

两类具有两个零点的最优三元循环码

何 潮¹, 曾学强²

¹四川职业技术学院通识教育学院, 四川 遂宁

²四川轻化大学数学与统计学院, 四川 自贡

收稿日期: 2024年9月13日; 录用日期: 2024年10月15日; 发布日期: 2024年10月23日

摘 要

本文从生成多项式的角度研究具有两个零点的三元循环码。运用有限域上的多变元、因式分解和低次不可约多项式解的结构等数学知识, 得到了两类参数为 $[3^m - 1, 3^m - 2m - 1, 4]$ 的三元循环码, 并关于 Sphere-Packing 界是紧的。

关键词

有限域, 循环码, Sphere-Packing 界

Two Classes of Optimal Ternary Cyclic Codes with Two Zeros

Chao He¹, Xueqiang Zeng²

¹College of General Education, Sichuan Vocational and Technical College, Suining Sichuan

²College of Mathematics and Statistics, Sichuan University of Science & Engineering, Zigong Sichuan

Received: Sep. 13th, 2024; accepted: Oct. 15th, 2024; published: Oct. 23rd, 2024

Abstract

This paper studies ternary cyclic codes with two zeros from the perspective of generating polynomials. By employing mathematical knowledge such as multivariate polynomials over finite fields, factorization, and the structure of solutions for low-degree irreducible polynomials, we obtain two classes of ternary cyclic codes with parameters $[3^m - 1, 3^m - 2m - 1, 4]$. These codes are shown to be tight with respect to the Sphere-Packing bound.

Keywords

Finite Field, Cyclic Code, Sphere Packing Bound

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

循环码作为线性码的一个重要子类, 主要有两大特点: 一是可以用许多优秀的数学工具(如多项式代数、有限域等)进行分析与研究码, 这使得循环码在理论上拥有很强的可研究性, 能够设计出高效的编码和译码算法; 二是循环码的编译码操作能够通过移位寄存器来完成, 这种方法在硬件上非常简单有效。因此, 循环码在工程中广泛应用, 特别是在数据传输和广播系统等对实时性和可靠性要求较高的场合。近些年来, 最优循环码的构造是一个热门研究课题, 尤其是对由两个或三个零点生成的循环码的最优性的研究。

设 F_{p^m} 是含有 p^m 个元素的有限域, 其特征为 p 。 $F_{p^m}^*$ 表示 F_{p^m} 中的非零元素集合。有限域 F_p 上参数为 $[n, k, d]$ 线性码 C 是 F_p^n 中的一个 k 维子空间, 其最小汉明距离为 d 。若对任意码字 $(c_0, c_1, \dots, c_{n-1}) \in C$ 循环移位后, 仍有 $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$, 则称 C 是参数为 $[n, k, d]$ 的循环码。一个参数为 $[n, k]$ 码的码字 $(c_0, c_1, \dots, c_{n-1})$ 可以与一个次数小于 n 的多项式相对应。因此, 长度为 n 且在有限域 F_p 上的任何循环码都对应于多项式剩余类环 $F_p[x]/(x^n - 1)$ 的一个理想。对于 $\gcd(n, p) = 1$, 注意到 $F_p[x]/(x^n - 1)$ 中的每个理想都是主理想, 码长为 n 的循环码 C 在有限域 F_p 上可以表示为 $C = \langle g(x) \rangle$, 其中 $g(x)$ 是首项系数为 1 且次数最小的多项式, 称之为循环码 C 的生成多项式, 将生成多项式的零点称为循环码的零点。设 α 是有限域 F_{p^m} 中的一个本原元, 对于任意的一个整数 $1 \leq t \leq p^m - 1$, 记 F_{p^m} 上 α^t 的极小多项式为 $m_{\alpha^t}(x)$ 。记生成多项式为 $g(x) = m_{\alpha^{t_1}}(x)m_{\alpha^{t_2}}(x)\cdots m_{\alpha^{t_i}}(x)$ 生成的循环码为 $C_{(t_1, t_2, \dots, t_i)}$, 其中 $1 \leq t_1, \dots, t_i \leq p^m - 1$ 。近些年, 研究两个或三个零点生成的循环码的最小距离及其对偶码的重量分布是一个热门话题。2005 年, Carlet、Ding 和 Yuan [1] 首次得到了参数为 $[3^m - 1, 3^m - 2m - 1, 4]$ 循环码 $C_{(1, e)}$, 并达到了 Sphere-Packing 界。2013 年, Ding 和 Helleseht [2] 基于有限域 F_{3^m} 上的一些单项式函数构造出了几类三元最优循环码 $C_{(1, e)}$ 及其相关刻画, 并基于数学软件 Magma 搜索提出了九个公开问题。2014 年, N. Li 与 C. Li 等人 [3] 利用有限域上低次多项式求根的方法解决了文献 [2] 中的第一个公开问题。2015 年, N. Li 和 Z. Zhou 等人 [4] 通过解特定的方程解决了文献 [2] 中第二个公开问题。2019 年, Han 和 Yan [5] 解决了文献 [2] 中的三个公开问题。基于作者查阅文献, 目前为止, 就这三个问题完全得到了解决。除此之外, 许多学者围绕剩余的 6 个公开问题进行探究, 得到了特定条件下的结果与提出了新的三元最优循环码, 具体情况, 可以查阅文献 [6]-[17]。

