Pure Mathematics 理论数学, 2026, 16(4), 252-261
Published Online April 2026 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2026.164110

Hans汉斯

一类最优7-元循环码

张　鲜[1]，黄月梅[1,2,3*]

[1]内蒙古师范大学数学科学学院，内蒙古　呼和浩特
[2]内蒙古自治区应用数学中心，内蒙古　呼和浩特
[3]无穷维哈密尔顿系统及其算法应用教育部重点实验室，内蒙古　呼和浩特

收稿日期：2026年3月10日；录用日期：2026年4月16日；发布日期：2026年4月27日

摘　要

基于其丰富的代数结构和高效的实现，有限域上的循环码成为编码理论中的一个热门课题。虽然二元和三元循环码已被广泛研究，但诸如$\mathbb{F}_7$等更大域上的码字研究还相对较少。根据已有判定七元循环码最优性的方法，构造出参数为$\left[7^m-1,7^m-2m-2,4\right]$的最优7-元循环码。对比现有构造，本文的参数选取条件给出了新的不相交的码族，丰富了更高阶循环码的最优构造理论。

关键词

有限域，完美非线性函数，最小距离，球填充界，循环码

A Class of Optimal 7-Ary Cyclic Codes

Xian Zhang[1], Yuemei Huang[1,2,3*]

[1]College of Mathematics Science, Inner Mongolia Normal University, Hohhot Inner Mongolia
[2]Inner Mongolia Autonomous Region Center for Applied Mathematics, Hohhot Inner Mongolia
[3]Laboratory of Infinite-Dimensional Hamiltonian System and Its Algorithm Application, Hohhot Inner Mongolia

Received: March 10, 2026; accepted: April 16, 2026; published: April 27, 2026

Abstract

Due to the rich algebraic structures and efficient implementations, cyclic codes over finite fields have become a popular topic in coding theory. While binary and ternary cyclic codes have been extensively studied, research on codes over larger fields, such as $\mathbb{F}_7$, remains relatively limited. Using a verified method for determining the optimality of 7-ary cyclic codes, we constructs a new 7-ary

*通讯作者。

文章引用: 张鲜, 黄月梅. 一类最优 7-元循环码[J]. 理论数学, 2026, 16(4): 252-261.
DOI: 10.12677/pm.2026.164110

cyclic codes with parameters $\left[7^m-1,7^m-2m-2,4\right]$. Compared with existing constructions, the parameter selection conditions in this paper yield a new disjoint family of codes, thereby enriching the theory of optimal constructions for higher-order cyclic codes.

Keywords

Finite Field, Perfect Nonlinear Function, Minimum Distance, Sphere Packing Bound, Cyclic Codes

1. 引言

源于其良好的代数性质以及其由线性反馈移位寄存器带来的实现友好性，循环码成为编码理论重要研究对象之一。

设 $\mathbb{F}_{p^m}$ 为含有 p^m 个元素的有限域，其中 p 是素数，m 为正整数。一个 p 元 $[n,k,d]$ 线性码 $\mathcal{C}$ 是 $\mathbb{F}_{p^m}$ 的一个 k 维子空间，且最小距离为 d。若 $\mathcal{C}$ 中任意码字的循环移位仍是 $\mathcal{C}$ 中的码字，则称线性码 $\mathcal{C}$ 为循环码。若将码字 $(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$ 与多项式 $c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in\frac{\mathbb{F}_p[x]}{(x^n-1)}$ 对应，则 $\mathcal{C}$ 是循环码当且仅当它是环 $\frac{\mathbb{F}_p[x]}{(x^n-1)}$ 的一个理想。此外，循环码 $\mathcal{C}$ 中次数最低的首一多项式 $g(x)$，满足 $\mathcal{C}=\langle g(x)\rangle$，称为生成多项式。

