**Pure Mathematics** 理论数学, 2024, 14(8), 12-19
Published Online August 2024 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2024.148298

Hans汉斯

# 一类最小距离为4的三元最优循环码

**曾学强[1]，何　潮[2]**

[1]四川轻化大学数学与统计学院，四川　自贡
[2]四川职业技术学院教师教育学院，四川　遂宁

收稿日期：2024年5月23日；录用日期：2024年7月1日；发布日期：2024年8月13日

## 摘　要

**循环码作为线性码的一个重要子类，具有良好的通信性质和重要的应用意义。利用有限域上因式分解、低次不可约多项式的解等数学工具，从循环码生成多项式的角度研究具有两个零点的三元循环码，得到了一类最小距离为4的三元循环码，并且它们关于Sphere-Packing界是最优的。**

## 关键词

**有限域，循环码，不可约多项式，最小距离**

# A Class of Ternary Optimal Cyclic Codes with Minimum Distance 4

**Xueqiang Zeng[1], Chao He[2]**

[1]College of Mathematics and Statistics, Sichuan University of Science & Engineering, Zigong Sichuan
[2]College of Teacher Education, Sichuan Vocational and Technical College, Suining Sichuan

Received: May 23rd, 2024; accepted: Jul. 1st, 2024; published: Aug. 13th, 2024

## Abstract

**As an important subclass of linear codes, cyclic code has good communication properties and important application significance. By using mathematical tools such as factorization over finite field, solutions of low order irreducible polynomial, ternary cyclic code with two zeros are studied from the perspective of generating polynomials of cyclic code. A class of ternary cyclic code with minimum distance of 4 is obtained, and it is optimal with respect to Sphere Packing bounds.**

文章引用: 曾学强, 何潮. 一类最小距离为 4 的三元最优循环码[J]. 理论数学, 2024, 14(8): 12-19.
DOI: 10.12677/pm.2024.148298

**Keywords**

**Finite Field, Cyclic Code, Irreducible Polynomial, Minimum Distance**



## 1. 引言

1957 年，Prange 首次提出循环码的概念。随后，他对循环码进行了更深入的研究，并提出了一些译码算法。此后，编码理论有了迅速的发展，尤其是循环码理论。比如 BCH 码，这类码被广泛应用于储存系统和通信系统中。除此之外，循环码还可以用来构造其它的码、秘钥共享方案[1] [2]、跳频序列[3] [4]等。

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分析、研究码的结构，并在工程上找到实用的译码算法；二是循环码的编译码运算可用移位寄存器实现，硬件实现简单。因此，循环码被广泛运用于数据传输、广播系统和计算机软件中。总之，在纠错编码理论中，循环码理论的研究具有很重要的意义。

设 $n$ 是正整数， $q=p^m$ ，其中 $p$ 是素数，$m$ 是正整数，且 $\gcd(n,q)=1$。再设 $\mathcal{C}$ 表示 $F_q$ 上码长为 $n$ 的循环码，则循环码 $\mathcal{C}$ 是环 $F_q[x]/(x^n-1)$ 的一个理想，且可表示成

