a_2 = -1$, then

$$t^2 - t + 1 = 0.$$

It leads to $t^3 + 1 = (t + 1)^3 = 0$. Hence $t = \frac{y_1}{y_2} = -1$, i.e., $y_1 = -y_2$. Since $1 + \frac{3^m-1}{4}$ is odd, then

$$y_1^{1+\frac{3^m-1}{4}} + y_2^{1+\frac{3^m-1}{4}} = (-y_2)^{1+\frac{3^m-1}{4}} + y_2^{1+\frac{3^m-1}{4}} = 0,$$

This is a contradiction to the fact that (6).

(B3) When $a_1^2 = 1$, $a_2^2 = -1$, In this subcase, (8) becomes

$$y_1(y_1 + a_1a_2y_2) = 0.$$

Since $y_1 \neq 0$, $y_1 = -a_1a_2y_2$, we get $y_1^2 + y_2^2 = 0$. This is a contradiction to the fact that (7). Hence, the minimum distance d of the code $\mathcal{C}_{(u,v)}$ cannot be 3.

This implies that the minimum distance of $\mathcal{C}_{(u,v)}$ is no less than 4. Then we get that $\mathcal{C}_{(u,v)}$ is an optimal ternary cyclic code with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$. □

4. CONJECTURE ON WEIGHT DISTRIBUTION OF DUAL CODE OF $\mathcal{C}_{(u,v)}$

In this section, based on the results of Magam experiment, we determine the weight of dual code $\mathcal{C}^{\perp}_{(u,v)}$, and further propose a conjecture about the weight distribution of dual code $\mathcal{C}^{\perp}_{(u,v)}$, where $u = 1 + (3^m - 1)/4$, $v = 2$.

Theorem 4.1. The weight of the codeword $c(a, b)$ in $\mathcal{C}^{\perp}_{(u,v)}$ is 0 if $a = b = 0$, and otherwise takes values from

$$\{2 \cdot 3^{m-1}, 2 \cdot 3^{m-1} \pm 3^{(\frac{m}{2}-1)}, 2 \cdot 3^{m-1} \pm 2 \cdot 3^{(\frac{m}{2}-1)}\}.$$

The following are some examples of the weight distribution of dual codes derived from the Magma program:

Example 4.2. Let $p = 3$ and $m = 2$. Then the weight enumerator of $\mathcal{C}^{\perp}_{(u,v)}$ (which has parameters [8,8,4]) is

$$1 + 20x^4 + 32x^5 + 8x^6 + 16x^7 + 4x^8.$$

Example 4.3. Let $p = 3$ and $m = 4$. Then the weight enumerator of $\mathcal{C}^{\perp}_{(u,v)}$ (which has parameters[80,72,4])is

$$1 + 1320x^{48} + 2400x^{51} + 80x^{54} + 1920x^{57} + 840x^{60}.$$

Example 4.4. Let $p = 3$ and $m = 6$. Then the weight enumerator of $\mathcal{C}^{\perp}_{(u,v)}$ (which has parameters [728,716,4]) is

$$1 + 95004x^{468} + 183456x^{477} + 728x^{486} + 170352x^{495} + 81900x^{504}.$$

Based on the results of Magam experiment, we propose a conjecture about the weight distribution of $\mathcal{C}^{\perp}_{(u,v)}$:

Conjecture 4.5. Let $p = 3$, $u = 1 + \frac{3^m-1}{4}$ and $v = 2$ where m is even, the weight distribution of $\mathcal{C}^{\perp}_{(u,v)}$ is given by Table 1.

Table 1: Weight distribution of $\mathcal{C}_{(u,v)}^{\perp}$

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

5. COCLUDING REMARKS

In this paper, by studying the existence of solutions of some equations over $\mathbb{F}_{3^m}$, a new class of optimal ternary cyclic codes is determined and proved. Furthermore, based on the experimental results of Magam, the weight of the dual code $\mathcal{C}_{(u,v)}^{\perp}$ is found, and the conjecture about the weight distribution of the dual code $\mathcal{C}_{(u,v)}^{\perp}$ is given.

ACKNOWLEDGMENTS

The authors are very grateful to the instructor reviewers, for his comments which improved the presentation and quality of this paper.

REFERENCES

[1] C. Ding and T. Helleseth, Optimal ternary cyclic codes from monomials, IEEE Trans. Inf.Theory, 59 (2013), 5898C5904.

[2] N. Li, C. Li, T. Helleseth, C. Ding and X. Tang, Optimal ternary cyclic codes with minimun distance four and five, Finite Fields Appl., 30 (2014), 100C120.

[3] D. Han and H. Yan, On an open problem about a class of optimal ternary cyclic codes, Finite Fields Appl., 59 (2019), 335C343.

[4] N.Li,Z.C.Zhou and T.Helleseth,On a conjecture about a class of optimal ternary cyclic codes, Seventh International workshop on Signal Design and its Applications in Communications, 2015, 62-65.

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

[6] Z. Zha, L. Hu, Y. Liu, X. Cao, Further results on optimal ternary cyclic codes, Finite Fields Their Appl. vol.75, pp. 101898, 2021.

[7] Liu Y, Cao X, Lu W. Two classes of new optimal ternary cyclic codes[J]. Advances in Mathematics of Communications, 2021.

[8] L. Wang and G. Wu, Several classes of optimal ternary cyclic codes with minimal distance four, Finite Fields Appl.,40 (2016), 126C137.

[9] K. Feng and J. Luo, Weight distribution of some reducible cyclic codes, Finite Fields Appl.,14 (2008), 390C409

[10] C. J. Li, Q. Yue, and F. W. Li, Weight distributions of cyclic codes with respect to pairwise coprime order elements,Finite Fields Appl., 28 (2014) 94C114.

[11] M. Xiong and N. Li, Optimal cyclic codes with generalized Niho-type zeros and the weight distribution, IEEE Trans. Inf. Theory, 61 (2015), 4914C4922.

[12] Z. Zha and L. Hu, New classes of optimal ternary cyclic codes with minimum distance four,Finite Fields Appl., 64 (2020), 1016710.

[13] C. Ding, Y. Gao, Z. Zhou, Five Families of Three-Weight Ternary Cyclic Codes and Their Duals, IEEE Trans. Inf. Theory 59 (12) (2013) 7940C7946.

[14] W. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[15] Dandan Wang, Xiwang Cao. A family of optimal ternary cyclic codes with minimum distance five and their duals[J]. Cryptography and Communications,2021(prepublish).