模 $n=p^m-1$ 的包含 $j\left(0\le j\le n-1\right)$ 的 p-分圆陪集定义为

$$C_j=\left\{j\cdot p^i\left(\mathrm{mod\ n}\right):0\le i\le l_j-1\right\},$$

其中 l_j 是满足 $p^{l_j}\cdot j\equiv j\left(\mathrm{mod}\,p^m-1\right)$ 的最小正整数，且记 $\left|C_j\right|=l_j$。设 α 是 $\mathbb{F}_{p^m}^*$ 的一个生成元，且 $m_{\alpha^j}(x)$ 是 α^j 在 $\mathbb{F}_p$ 上的极小多项式，对于任意 $0\le j\le n-1$，有 $m_{\alpha^j}(x)=\prod_{i\in C_j}\left(x-\alpha^i\right)$。对于 r 个不同的 p-分圆陪集 $C_{j_1},C_{j_2},\cdots,C_{j_r}$，$\mathcal{C}_{(j_1,j_2,\cdots,j_r)}$ 表示以 $m_{\alpha^{j_1}}(x)\cdot m_{\alpha^{j_2}}(x)\cdots m_{\alpha^{j_r}}(x)$ 为生成多项式的循环码，其中 $j_1\in C_{j_1},j_2\in C_{j_2},\cdots,j_r\in C_{j_r}$。

给定长度和维数时，寻找具有最大或最小距离的循环码至关重要[1] [2]。近几十年来，研究者们根据有限域构造了许多的最优循环码[3]-[6]。Carlet 等[7]利用完美非线性(PN)函数 x^e，提出了一些参数为 $\left[3^m-1,3^m-2m-1,4\right]$ 的最优三元循环码 $\mathcal{C}_{(1,e)}$。Ding 等[8]使用几乎完美非线性(APN)函数及 $\mathbb{F}_{3^m}$ 上的其他单项式，构造了具有相同参数 $\left[3^m-1,3^m-2m-1,4\right]$ 的最优码 $\mathcal{C}_{(1,e)}$。文献[9]和[10]分别在其表 1 和表 2 中列出了已知的指数 e 的值及对应的最优三元循环码 $\mathcal{C}_{(1,e)}$ 和 $\mathcal{C}_{(u,v)}$ 中对应的 (u,v)。

虽然最优 3-元循环码的构造在[11]-[23]中得到了充分研究，但关于 p-元循环码的工作较少。Xu 等[24]利用 $\mathbb{F}_{p^m}$ 上的 PN 函数和逆函数，构造了参数为 $\left[p^m-1,p^m-2m-2,4\right]$ 的最优 $p(p\ge5)$ 元循环码 $\mathcal{C}_{(0,1,e)}$，利用 APN 函数和其它单项式构造了一些参数为 $\left[5^m-1,5^m-2m-2,4\right]$ 的最优 5-元循环码。Zhou 等