本文利用有限域上的多变元法、因式分解与低次不可约多项式的解等数学工具, 得到了两类新的三元循环码, 其参数为 $[3^m, 3^m - 2m - 1, 4]$ 。我们的结论丰富了文献 [7] [8] 中三元最优循环码的结论。

2. 基础知识

下面, 我们给出需要用到的引理与定理:

引理 1 [3] 设 m 是正整数, 对于任意正整数 e 满足 $1 \leq e \leq 3^m - 2$ 和 $\gcd(e, 3^m - 1) \leq 2$ 。则 3-次分圆陪集 C_e 的大小为 $|C_e| = m$ 。

引理 2 [18] 设 $\gcd(n, l) = 1$, 则有限域 F_{p^m} 上 n 次多项式 $g(x)$ 不可约的充要条件是 F_{p^m} 上 n 次多项式 $g(x)$ 不可约。

定理 1 [3] 设正整数 $e \notin C_e$ 且 $|C_e| = m$, 则三元循环码 $C_{(1, e)}$ 具有参数 $[3^m - 1, 3^m - 2m - 1, 4]$ 当且仅当如下条件成立:

- 1) 正整数 e 是偶数;
- 2) 方程 $(x+1)^e - x^e - 1 = 0$ 在有限域 F_{3^m} 中仅有一解 $x = 0$;
- 3) 方程 $(x+1)^e + x^e + 1 = 0$ 在有限域 F_{3^m} 中仅有一解 $x = 1$ 。

引理 3 [19] (Sphere-Packing 界) 对于 F_p 上一个参数为 $[n, k, d]$ 的线性码, 满足下列不等式

$$\sum_{i=0}^s \binom{n}{i} (p-1)^i \leq p^{n-k},$$

其中 $s = \left\lfloor \frac{d-1}{2} \right\rfloor$ 。

当 $p = 3$, 码长为 $n = 3^m - 1$, 维数为 $k = 3^m - 1 - 2m$, 其中 $m > 1$ 。则由上面的不等式, 可得

$$\sum_{i=0}^s \binom{3^m - 1}{i} 2^i - 3^{2m} \leq 0,$$

若 $s = 1$, 则有 $\sum_{i=0}^1 \binom{3^m - 1}{i} 2^i - 3^{2m} = -3^{2m} + 2 \cdot 3^m - 1 = -3^m \cdot (3^m - 2) - 1 \leq 0$ 。

若 $s = 2$, 则有 $\sum_{i=0}^2 \binom{3^m - 1}{i} 2^i - 3^{2m} = 3^m \cdot (3^m - 4) + 3 > 0$ 。

又当 $s > 2$ 时, $\sum_{i=0}^s \binom{3^m - 1}{i} 2^i > \sum_{i=0}^2 \binom{3^m - 1}{i} 2^i$ 。

综上分析, 当 $s \leq 1$ 时, $\sum_{i=0}^s \binom{3^m - 1}{i} 2^i \leq 3^{2m}$ 才成立, 其中 $s = \left\lfloor \frac{d-1}{2} \right\rfloor$ 。当 $d \leq 4$ 时, 才有 $s \leq 1$ 。从而可