$$\mathcal{C}=\langle g(x)\rangle,$$

其中 $g(x)$ 是 $F_q[x]$ 中次数最低且首项系数为 1 的多项式。多项式 $g(x)$ 称为 $\mathcal{C}$ 的生成多项式，$h(x)=(x^n-1)/g(x)$ 为 $\mathcal{C}$ 的校验多项式。设 $m_{\alpha^i}(x)$ 是 $\alpha^i$ 在 $F_p$ 上的极小多项式，其中 $\alpha$ 是 $F_{p^m}^*=F_{p^m}\setminus\{0\}$ 上的一个生成元。再设 $\mathcal{C}_{(1,e)}$ 表示 $F_p$ 上由生成多项式 $m_\alpha(x)m_{\alpha^e}(x)$ 生成的循环码，其中 $1\le e\le p^m-1$ 和 1、$e$ 在不同的分圆陪集。2005 年，Carlet、Ding 和 Yuan [1]证明了参数为 $[3^m-1,3^m-2m-1,4]$ 三循环码 $\mathcal{C}_{(1,e)}$ 是最优的(根据 Sphere-Packing 界)，其中 $p=3$，$e$ 是使 $x^e$ 是完全非线性单项式的整数。2013 年，Ding 和 Helleseth [5]使用 $F_{3^m}$ 上一些单项式 $x^e$，构造了几类三元最优循环码，并提出了 9 个公开问题。基于作者的了解，文献[5]中的 9 个公开问题，目前为主，完全解决的了三个。在 2014 年，N. Li 与 C. Li 等人[6]解决了文献[5]中的第一个公开问题，其中指数为 $(1,2(3^{m-1}-1))$。2015 年，N. Li 和 Z. Zhou 等人[7]解决了第二个公开问题，其中指数为 $(1,2(3^h+1))$。2019 年，Han 和 Yan [8]解决了三个公开问题，其中指数为 $(1,3^h+5)$。与此同时，许多学者围绕三元循环码的 9 个问题进行探究，给出了特定条件下的结果或提出了新的三元最优循环码，具体情况，请参考文献[9]-[19]。

本文利用有限域上因式分解、低次不可约多项式的解等数学工具，得到了一类新的三元循环码，其参数为 $[3^m,3^m-2m-1,4]$。我们的结论丰富了已有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** [5]设 $m$ 是正整数，对于任意正整数 $e$ 满足 $1\le e\le 3^m-2$ 和 $\gcd(e,3^m-1)\le 2$。则 3-次分圆陪集 $C_e$ 的大小为 $|C_e|=m$。

**引理 2** [20]设 $q$ 是一素数方幂，$g(x)$ 是 $F_q[x]$ 上任一多项式，则对任意的多项式 $f(x)\in F_q[x]$，必存在多项式 $h(x)r(x)\in F_q[x]$ 使得 $f(x)=g(x)h(x)+r(x)$ 成立，其中 $\deg(r(x))<\deg(g(x))$ 且有 $\gcd(f(x),g(x))=\gcd(g(x),r(x))$。

**引理 3** [20]设 $q$ 是一素数方幂，对于任一有限域 $F_q$ 以及任一正整数 $n$，所有 $F_q[x]$ 上次数整除 $n$ 的首一不可约多项式乘积等于 $x^{q^n}-x$。

为了说明如何运用引理 3，本节给出以下实例。设 $f(x)=x^7-x^6+x^4-x^3+x^2+1\in F_3[x]$，运用引理 2，可得多项式最大公因子等式 $\gcd(f(x),x^3-x)=\gcd(f(x),x^{3^2}-x)=1$，$\gcd(f(x),x^{3^3}-x)=x^3-x-1$ 和 $\gcd(f(x),x^{3^4}-x)=x^4-x^3+x^2+x-1$，于是利用引理 3 可知，多项式 $f(x)$ 含有三次与四次不可约因子 $x^3-x-1$ 与 $x^4-x^3+x^2+x-1$，此即意味着多项式 $f(x)$ 可以因式分解为 $f(x)=(x^3-x-1)(x^4-x^3+x^2+x-1)$。

**引理 4** [20]设 $q$ 是一素数方幂且 $f(x)$ 是有限域 $F_q$ 上次数为 $n$ 的不可约多项式，则 $f(x)=0$ 在有限域 $F_q^n$ 中有一解 $x$ 且 $f(x)=0$ 在有限域 $F_q^n$ 中的 $n$ 个不同的解分别为 $x,x^q,x^{q^2},\cdots,x^{q^{n-1}}$。

给定有限域 $F_q$ 上方程 $f(x)=0$，若能将多项式 $f(x)$ 分解成不可约多项式的乘积，则利用引理 4 可判断其方程解的情况。如取 $f(x)=x^2+x-1\in F_3[x]$，由 $f(0)=2\neq 0$，$f(1)=1\neq 0$ 和 $f(2)=f(-1)=2\neq 0$ 可知，多项式 $f(x)$ 在 $F_3[x]$ 上是不可约多项式，从而利用引理 4 可知，方程 $f(x)=0$ 在有限域 $F_{3^m}$ 中有解当且仅当 $m\neq 0(\bmod 2)$。