[25]确定了参数为$\left[\frac{5^m-1}{2},\frac{5^m-1}{2}-2m,4\right]$的最优 5-元负循环码$\mathcal{C}_{(1,e)}$。文献[26]总结了现有最优 3-元循环码，并在其表 1、2 和 3 中给出了参数为$\left[5^m-1,5^m-2m-2,4\right]$的最优 5-元循环码$\mathcal{C}_{(0,1,e)}$和$\mathcal{C}_{(1,k,e)}\left(k=\frac{5^m-1}{2}\right)$。Liao 等[27]给出了参数为$\left[\frac{2\left(p^m-1\right)}{(p-1)},\frac{2\left(p^m-1\right)}{(p-1)}-2m,4\right]$的 p-元循环码。在文献[28]中，Liu 等首先提出了 5-元循环码$\mathcal{C}_{(1,k,e)}$最优性的充要条件，后续又确定了参数为$\left[\frac{2\left(p^m-1\right)}{(p-1)},\frac{2\left(p^m-1\right)}{(p-1)}-2m,4\right]$的 p-元循环码[17]，并由此给出了三种显式构造。文献[29]中 Liu 和 Cao 等通过讨论$\mathbb{F}_{5^m}$上某些方程的解，给出了八类新的最优 5-元循环码，其形式为$\mathcal{C}_{(1,e,s)}$。Liu 和 Huang 等[30]通过分析方程在$\mathbb{F}_{5^m}$上的解，并利用多元方法，提出了八类与已知循环码不等价的最优 5-元循环码$\mathcal{C}_{\left(1,e,\frac{5^m-1}{2}\right)}$，并证明了 5-元循环码$\mathcal{C}_{\left(\frac{5^m+1}{2},\frac{5^m+1}{2}+e,5^m-1\right)}$与$\mathcal{C}_{\left(1,e,\frac{5^m-1}{2}\right)}$具有相同的最优性。在 2025 年，Liu 和 Cao 等[31]又通过考虑有限域上某些方程的解，给出了三类新的参数为$\left[5^m-1,5^m-2m-2,4\right]$的最优 5-元循环码的无限族$\mathcal{C}_{(1,e,s)}$。通过分析有限域上某些多项式的解，Wu 等[32]构造了两类最优 p-元循环码$\mathcal{C}_{(0,1,e)}$和$\mathcal{C}_{(1,k,e)}\left(k=\frac{5^m-1}{2}\right)$，参数为$\left[p^m-1,p^m-\frac{3m}{2}-2,4\right]$，其中 m 为偶数，且$e=1+p^{\frac{m}{2}}$或$e=\frac{p^m-1}{2}+1+p^{\frac{m}{2}}$，又提出了三类新的最优 7-元循环码$\mathcal{C}_{(0,1,e)}$，其参数为$\left[7^m-1,7^m-2m-2,4\right]$。

本文在此基础上，通过引入新的参数选取条件，并利用一种确定其最优性的有效方法，构造了一类结构相似但参数集不相交的 7-元循环码$\mathcal{C}_{(0,1,e)}$。具体而言，当 m 为奇数且满足 $m\mid k$ 时，本文构造的码字与[32]中的码字具有不同的生成元幂等元形式，从而填补了该参数区域内非二元最优码构造的空白。此外，我们证明了所构造码的最小距离达到$d_{\min}=4$，验证了其最优性。

本文组织如下：第 2 章给出后续证明过程所需的基本知识；在第 3 章构造一类具有三个零点的最优 7-元循环码；最后一章对全文内容进行总结。

2. 预备知识

定义 1 $\mathbb{F}_{p^m}$上的二次特征 χ 定义为

$$\chi(x)=\begin{cases}0, & x=0,\\ 1, & x\text{是非零平方元},\\ -1, & x\text{是非零非平方元}.\end{cases}$$

换言之，对于$x\in\mathbb{F}_{p^m}^*$，若存在 $y\in\mathbb{F}_{p^m}^*$ 使得 $x=y^2$，则称 x 为非零平方元；否则，称 x 为非零非平方元。

定义 2 (Frobenius 自同态) 设 $\mathbb{F}$ 是特征为素数 p 的域。定义该域上的 Frobenius 自同态 ϕ 为映射：

$$\phi:\mathbb{F}\to\mathbb{F},\phi(x)=x^p$$

对所有 $x\in\mathbb{F}$ 成立。

迭代：ϕ 的 n 次迭代$(n\geq 1)$也是一个自同态，定义为：

$$\phi^n:\mathbb{F}\to\mathbb{F},\quad \phi^n(x)=x^{p^n}$$

有限域$\mathbb{F}_{p^k}$上：ϕ^k是恒等映射，即对所有$x\in\mathbb{F}_{p^k}$有$x^{p^k}=x$。

引理 1 ([24]，引理 1) 设p为素数，$n=p^m-1$。对于$1\le e\le n-1$且$\gcd(e,n)=d$，若$1\le d\le p-1$，则$l_e=m$。

引理 2 ([32]，引理 10) 设C_e是模7^m-1的包含e的 7-分圆陪集。若e为偶数或$e\equiv 3(\mathrm{mod}6)$或$e\equiv 5(\mathrm{mod}6)$，则$e\notin C_1$。