得, 若循环码 $C_{(1,e)}$ 的码长为 $n = 3^m - 1$ 与维数为 $k = 3^m - 1 - 2m$ 时, 则它的最小距离 $d \leq 4$ 。因此, 参数为 $[3^m - 1, 3^m - 2m - 1, 4]$ 的循环码 $C_{(1,e)}$ 达到了 Sphere-Packing 界, 则称该三元循环码 $C_{(1,e)}$ 是最优的。

3. 两类三元最优循环码

接下来, 首先运用有限域上的多元知识将求解的问题转化为低次多项式解的问题[7][8], 再利用因式分解与低次不可约多项式的解的结构等方法, 我们得到了两类最小距离为 4 的最优三元循环码。

定理 3: 设 m 是奇数, e 是正整数且满足 $11e \equiv 2 \cdot 3^h \pmod{3^m - 1}$, 其中 $0 \leq h \leq m - 1$ 。若有 $m \not\equiv 0 \pmod{5}$ 和 $m \not\equiv 0 \pmod{9}$, 则生成多项式为 $m_1(x)m_e(x)$ 的三元循环码 $C_{(1,e)}$ 的参数为 $[3^m - 1, 3^m - 2m - 1, 4]$ 且是最优的。

证: 因 $\gcd(3^5 - 1, 11) = 11$, 易得当 $m \not\equiv 0 \pmod{5}$ 时, $\gcd(3^m - 1, 11) = 1$ 。由同余的性质可得, $11e \equiv 2 \cdot 3^h \pmod{3^m - 1}$ 有解 e , 并且 e 是偶数, $e \notin C_1$ 。又因为 $\gcd(11e, 3^m - 1) = \gcd(2 \cdot 3^h, 3^m - 1) = 2$, 所以 $(e, 3^m - 1) = 2$ 。由引理 1, 可得 $|C_e| = m$ 。因此, 三元循环码 $C_{(1,e)}$ 的维数为 $3^m - 2m - 1$ 。

因 $m \not\equiv 0 \pmod{5}$, 可得 $\gcd(11, 3^m - 1) = 1$ 。因此, 对 $\forall x \in F_{3^m}$, 存在 $\theta, \beta \in F_{3^m}$ 使 $x + 1 = \lambda^{11}$ 和 $x = \beta^{11}$, 则有

$$\theta^{11} - \beta^{11} = 1. \quad (10)$$

下面讨论定理 1 中条件 2) 与条件 3):

由方程 $(x+1)^e - x^e - 1 = 0$, 可得 $\theta^{11e} - \beta^{11e} = 1$ 。由 $11e \equiv 2 \cdot 3^h \pmod{3^m - 1}$, 则有 $\theta^{2 \cdot 3^h} - \beta^{2 \cdot 3^h} = 1$, 从而 $\theta^2 - \beta^2 = 1$ 。设 $y = \theta + \beta$, 则由 $1 = (\theta + \beta)(\theta - \beta)$ 可得 $y \in F_{3^m}^*$ 和 $\theta - \beta = \frac{1}{y}$ 。从而, 可得 $\theta = -y - \frac{1}{y}$ 和

$\beta = -y + \frac{1}{y}$, 并代入方程(10), 则有

$$\left(-y - \frac{1}{y}\right)^{11} - \left(-y + \frac{1}{y}\right)^{11} = 1. \quad (11)$$

展开整理可得 $y^{20} + y^{11} - y^4 - 1 = 0$ 。再因式分解:

$$(y-1)^2 (y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 - 1)(y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 - y + 1) = 0$$

其中 $y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 - 1$ 与 $y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 - x + 1$ 是 F_3 上的不可约多项式。

由引理 2 可得, 当 $m \not\equiv 0 \pmod{9}$ 时, 方程(11)只有解 $y=1$ 。从而, 可得有唯一解 $x=0$ 。定理 1 中条件 2) 满足。