**引理 5** [21] (Sphere-Packing 界)对 $F_p$ 上一个参数为 $[n,k,d]$ 的线性码，其满足下面的不等式

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

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

当 $p=3$，长度 $n=p^m-1$，维数 $k=p^m-1-2m$，验证上面的不等式，可得最小距离 $d$ 不超过 4，且当 $d=4$ 时，有 $p^{n-k}=\sum_{i=0}^{t}\binom{n}{i}(p-1)^i$，称线性码 $\mathcal{C}$ 是最优的。

## 3. 三元循环码 $\mathcal{C}_{(t,e)}$ 的构造

设 $n=3^m-1$，$m$ 是整数，且 $e,(1<e\leq n-1)$ 满足 $e\notin C_1$ 的整数，则 $F_3$ 上一个 $n$ 长循环码 $\mathcal{C}_{(1,e)}$ 定义如下：

$$C_{(1,e)}=\langle m_1(x)m_e(x)\rangle,$$

其中 $\alpha$ 是 $F_{3^m}^*=F_{3^m}\setminus\{0\}$ 上的生成元，$m_1(x)$、$m_e(x)$ 分别是 $\alpha^1$、$\alpha^e$ 在 $F_3$ 的极小多项式。

从而，可得循环码 $\mathcal{C}_{(1,e)}$ 的参数为 $[3^m-1,3^m-1-m-|C_e|,d]$，其中 $|C_e|$ 分别为 $e$ 所对应的分圆陪集的大小，$d$ 为循环码 $\mathcal{C}_{(1,e)}$ 的最小距离。

参数为 $[3^m-1,3^m-2m-1,4]$ 的循环码 $\mathcal{C}_{(1,e)}$ 是达到了 Sphere-Packing 界，则三元循环码 $\mathcal{C}_{(1,e)}$ 是最优的。在数据库中，我们可在著名的线性码表的集合 Markus Grassl (http://www.codetables.de/)上查相应的信息。

## 4. 三元最优循环码

文献[15]中研究了一类由指数为 $(t,e)=\left(\frac{3^m+1}{2},3^r+2\right)$ 确定的三元最优循环码。对于指数 $(t,e)=\left(\frac{3^m+1}{2},3^r-2\right)$ 确定的三元循环码是否是最优的呢？接下来，利用 $F_3$ 上因式分解与低次不可约多项

式的解的结构，基于 Sphere-Packing 界探讨指数为 $(t,e)=\left(\frac{3^m+1}{2},3^r-2\right)$ 的三元循环码 $\mathcal{C}_{(t,e)}$ 的最优性。

**定理 6：**设 $m>1$ 是奇数，$t=\frac{3^m+1}{2}$，$e=3^r-2$。若 $m\not\equiv 0(\bmod 5)$ 与 $2r\equiv 1(\bmod m)$，则三元循环码 $\mathcal{C}_{(t,e)}$ 的参数为 $\left[3^m-1,3^m-2m-1,4\right]$ 且是最优的。

证：因 $m$ 是奇数，易得 $\gcd\left(\frac{3^m+1}{2},3^m-1\right)=2$。由引理 1，可得 $|C_t|=m$。又因 $2r\equiv 1(\bmod m)$，则有 $\gcd\left(3^{2r}-4,3^m-1\right)=\gcd\left(3^{m+1}-4,3^m-1\right)=1$。从而，可得 $\gcd\left(3^r-2,3^m-1\right)=1$。同理可得 $|C_e|=m$。易得，$\frac{3^m+1}{2}$ 是偶数，$3^r-2$ 是奇数。因此，三元循环码 $\mathcal{C}_{(1,e)}$ 的维数为 $3^m-2m-1$。

现证明最小距离 $d=4$。由三元循环码 $\mathcal{C}_{(t,e)}$ 的定义，$\mathcal{C}_{(t,e)}$ 没有汉明距离 $\omega$ 的码字当且仅存在 $\omega$ 个非零元素 $c_1,c_2,\cdots,c_\omega\in F_3$ 和 $k$ 个非零的不同元素 $x_1,x_2,\cdots,x_\omega\in F_{3^m}$，使方程组

$$\begin{cases}c_1x_1^t+c_2x_2^t+\cdots+c_\kappa x_\omega^t=0,\\ c_1x_1^e+c_2x_2^e+\cdots+c_\kappa x_\omega^e=0\end{cases}\tag{1}$$