引理 3 ([24]，引理 5) 设$p\ge 5$为素数，$m>1$。对于任意$e\notin C_1$且$|C_e|=m$，循环码$\mathcal{C}_{(0,1,e)}$的最小距离d满足$d\le 4$。

引理 4 ([18]，引理 2.2) (球填充界)一个p元$[n,k,d]$线性码满足

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

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

引理 7 ([32]，引理 7) 设$f(x)=ax^2+bx+c(a\ne 0)$是F_{p^m}上的多项式。定义$\Delta=b^2-4ac(\Delta\ne 0)$。那么，若$\chi(\Delta)=1$，则$f(x)$在$F_{p^m}$上有解；若$\chi(\Delta)=-1$，则$f(x)$在$F_{p^m}$上无解，其中$\chi$是$F_{p^m}$上的二次特征。

引理 8 ([32]，定理 5) 设$e\notin C_1$且$|C_e|=m$。那么，7-元循环码$\mathcal{C}_{(0,1,e)}$是最优的且具有参数$[7^m-1,7^m-2m-2,4]$，如果满足以下条件之一：

(1) $e\equiv 2(\mathrm{mod}6)$，方程$(x+5)^e+x^e=-5$和$(x+4)^e+2x^e=-1$在$\mathbb{F}_{7^m}^*\setminus\{1\}$中无根；或

(2) $e\equiv 5(\mathrm{mod}6)$，方程$(x+5)^e-x^e=5$和$(x+4)^e-2x^e=1$在$\mathbb{F}_{7^m}^*\setminus\{1\}$中无根。

3. 参数为$[7^m-1,7^m-2m-2,4]$的最优 7-元循环码$\mathcal{C}_{(0,1,e)}$

本节构造一类参数为$[7^m-1,7^m-2m-2,4]$的 7-元循环码。参数e的选取是构造的核心：我们期望C_e的维数恰好为m且最小距离尽可能大。为此，令$n=\frac{7^m-1}{2}$并选取n满足$\gcd(e,7^m-1)=\frac{7^m-1}{n}$，从而保证生成多项式以$\alpha^e$为根，且维数$m$等于 7 模$n$的乘法阶。条件$m|k$旨在利用子域性质，可将高次方程简化为二次方程，进而精确刻画最小距离。此外，限制m $(m>1)$为奇数可避免某些特殊情形的出现，确保分圆陪集不发生合并，从而与文献[32]的构造形成区分。

在下面的定理中，我们将给出当$e=\frac{7^m-1}{2}+r$，其中$r=\frac{7^k+3}{2}$时，七元循环码$\mathcal{C}_{(0,1,e)}$的最优性。

定理 1 设m,k为奇数，$m>1$且$m|k$。那么，当$e=\frac{7^m-1}{2}+\frac{7^k+3}{2}$时，七元循环码$\mathcal{C}_{(0,1,e)}$是最优的，且有参数$[7^m-1,7^m-2m-2,4]$。

证明：首先，当m为奇数时，$e\equiv 2(\mathrm{mod}6)$。那么，由引理 2 可得$e\notin C_1$。其次，因为$gcd(2e,7^m-1)=\gcd(7^m-1+7^k+3,7^m-1)=\gcd(4,7^m-1)=2$，所以$\gcd(e,7^m-1)\le 2$。设$n=\frac{7^m-1}{2}$，且$e$满足$\gcd(e,7^m-1)=\frac{7^m-1}{n}$。通过分析 7 模$n$的乘法阶，并结合$e$的选取条件，可得$\mathrm{ord}_n(7)=m$。由循环码的维数公式$\dim(C_e)=\mathrm{ord}_n(7)$，可严格推导出$|C_e|=m$。因此，码$\mathcal{C}_{(0,1,e)}$的维数为$7^m-2m-2$。最后，由引理 3，我们可知$d\le 4$ (具体证明见文献[24]定理 3.1)，即证明当$d=4$时$\mathcal{C}_{(0,1,e)}$是最优的。换句话说，此

处只需证明对于奇数 m，方程 $(x+5)^e+x^e=-5$ 和 $(x+4)^e+2x^e=-1$ 在 $\mathbb{F}_{7^m}^*\setminus\{1\}$ 中无根。