下面讨论方程 $(x+1)^e + x^e + 1 = 0$ 的解。

同理, 方程 $(x+1)^e + x^e + 1 = 0$ 可变形为 $\theta^{2 \cdot 3^h} + \beta^{2 \cdot 3^h} = -1$, 从而 $\theta^2 + \beta^2 = -1$ 。设 $\theta - \beta = u$ 和 $\theta\beta = v$, 则有

$$u^2 - v = -1 \quad (12)$$

注意到,

$$\begin{aligned} \theta^5 - \beta^5 &= (\theta^3 - \beta^3)(\theta^2 + \beta^2) - \theta^2 \beta^2 (\theta - \beta) = -u^3 - u \cdot v^2, \\ \theta^7 - \beta^7 &= (\theta^5 - \beta^5)(\theta^2 + \beta^2) - \theta^2 \beta^2 (\theta^3 - \beta^3) = u^3 + uv^2 - u^3 v^2, \\ \theta^9 - \beta^9 &= (\theta^7 - \beta^7)(\theta^2 + \beta^2) - \theta^2 \beta^2 (\theta^5 - \beta^5) = -u^3 - uv^2 - u^3 v^2 + uv^4, \\ \theta^{11} - \beta^{11} &= (\theta^9 - \beta^9)(\theta^2 + \beta^2) - \theta^2 \beta^2 (\theta^7 - \beta^7) = u^3 + uv^2 + uv^4 + u^3 v^4. \end{aligned}$$

从而, 可得 $u^3 + uv^2 + uv^4 + u^3 v^4 = 1$ 。联立方程(12), 则有

$$u^{11} - u^9 + u^7 - u^5 - u^3 - u + 1 = 0 \quad (13)$$

在 F_3 上因式分解可得,

$$(u-1)^5 (u^2 + u - 1)(u^4 + u^3 - u^2 - u - 1) = 0,$$

其中 $u^2 - u - 1$ 与 $u^4 - u^3 - u^2 + u - 1$ 是 F_3 上的不可约多项式。

由引理 2 可得, 当 m 是奇数时, 方程(13)只有解 $u=1$, 并代入方程(12)有 $v=-1$ 。因此, $\theta - \beta = 1$, $\theta\beta = -1$, 则有 $(\beta+1)\beta = -1$ 。从而, $\beta=1$, 可得 $x=1$ 。因此, 定理 1 中的条件 3) 满足。

综上可得, 三元循环码 $C_{(1,e)}$ 的参数为 $[3^m - 1, 3^m - 2m - 1, 4]$ 且是最优的。

例 1 设 $m=3, h=0$, α 是 $F_{3^m}^*$ 上的生成元, 且满足条件 $\alpha^3 + 2\alpha + 1 = 0$ 。则由 $11e \equiv 2 \cdot 3^h \pmod{3^m - 1}$ 可得 $e=12$ 。利用 Magma 可得, $C_{(1,e)}$ 是参数为 $[26, 20, 4]$ 的三元循环码, 其生成多项式为 $x^6 + x^5 + 2x^4 + 2x^3 + x^2 + x + 2$ 。

例 2 设 $m=7, h=0$, α 是 $F_{3^m}^*$ 上的生成元, 且满足条件 $\alpha^7 - \alpha^2 + 1 = 0$, 则由 $11e \equiv 2 \cdot 3^h \pmod{3^m - 1}$ 可得 $e=1590$ 。利用 Magma 可得, $C_{(1,e)}$ 是参数为 $[2186, 2172, 4]$ 的三元循环码, 其生成多项式为 $x^{14} + 2x^{13} + x^{12} + 2x^{11} + 2x^9 + x^8 + 2x^7 + x^5 + 2x^4 + x^2 + 2$ 。

例 3 设 $m=7, h=1$, α 是 $F_{3^m}^*$ 上的生成元, 且满足条件 $\alpha^7 - \alpha^2 + 1 = 0$, 则由 $11e \equiv 2 \cdot 3^h \pmod{3^m - 1}$ 可

得 $e = 1590$ 。利用 Magma 可得, $C_{(1,e)}$ 是参数为 $[2186, 2172, 4]$ 的三元循环码, 其生成多项式为 $x^{14} + 2x^{13} + x^{12} + 2x^{11} + 2x^9 + x^8 + 2x^7 + x^5 + 2x^4 + x^2 + 2$ 。