在 $F_{3^m}$ 无解。

现证明三元循环码 $\mathcal{C}_{(t,e)}$ 没有汉明距离 $\omega=3$ 的码字。设 $x=\frac{x_1}{x_2},y=\frac{x_3}{x_1}$，其中 $x,y\neq 0,1$ 与 $x\neq y$。方程组(1)变形为

$$\begin{cases}c_1x^t+c_2y^t+c_3=0,\\ c_1x^e+c_2y^e+c_3=0.\end{cases}\tag{2}$$

因为方程组(2)的对称性，从两种情形讨论方程组(1)在 $F_{3^m}$ 中解的情况：

情形一：当 $c_1=c_2=c_3=1$ 时，则有

$$\begin{cases}x^t+y^t+1=0,\\ x^e+y^e+1=0.\end{cases}\tag{3}$$

注意到 $t=\frac{3^m+1}{2}=\frac{3^m-1}{2}+1$，当 $\alpha$ 是 $F_{3^m}^*$ 中的平方元，则有 $\alpha^t=\alpha$；当 $\alpha$ 是 $F_{3^m}^*$ 中的平方元，则有 $\alpha^t=-\alpha$。我们分下面 4 中情况，证明方程组(3)在 $F_{3^m}\setminus\{0,1\}$ 中无解。

(I) $x,y$ 是 $F_{3^m}^*$ 中的平方元。则方程组(3)可变形为

$$\begin{cases}x+y+1=0,\\ x^e+y^e+1=0.\end{cases}\tag{4}$$

代入消元可得 $(x+1)^e=x^e+1$，再两边同时乘以 $x^2(x+1)^2$ 可得：

$$x^2(x+1)^{3^r}=(x+1)^2x^{3^r}+x^2(x+1)^2$$

展开整理，并因式分解可得 $x^3(x-1)\left(x^{3^r-1}-1\right)=0$。从而，$x=0$ 或 $x=1$ 或 $x^{3^r-1}=1$。因 $m$ 是奇数与 $2r\equiv 1(\bmod m)$，易得 $\gcd(r,m)=1$，从而 $\gcd\left(3^r-1,3^m-1\right)=2$。因此，$x^{3^r-1}=1$，可得 $x=\pm 1$。若 $x=-1$，由方程组(3)的第一个方程可得 $y=0$，这与 $y\neq 0$ 矛盾。从而，方程组(4)在 $F_{3^m}\setminus\{0,1\}$ 中无解。

(II) $x,y$ 是 $F_{3^m}^*$ 中的非平方元。则方程组(3)可变形为

$$\begin{cases} x+y-1=0, \\ x^e+y^e+1=0. \end{cases} \tag{5}$$

代入消元可得 $(x-1)^e=x^e+1$，再两边同时乘以 $x^2(x-1)^2$ 可得：

$$x^2(x-1)^{3^r}=(x-1)^2x^{3^r}+x^2(x-1)^2$$

展开整理可得 $x^{3^r}(x+1)=x^2-x^3-x^4$。

注意到，$x+1\neq 0$。否则，$x=-1$，由方程组(5)的第一个方程可得 $y=-1$，这与 $x\neq y$ 矛盾。因此，则有

$$x^{3^r}=\frac{x^2-x^3-x^4}{x+1}:=\frac{f(x)}{g(x)}. \tag{6}$$

其中 $f(x)=x^2-x^3-x^4$，$g(x)=x+1$。再方程(6)两边取 $3^r$ 幂，则有

$$x^{3^{2r}}=\frac{x^{2\cdot 3^r}-x^{3\cdot 3^r}-x^{4\cdot 3^r}}{x^{3^r}+1}. \tag{7}$$