当 m 为奇数时，有 $e=\frac{7^m-1}{2}+\frac{7^k+3}{2}\equiv 2(\mathrm{mod}6)$。那么，$(x+5)^e+x^e=-5,$

即

$$(x+5)^{\frac{7^m-1}{2}+\frac{7^k+3}{2}}+x^{\frac{7^m-1}{2}+\frac{7^k+3}{2}}=-5,$$

进一步化简得

$$\chi(x+5)(x+5)^{\frac{7^k+3}{2}}+\chi(x)x^{\frac{7^k+3}{2}}=-5, \tag{1}$$

其中 χ 是 F_{7^m} 上的二次特征。

根据 χ 的取值分以下四种情况讨论。

情形 A： $(\chi(x+5),\chi(x))=(1,1)$

此时方程(1)变为

$$(x+5)^{\frac{7^k+3}{2}}+x^{\frac{7^k+3}{2}}=-5, \tag{2}$$

因 $-5\equiv 2(\mathrm{mod}7)$，所以(2)等价于 $(x+5)^{\frac{7^k+3}{2}}+x^{\frac{7^k+3}{2}}=2$。

由引理 6 中 Frobenius 自同态可知，有限域上对所有 $x\in F_{p^k}$ 有 $x^{p^k}=x$。因此可得 $(x+5)^{7^k}=x+5$。类似地 $x^{7^k}=x$，那么，

$$(x+5)^{7^k+3}=(x+5)^{7^k}(x+5)^3=(x+5)^4.$$

类似地，

$$x^{7^k+3}=x^{7^k}\cdot x^3=x^4.$$

因此，

$$(x+5)^{\frac{7^k+3}{2}}=\left((x+5)^{7^k+3}\right)^{\frac{1}{2}}=\left((x+5)^4\right)^{\frac{1}{2}}=(x+5)^2,$$

$$x^{\frac{7^k+3}{2}}=\left(x^{7^k+3}\right)^{\frac{1}{2}}=\left(x^4\right)^{\frac{1}{2}}=x^2.$$

方程(2)变为 $(x+5)^2+x^2=2$，即

$$2x^2+3x+2=0. \tag{3}$$

显然 $x=1$ 是(3)的一个解。由于 $x\in\mathbb{F}_{7^m}^*\setminus\{1\}$，故(2)无根。

情形 B： $(\chi(x+5),\chi(x))=(1,-1)$

方程(1)变为

$$(x+5)^{\frac{7^k+3}{2}}-x^{\frac{7^k+3}{2}}=-5. \tag{4}$$

类似地，(4)等价于 $(x+5)^{\frac{7^k+3}{2}}-x^{\frac{7^k+3}{2}}=2$。我们有

$$(x+5)^{7^k+3}=(x+5)^4,\quad x^{7^k+3}=x^4.$$

$$(x+5)^{\frac{7k+3}{2}}=(x+5)^2,\quad x^{\frac{7k+3}{2}}=x^2.$$

则方程(4)变为$(x+5)^2-x^2=2$，即$3x+2=0$。因此，$x=4$是(4)的一个解。根据假设，我们有$\chi(4)=-1$。但这与$\chi(4)=1$矛盾。

情形 C：$(\chi(x+5),\chi(x))=(-1,1)$

方程(1)变为

$$-(x+5)^{\frac{7k+3}{2}}+x^{\frac{7k+3}{2}}=-5. \tag{5}$$

与情形 B 相同，(5)可简化为

$$-(x+5)^2+x^2=2,$$

即

$$3x+6=0.$$

所以$x=5$是(5)的一个解。由二次特征，$\chi(5)=-1$，这与假设矛盾。

情形 D：$(\chi(x+5),\chi(x))=(-1,-1)$

方程(1)变为

$$-(x+5)^{\frac{7k+3}{2}}-x^{\frac{7k+3}{2}}=-5. \tag{6}$$

类似地，方程(6)可简化为

$$-(x+5)^2-x^2=2,$$

即

$$x^2+5x+3=0.$$

于是判别式

$$\Delta=b^2-4ac=5^2-4\cdot1\cdot3=25-12=13\equiv6(\mathrm{mod}7).$$

那么，$\chi(\Delta)=\chi(6)=-1$。因此，由引理 7，方程(6)在$\mathbb{F}_{7^m}^*\setminus\{1\}$中无根。