定理 4: 设 m 是奇数, e 是正整数且满足 $13e \equiv 2 \cdot 3^h \pmod{3^m - 1}$, 其中 $0 \leq h \leq m - 1$ 。若有 $m \not\equiv 0 \pmod{3}$, 则生成多项式为 $m_1(x)m_e(x)$ 的三元循环码 $C_{(1,e)}$ 的参数为 $[3^m - 1, 3^m - 2m - 1, 4]$ 且是最优的。

证: 因 $\gcd(3^3 - 1, 13) = 13$, 易得当 $m \not\equiv 0 \pmod{3}$ 时, $\gcd(3^m - 1, 13) = 1$ 。由同余的性质可得, $13e \equiv 2 \cdot 3^h \pmod{3^m - 1}$ 有解 e , 并且 e 是偶数, $e \notin C_1$ 。因为 $\gcd(13e, 3^m - 1) = \gcd(2 \cdot 3^h, 3^m - 1) = 2$, 所以 $(e, 3^m - 1) = 2$ 。由引理 1, 可得 $|C_e| = m$ 。因此, 三元循环码 $C_{(1,e)}$ 的维数为 $3^m - 2m - 1$ 。

因 $m \not\equiv 0 \pmod{3}$, 可得 $\gcd(13, 3^m - 1) = 1$ 。因此, 对 $\forall x \in F_{3^m}$, 存在 $\theta, \beta \in F_{3^m}$ 使 $x + 1 = \theta^{13}$ 和 $x = \beta^{13}$, 则有

$$\theta^{13} - \beta^{13} = 1. \tag{14}$$

下面讨论定理 1 中条件 2) 与条件 3):

由方程 $(x + 1)^e - x^e - 1 = 0$, 可得 $\theta^{13e} - \beta^{13e} = 1$ 。由 $13e \equiv 2 \pmod{3^m - 1}$, 则有 $\theta^{2 \cdot 3^h} - \beta^{2 \cdot 3^h} = 1$, 从而 $\theta^2 - \beta^2 = 1$ 。设 $y = \theta + \beta$, 则由 $1 = (\theta + \beta)(\theta - \beta)$ 可得 $y \in F_{3^m}^*$ 和 $\theta - \beta = \frac{1}{y}$ 。从而, 可得 $\theta = -y - \frac{1}{y}$ 和 $\beta = -y + \frac{1}{y}$, 并代入方程(14), 则有

$$\left(-y - \frac{1}{y}\right)^{13} - \left(-y + \frac{1}{y}\right)^{13} = 1. \tag{15}$$

展开整理可得 $y^{24} + y^{20} - y^{13} + y^8 + 1 = 0$ 。再因式分解:

$$(y - 1)^2 (y^3 - y + 1) (y^3 + y^2 + y - 1) (y^4 + y^3 - 1) (y^{12} - y^{10} + y^9 + y^8 + y^6 - y^5 - y^4 - y^3 - y^2 + y + 1) = 0$$

其中 $y^{12} - y^{10} + y^9 + y^8 + y^6 - y^5 - y^4 - y^3 - y^2 + y + 1$, $y^3 - y + 1$, $y^3 + y^2 + y - 1$, 与 $y^4 + y^3 - 1$ 是 F_3 上的不可约多项式。

由引理 2 可得, 当 m 是奇数与 $m \not\equiv 0 \pmod{3}$ 时, 方程(15)只有解 $y = 1$ 。从而, 可得有唯一解 $x = 0$ 。定理 1 中条件 2) 满足。

下面讨论方程 $(x + 1)^e + x^e + 1 = 0$ 的解。

同理, 方程 $(x + 1)^e + x^e + 1 = 0$ 可变形为 $\alpha^2 + \beta^2 = -1$ 。设 $\theta - \beta = u$ 和 $\theta\beta = v$, 则有