把方程(6)代入方程(7)，可得

$$x^{3^{2r}}=\frac{g(x)^2f(x)^2-g(x)f(x)^3-f(x)^4}{f(x)g(x)^3+g(x)^4}.$$

注意到 $2r\equiv 1(\mathrm{mod}\,m)$，则有 $x^{3^{2r}}=x^3$，从而

$$x^3\left(f(x)g(x)^3+g(x)^4\right)=g(x)^2f(x)^2-g(x)f(x)^3-f(x)^4. \tag{8}$$

整理可得：

$$\begin{aligned} 0&=x^3\left(f(x)g(x)^3+g(x)^4\right)-g(x)^2f(x)^2+g(x)f(x)^3+f(x)^4 \\ &=x^{16}+x^{15}-x^{14}-x^{11}-x^{10}-x^9+x^8-x^6+x^5+x^3 \\ &=x^3\cdot\left(x^{13}+x^{12}-x^{11}-x^8-x^7-x^6+x^5-x^3+x^2+1\right) \\ &=x^3\cdot\varphi(x) \end{aligned}$$

其中 $\varphi(x)=x^{13}+x^{12}-x^{11}-x^8-x^7-x^6+x^5-x^3+x^2+1$。

又 $\gcd\left(\varphi(x),x^3-x\right)=\gcd\left(\varphi(x),x^{3^3}-x\right)=\gcd\left(\varphi(x),x^{3^4}-x\right)=x-1$，可得多项式 $\varphi(x)$ 中含有 1 次不可约因子 $x+1$，不含有 2 次、3 次、4 次不可约因子。由 $\gcd\left(\varphi(x),x^{3^5}-x\right)=x^{11}+x^9-x^8-x^5-x^3+x^2-x+1$，可得多项式 $\varphi(x)$ 含有两个 5 次不可约因子。因此，多项式 $\varphi(x)$ 中含有 $(x-1)^3$ 的因子。由引理 2，可得 $\varphi(x)=(x-1)^3\cdot\left(x^{10}+x^9-x^8+x^7+x^6+x^5-x^2-1\right)$，其中多项式 $x^{10}+x^9-x^8+x^7+x^6+x^5-x^2-1$ 为 $F_3$ 上的两个 5 次不可约多项式的乘积。再因式分解，可得 $\varphi(x)=(x-1)^3\left(x^5-x^3-x^2+x+1\right)\left(x^5+x^4+x-1\right)$。因此，由(8)可得

$$x^3(x-1)^3\left(x^5-x^3-x^2+x+1\right)\left(x^5+x^4+x-1\right)=0 \tag{9}$$

其中 $x^5-x^3-x^2+x+1$ 与 $x^5+x^4+x-1$ 是 $F_3$ 上的不可约多项式。由引理 4 可得，当 $m\neq 0(\mathrm{mod}\,5)$，方程(9)在 $F_{3^m}\setminus\{0,1\}$ 中无解。因此，方程组(5)在 $F_{3^m}\setminus\{0,1\}$ 中无解。

(III) $x$ 是 $F_{3^m}^*$ 中的平方元，$y$ 是 $F_{3^m}^*$ 中的非平方元。则方程组(3)可变形为

$$\begin{cases} x-y+1=0, \\ x^e+y^e+1=0. \end{cases} \tag{10}$$

代入消元可得 $(x+1)^e+x^e+1=0$，再两边同时乘以 $x^2(x+1)^2$ 可得：

$$x^2(x+1)^{3^r}+(x+1)^2x^{3^r}+x^2(x+1)^2=0.$$

展开整理可得 $x^{3^r}(x^2+x-1)=x^4-x^3-x^2$。

注意到，$x^2+x-1\neq 0$。若 $x^2+x-1=0$，则有 $x^4-x^3-x^2=0$，从而 $x=0$。这与前提矛盾。因此，则有

$$x^{3^r}=\frac{x^4-x^3-x^2}{x^2+x-1}:=\frac{f(x)}{g(x)}.$$

其中 $f(x)=x^4-x^3-x^2$，$g(x)=x^2+x-1$。再方程两边取 $3^r$ 幂，则有

$$x^{3^{2r}}=\frac{x^{4\cdot 3^r}-x^{3\cdot 3^r}-x^{2\cdot 3^r}}{x^{2\cdot 3^r}+x^{3^r}-1}.$$