因此，我们知道$(x+5)^e+x^e=-5$在$\mathbb{F}_{7^m}^*\setminus\{1\}$中无根。

ii) 考虑第二个方程

代入e的值到$(x+4)^e+2x^e=-1$, 有

$$(x+4)^{\frac{7^m-1}{2}+\frac{7^k+3}{2}}+2x^{\frac{7^m-1}{2}+\frac{7^k+3}{2}}=-1,$$

即

$$(x+4)^{\frac{7^m-1}{2}+\frac{7^k+3}{2}}+2x^{\frac{7^m-1}{2}+\frac{7^k+3}{2}}=-1,$$

进一步化简得

$$\chi(x+4)(x+4)^{\frac{7^k+3}{2}}+2\chi(x)x^{\frac{7^k+3}{2}}=-1, \tag{7}$$

其中χ是F_{7^m}上的二次特征。

类似地，我们讨论以下情形。

情形 A： $\left(\chi\left(x+4\right),\chi\left(x\right)\right)=\left(1,1\right)$

(7)变为

$$\left(x+4\right)^{\frac{7^k+3}{2}}+2x^{\frac{7^k+3}{2}}=-1. \tag{8}$$

因为 $-1\equiv 6\left(\mathrm{mod}7\right)$，所以(8)等价于 $\left(x+4\right)^{\frac{7^k+3}{2}}+2x^{\frac{7^k+3}{2}}=6$。类似地，由 Frobenius 自同态，我们有 $\left(x+4\right)^{\frac{7^k+3}{2}}=\left(x+4\right)^2$ 和 $2x^{\frac{7^k+3}{2}}=2x^2$。即

$$\left(x+4\right)^{\frac{7^k+3}{2}}=\left(x+4\right)^2,\quad 2x^{\frac{7^k+3}{2}}=2x^2.$$

则方程(8)变为 $\left(x+4\right)^2+2x^2=6$，即 $\left(x-1\right)^2=0$。因此，$x=1$ 是(8)的一个解。故在 $\mathbb{F}_{7^m}^*\setminus\left\{1\right\}$\中无根。

情形 B： $\left(\chi\left(x+4\right),\chi\left(x\right)\right)=\left(1,-1\right)$

(7)变为

$$\left(x+4\right)^{\frac{7^k+3}{2}}-2x^{\frac{7^k+3}{2}}=-1. \tag{9}$$

同上，通过模运算我们得出结论，(9)等价于 $\left(x+4\right)^{\frac{7^k+3}{2}}-2x^{\frac{7^k+3}{2}}=6$。

类似地，有 $\left(x+4\right)^{\frac{7^k+3}{2}}=\left(x+4\right)^2$ 和 $2x^{\frac{7^k+3}{2}}=2x^2$。因此，(9)可简化为

$$\left(x+4\right)^2-2x^2=6,$$

即

$$x^2+6x+4=0.$$

于是

$$\Delta=b^2-4ac=6^2-4\cdot 1\cdot 4=36-16=20\equiv 6\left(\mathrm{mod}7\right).$$

那么，$\chi\left(\Delta\right)=\chi\left(6\right)=-1$。因此，方程(9)在 $\mathbb{F}_{7^m}^*\setminus\left\{1\right\}$ 中无解。

情形 C： $\left(\chi\left(x+4\right),\chi\left(x\right)\right)=\left(-1,1\right)$

(7)变为

$$-\left(x+4\right)^{\frac{7^k+3}{2}}+2x^{\frac{7^k+3}{2}}=-1. \tag{10}$$

与情形 B 相同，上述方程可简化为

$$-\left(x+4\right)^2+2x^2=-1,$$

即

$$x^2+6x+6=0.$$

那么，

$$\Delta=b^2-4ac=6^2-4\cdot 1\cdot 6=36-24=12\equiv 5\left(\mathrm{mod}7\right).$$