$$u^2 - v = -1. \tag{16}$$

注意到,

$$\begin{aligned} \theta^5 - \beta^5 &= (\theta^3 - \beta^3)(\theta^2 + \beta^2) - \theta^2\beta^2(\theta - \beta) = -u^3 - u \cdot v^2, \\ \theta^7 - \beta^7 &= (\theta^5 - \beta^5)(\theta^2 + \beta^2) - \theta^2\beta^2(\theta^3 - \beta^3) = u^3 + uv^2 - u^3v^2, \\ \theta^9 - \beta^9 &= (\theta^7 - \beta^7)(\theta^2 + \beta^2) - \theta^2\beta^2(\theta^5 - \beta^5) = -u^3 - uv^2 - u^3v^2 + uv^4, \\ \theta^{11} - \beta^{11} &= (\theta^9 - \beta^9)(\theta^2 + \beta^2) - \theta^2\beta^2(\theta^7 - \beta^7) = u^3 + uv^2 + uv^4 + u^3v^4, \\ \theta^{13} - \beta^{13} &= (\theta^{11} - \beta^{11})(\theta^2 + \beta^2) - \theta^2\beta^2(\theta^9 - \beta^9) = -u^3 - uv^2 + u^3v^2 - uv^6. \end{aligned}$$

从而, 可得 $-u^3 - uv^2 + u^3v^2 - uv^6 = 1$ 。联立方程(16), 则有

$$u^{13} + u^7 - u^5 - u^3 - u + 1 = 0 \tag{17}$$

在 F_3 上因式分解可得,

$$(u-1)(u^3-u^2+1)(u^9-u^8-u^5-u^3-u^2-1)=0,$$

其中 u^3-u^2+1 与 $u^9-u^8-u^5-u^3-u^2-1$ 是 F_3 上的不可约多项式。

由引理 2 可得, 当 $m \not\equiv 0 \pmod{3}$ 时, 方程(17)只有解 $u=1$, 并代入方程(16)有 $v=-1$ 。因此, $\theta-\beta=1$, $\theta\beta=-1$, 则有 $(\beta+1)\beta=-1$ 。从而, $\beta=1$, 可得 $x=1$ 。因此, 定理 1 中的条件 3) 满足。

综上可得, 三元循环码 $C_{(1,e)}$ 的参数为 $[3^m-1, 3^m-2m-1, 4]$ 且是最优的。

例 3 设 $m=5, h=0$, α 是 $F_{3^m}^*$ 上的生成元, 且满足条件 $\alpha^5+2\alpha+1=0$, 则由 $13e \equiv 2 \cdot 3^h \pmod{3^m-1}$ 可得 $e=56$ 。利用 Magma 可得, $C_{(1,e)}$ 是参数为 $[242, 232, 4]$ 的三元循环码, 其生成多项式为 $x^{10}+2x^8+x^7+x^4+x^3+2x+2$ 。

例 4 设 $m=7, h=0$, α 是 $F_{3^m}^*$ 上的生成元, 且满足条件 $\alpha^7+2\alpha^2+1=0$, 则由 $13e \equiv 2 \cdot 3^h \pmod{3^m-1}$ 可得 $e=2018$ 。利用 Magma 可得, $C_{(1,e)}$ 是参数为 $[2186, 2172, 4]$ 的三元循环码, 其生成多项式为 $x^{14}+x^{13}+2x^{11}+x^{10}+x^9+2x^6+2x^5+x+2$ 。

4. 总结

本文通过对单项式函数构造的三元循环码进行研究, 得到了两类参数为 $[3^m-1, 3^m-2m-1, 4]$ 的最优的三元循环码 $C_{(1,e)}$ 。这些最优的三元循环码丰富了已有最优三元循环码的种类。我们注意到, 具有 $e(3^h+2) \equiv 2 \pmod{3^m-1}$ 或 $e(3^h+4) \equiv 2 \pmod{3^m-1}$ 等的循环码 $C_{(1,e)}$, h 取较小值时, 也可以以类似的方式建立得到三元最优循环码。更一般性的结论, 更加复杂, 可能需要其他方法。