注意到 $2r\equiv 1(\mathrm{mod}\, m)$，则有 $x^{3^{2r}}=x^3$，从而

$$x^3\left(f(x)^2g(x)^2+g(x)^3f(x)-g(x)^4\right)=f(x)^4-f(x)^3g(x)-f(x)^2g(x)^2. \tag{11}$$

整理可得：

$$\begin{aligned} 0&=x^3\left(f(x)^2g(x)^2+g(x)^3f(x)-g(x)^4\right)-f(x)^4+f(x)^3g(x)+f(x)^2g(x)^2 \\ &=-x^{16}-x^{15}-x^{14}+x^{12}+x^{11}+x^8+x^7-x^5-x^4-x^3 \\ &=-x^3\cdot\left(x^{13}+x^{12}+x^{11}-x^9-x^8-x^5-x^4+x^2+x+1\right) \\ &=-x^3\cdot h(x) \end{aligned}$$

其中 $h(x)=x^{13}+x^{12}+x^{11}-x^9-x^8-x^5-x^4+x^2+x+1$。

又 $\gcd(h(x),x^3-x)=\gcd(h(x),x^{3^3}-x)=\gcd(h(x),x^{3^4}-x)=x+1$，可得多项式 $h(x)$ 中含有 1 次不可约因子 $x+1$，不含有 2 次、3 次、4 次不可约因子。由 $\gcd(h(x),x^{3^5}-x)=x^{11}-x^{10}-x^9-x^6-x^5-x^2-x+1$，可得多项式 $h(x)$ 含有两个 5 次不可约因子。因此，多项式 $h(x)$ 中含有 $(x+1)^3$ 的因子。由引理 2，可得 $h(x)=(x+1)^3\left(x^{10}+x^9+x^8-x^7+x^6+x^5+x^4-x^3+x^2+x+1\right)$，其中多项式 $x^{10}+x^9+x^8-x^7+x^6+x^5+x^4-x^3+x^2+x+1$ 为 $F_3$ 上的两个 5 次不可约多项式的乘积。再因式分解，可得 $h(x)=(x+1)^3\left(x^5+x^3+x+1\right)\left(x^5+x^4+x^2+1\right)$。因此，由(11)可得

$$x^3(x+1)^3\left(x^5+x^3+x+1\right)\left(x^5+x^4+x^2+1\right)=0, \tag{12}$$

其中 $x+1$、$x^5+x^3+x+1$ 与 $x^5+x^4+x^2+1$ 是 $F_3$ 上的不可约多项式。

因此，由引理 4 可得，当 $m\neq 0(\mathrm{mod}\, 5)$，方程(12)有解 $x=0$ 或 $x=-1$。若 $x=-1$，由方程组(10)的第一个方程可得 $y=0$，这与 $y\neq 0$ 矛盾。因此，方程组(10)在 $F_{3^m}\setminus\{0,1\}$ 中无解。

(IV) $x$ 是 $F_{3^m}^*$ 中的非平方元，$y$ 是 $F_{3^m}^*$ 中的平方元。这种情况类似于情形一的情况(III)，方程组在 $F_{3^m}\setminus\{0,1\}$ 中无解。

情形二：当 $c_1=c_2=1, c_3=-1$ 时，则有

$$\begin{cases} x+y-1=0, \\ x^e+y^e-1=0. \end{cases} \tag{13}$$

注意到 $t$ 是偶数，$e$ 是奇数。设 $\bar{x}=-x,\bar{y}=-y$。则有

$$\begin{cases}\bar{x}+\bar{y}-1=0,\\ \bar{x}^e+\bar{y}^e+1=0.\end{cases}$$

因此，该情形的讨论类似情形一，可得方程组(13)在 $F_{3^m}\setminus\{0,1\}$ 中无解。

综上可得，该三元循环码 $\mathcal{C}_{(t,e)}$ 没有汉明距离 $\omega=3$ 的码字，最小距离 $d\geq 4$。

由 Sphere-Packing 界知，码长为 $n=3^m-1$ 与维数 $k=3^m-2m-1$ 的三元循环码的最小距离 $d\leq 4$。因此，三元循环码 $\mathcal{C}_{(1,e)}$ 的最小距离为 4。此时，三元循环码 $\mathcal{C}_{(1,e)}$ 参数为 $\left[3^m-1,3^m-2m-1,4\right]$，达到了 Sphere-Packing 界，是最优的。