因此，$\chi\left(\Delta\right)=\chi\left(5\right)=-1$。由引理 7，(10)在 $\mathbb{F}_{7^m}^*\setminus\left\{1\right\}$ 中无解。

情形 D： $\left(\chi\left(x+4\right),\chi\left(x\right)\right)=\left(-1,-1\right)$

(7)变为

$$-(x+4)^{\frac{7^k+3}{2}}-2x^{\frac{7^k+3}{2}}=6. \tag{11}$$

类似地，(11)可简化为

$$-(x+4)^2-2x^2=6,$$

即

$$x^2+5x+5=0.$$

那么，

$$\Delta=b^2-4ac=5^2-4\cdot1\cdot5=25-20=5\equiv5(\mathrm{mod}7).$$

因此，$\chi(\Delta)=\chi(5)=-1$。(11)在$\mathbb{F}_{7^m}^*\setminus\{1\}$中无解。我们知道$(x+4)^e+2x^e=-1$在$\mathbb{F}_{7^m}^*\setminus\{1\}$中无根。

综上所述，对于奇数m,k，$m>1$且$m|k$，方程$(x+5)^e+x^e=-5$和$(x+4)^e+2x^e=-1$在$\mathbb{F}_{7^m}^*\setminus\{1\}$中无根。

通过以上证明，我们得到当$e=\frac{7^m-1}{2}+\frac{7^k+3}{2}$时，7-元循环码$\mathcal{C}_{(0,1,e)}$是最优的，且具有参数$\left[7^m-1,7^m-2m-2,4\right]$。

例：根据设定的m,k（$m|k$），我们可取$m=3$，$k=9$，那么$n=7^m-1=7^3-1=343-1=342$，$e=\frac{7^m-1}{2}+\frac{7^k+3}{2}=\frac{342}{2}+\frac{7^9+3}{2}\equiv173(\mathrm{mod}342)$，参数为$[342,335,4]$的7-元循环码$\mathcal{C}_{(0,1,173)}$是最优的，且生成多项式为$g(x)=x^7+6x^6+3x^5+2x^4+4x^3+5x^2+3x+1$。

4. 结论

循环码作为一类重要的线性分组码，因其高效的编译码算法及优异的纠错能力，在通信系统、数据存储和网络安全等领域展现出了重要的应用价值。随着5G通信、量子计算等新兴技术产业的发展，对该领域的研究不仅有助于完善编码理论框架，也为下一代通信技术提供了关键的理论基础。通过验证已有的条件，本文构造了一类参数为$\left[7^m-1,7^m-2m-2,4\right]$的最优7-元循环码$\mathcal{C}_{(0,1,e)}$，并证明了该码字在给定维数下达到最优。与文献[32]相比，本文的参数选取条件(m,k为奇数且$m|k$)给出了一个不相交的码字集合，丰富了对非二元循环码最优构造的认识。该码字具有清晰的代数结构，其生成多项式由特定分圆陪集确定，为进一步研究其自同构群、对偶码的重量分布及在CSS量子码构造中的潜在应用提供了理论基础。后续工作可考虑将该构造方法推广到其它非素数基的有限域，并探索其与量子纠错码的联系。

参考文献

[1] Charpin, P., Tietäväinen, A. and Zinoviev, V. (1999) On the Minimum Distances of Non-Binary Cyclic Codes. *Designs, Codes and Cryptography*, **17**, 81-85. https://doi.org/10.1023/a:1008354504832

[2] Charpin, P., Tietvinen, A. and Zinoviev, V. (1997) On Binary Cyclic Codes with Minimum Distance *d*=3. *Problems Inf. Transmiss*, **33**, 3-14.

[3] Lidl, R. and Niederreiter, H. (1977) Finite Fields. Cambridge University Press.