参考文献

- [1] Carlet, C., Ding, C. and Yuan, J. (2005) Linear Codes from Perfect Nonlinear Mappings and Their Secret Sharing Schemes. *IEEE Transactions on Information Theory*, **51**, 2089-2102. <https://doi.org/10.1109/tit.2005.847722>
- [2] Ding, C. and Helleseht, T. (2013) Optimal Ternary Cyclic Codes from Monomials. *IEEE Transactions on Information Theory*, **59**, 5898-5904. <https://doi.org/10.1109/tit.2013.2260795>
- [3] Li, N., Li, C., Helleseht, T., Ding, C. and Tang, X. (2014) Optimal Ternary Cyclic Codes with Minimum Distance Four and Five. *Finite Fields and Their Applications*, **30**, 100-120. <https://doi.org/10.1016/j.ffa.2014.06.001>
- [4] Li, N., Zhou, Z. and Helleseht, T. (2015) On a Conjecture about a Class of Optimal Ternary Cyclic Codes. 2015 *Seventh International Workshop on Signal Design and Its Applications in Communications (IWSDA)*, Bengaluru, 14-18 September 2015, 62-65. <https://doi.org/10.1109/iwsda.2015.7458415>
- [5] Han, D. and Yan, H. (2019) On an Open Problem about a Class of Optimal Ternary Cyclic Codes. *Finite Fields and Their Applications*, **59**, 335-343. <https://doi.org/10.1016/j.ffa.2019.07.002>
- [6] Zha, Z. and Hu, L. (2020) New Classes of Optimal Ternary Cyclic Codes with Minimum Distance Four. *Finite Fields and Their Applications*, **64**, Article ID: 101671. <https://doi.org/10.1016/j.ffa.2020.101671>
- [7] Fan, J. and Wang, B. (2022) Two Families of Optimal Ternary Cyclic Codes with Two Zeros. *IEEE Access*, **10**, 72290-72300. <https://doi.org/10.1109/access.2022.3188696>
- [8] Fan, C., Li, N. and Zhou, Z. (2016) A Class of Optimal Ternary Cyclic Codes and Their Duals. *Finite Fields and Their Applications*, **37**, 193-202. <https://doi.org/10.1016/j.ffa.2015.10.004>
- [9] Wang, L. and Wu, G. (2016) Several Classes of Optimal Ternary Cyclic Codes with Minimal Distance Four. *Finite Fields and Their Applications*, **40**, 126-137. <https://doi.org/10.1016/j.ffa.2016.03.007>
- [10] Zha, Z., Hu, L., Liu, Y. and Cao, X. (2021) Further Results on Optimal Ternary Cyclic Codes. *Finite Fields and Their Applications*, **75**, 101898. <https://doi.org/10.1016/j.ffa.2021.101898>
- [11] Yan, H., Zhou, Z. and Du, X. (2018) A Family of Optimal Ternary Cyclic Codes from the Niho-Type Exponent. *Finite Fields and Their Applications*, **54**, 101-112. <https://doi.org/10.1016/j.ffa.2018.08.004>
- [12] Zhou, Z. and Ding, C. (2014) A Class of Three-Weight Cyclic Codes. *Finite Fields and Their Applications*, **25**, 79-93. <https://doi.org/10.1016/j.ffa.2013.08.005>
- [13] Liu, Y., Cao, X. and Lu, W. (2023) Two Classes of New Optimal Ternary Cyclic Codes. *Advances in Mathematics of Communications*, **17**, 979-993. <https://doi.org/10.3934/amc.2021033>

- [14] He, C., Ran, X. and Luo, R. (2024) Two Classes of Optimal Ternary Cyclic Codes with Minimum Distance Four. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **107**, 1049-1052. <https://doi.org/10.1587/transfun.2023eal2055>
- [15] Wu, G., You, Z., Zha, Z. and Zhang, Y. (2024) Several New Classes of Optimal Ternary Cyclic Codes with Two or Three Zeros. arXiv: 2407.07332. <https://arxiv.org/abs/2407.07332>
- [16] 李念. 高非线性函数的构造及其在序列编码中的应用[D]: [博士学位论文]. 成都: 西南交通大学, 2014.
- [17] 聂浏杰. 几类极小距离为 4 的三元最优循环码[D]: [硕士学位论文]. 武汉: 湖北大学, 2021.
- [18] Lidl, R. and Niederreiter, H. (1996) *Finite Fields*. 2nd Edition, Cambridge University Press. <https://doi.org/10.1017/cbo9780511525926>
- [19] Huffman, W.C. and Pless, V. (2003) *Fundamentals of Error-Correcting Codes*. Cambridge University Press. <https://doi.org/10.1017/cbo9780511807077>