例 1 设 $m=3,r=1$，$\alpha$ 是 $F_{3^m}^*$ 上的生成元，且满足条件 $\alpha^3-\alpha+1=0$。利用 Magma 可得，$\mathcal{C}_{(1,e)}$ 是参数为 $\left[26,20,4\right]$ 的三元循环码，其生成多项式为 $x^6+x^5+x^4+2x^3+2$。

例 2 设 $m=7,r=4$，$\alpha$ 是 $F_{3^m}^*$ 上的生成元，且满足条件 $\alpha^7+2\alpha^2+1=0$。利用 Magma 可得，$\mathcal{C}_{(1,e)}$ 是参数为 $\left[2186,2172,4\right]$ 的三元循环码，其生成多项式为

$$x^{14}+2x^{13}+x^{12}+2x^{10}+2x^9+x^8+x^7+x^6+x^5+x^4+x+2.$$

## 5. 总结

本文通过对单项式函数构造的三元循环码进行研究，得到了三类参数为 $\left[3^m-1,3^m-2m-1,4\right]$ 的三循环码 $\mathcal{C}_{(1,e)}$，并达到了 Sphere-Packing 界。通过与文献[13]相比较，我们得到了新的一类最优三元循环码，这类最优三元循环码丰富了已有三元最优循环码的种类。

## 基金项目

有限域上几类三元最优循环码的研究，四川职业技术学院科研校级项目(2022YBO12)；三元最优循环码及性质的研究，桥梁无损检测与工程计算四川省高校重点实验室 2023 年度开放基金项目(2023QYY08)。

## 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 Salomaa, A. (2006) Secret Sharing Schemes with Nice Access Structures. *Fundamenta Informaticae*, **71**, 65-79.

[3] Ding, C., Fuji-Hara, R., Fujiwara, Y., Jimbo, M. and Mishima, M. (2009) Sets of Frequency Hopping Sequences: Bounds and Optimal Constructions. *IEEE Transactions on Information Theory*, **55**, 3297-3304. https://doi.org/10.1109/tit.2009.2021366

[4] Ding, C., Yang, Y. and Tang, X. (2010) Optimal Sets of Frequency Hopping Sequences from Linear Cyclic Codes. *IEEE Transactions on Information Theory*, **56**, 3605-3612. https://doi.org/10.1109/tit.2010.2048504

[5] Ding, C. and Helleseth, T. (2013) Optimal Ternary Cyclic Codes from Monomials. *IEEE Transactions on Information Theory*, **59**, 5898-5904. https://doi.org/10.1109/tit.2013.2260795

[6] Li, N., Li, C., Helleseth, 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

[7] Li, N., Zhou, Z. and Helleseth, 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

[8] 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

[9] Zha, Z. and Hu, L. (2020) New Classes of Optimal Ternary Cyclic Codes with Minimum Distance Four. *Finite Fields and Their Applications*, **64**, Article 101671. https://doi.org/10.1016/j.ffa.2020.101671

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] Zha, Z., Hu, L., Liu, Y. and Cao, X. (2021) Further Results on Optimal Ternary Cyclic Codes. *Finite Fields and Their Applications*, **75**, Article 101898. https://doi.org/10.1016/j.ffa.2021.101898

[16] 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

[17] Zhao, H., Luo, R. and Sun, T. (2022) Two Families of Optimal Ternary Cyclic Codes with Minimal Distance Four. *Finite Fields and Their Applications*, **79**, Article 101995. https://doi.org/10.1016/j.ffa.2022.101995

[18] 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.

[19] 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.

[20] Lidl, R. and Niederreiter, H. (1996) Finite Fields. 2nd Edition, Cambridge University Press. https://doi.org/10.1017/cbo9780511525926

[21] Huffman, W.C. and Pless, V. (2003) Fundamentals of Error Correcting Codes. Cambridge University Press. https://doi.org/10.1017/CBO9780511807077