[4] Macwilliams, F. and Sloane, N. (1977) The Theory of Error-Correcting Codes. Elsevier.

[5] Ireland, K. and Rosen, M. (1990) A Classical Introduction to Modern Number Theory. Springer-Verlag.

[6] El Rouayheb, S.Y., Georghiades, C.N., Soljanin, E. and Sprintson, A. (2007) Bounds on Codes Based on Graph Theory.

2007 *IEEE International Symposium on Information Theory*, Nice, 24-29 June 2007, 1876-1879. https://doi.org/10.1109/isit.2007.4557151

[7] Carlet, C., Ding, C.S. and Yuan, J. (2005) Linear Codes from Highly Nonlinear Functions and Their Secret Sharing Schemes. *IEEE Transactions on Information Theory*, **51**, 2089-2102.

[8] Ding, C.S. 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

[9] Liu, Q., Dong, X.B. and Lian, Z.Z. (2025) Several Classes of Optimal Ternary Cyclic Codes with Two Zeros. *Cryptography and Communications*, **18**, 251-278. https://doi.org/10.1007/s12095-025-00843-1

[10] Wu, G.F., You, Z.H., Zha, Z.B. and Zhang, Y.Q. (2024) Several New Classes of Optimal Ternary Cyclic Codes with Two or Three Zeros. *Designs, Codes and Cryptography*, **93**, 769-786. https://doi.org/10.1007/s10623-024-01541-4

[11] Han, D.C. and Yan, H.D. (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

[12] Li, L.Q., Zhu, S.X. and Liu, L. (2019) Three Classes of Optimal Ternary Cyclic Codes and the Weight Distributions of Their Duals. *Chinese Journal of Electronics*, **28**, 674-681. https://doi.org/10.1049/cje.2019.04.001

[13] Li, N., Li, C.L., Helleseth, T., Ding, C.S. and Tang X.H. (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

[14] Li, N., Zhou, Z.C. and Helleseth, T. (2015) On a Conjecture about a Class of Optimal Ternary Cyclic Codes. 2015 7*th 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

[15] Liu, Q. and Liu, X.M. (2022) On Some Conjectures about Optimal Ternary Cyclic Codes. *Applicable Algebra in Engineering, Communication and Computing*, **33**, 419-436. https://doi.org/10.1007/s00200-020-00458-4

[16] Liu, Y., Cao, X.W. and Lu, W. (2020) On Some Conjectures about Optimal Ternary Cyclic Codes. *Designs, Codes and Cryptography*, **88**, 297-309. https://doi.org/10.1007/s10623-019-00679-w

[17] Liu, Y. and Cao, X.W. (2023) Optimal P-Ary Cyclic Codes with Two Zeros. *Applicable Algebra in Engineering, Communication and Computing*, **34**, 129-138. https://doi.org/10.1007/s00200-021-00489-5

[18] Wang, D.D. and Cao, X.W. (2022) A Family of Optimal Ternary Cyclic Codes with Minimum Distance Five and Their Duals. *Cryptography and Communications*, **14**, 1-13. https://doi.org/10.1007/s12095-021-00493-z

[19] Wang, L.S. and Wu, G.F. (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

[20] Yan, H.D., Zhou, Z.C. and Du, X.N. (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

[21] Zha, Z.B. 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

[22] Zha, Z.B., Hu, L., Liu, Y. and Cao, X.W. (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

[23] Zhao, H., Luo, R. and Sun, T.J. (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

[24] Xu, G.K., Cao, X.W. and Xu, S.D. (2016) Optimal P-Ary Cyclic Codes with Minimum Distance Four from Monomials. *Cryptography and Communications*, **8**, 541-554. https://doi.org/10.1007/s12095-015-0159-0

[25] Zhou, Y.J., Kai, X.S., Zhu, S.X. and Li, J. (2019) On the Minimum Distance of Negacyclic Codes with Two Zeros. *Finite Fields and Their Applications*, **55**, 134-150. https://doi.org/10.1016/j.ffa.2018.09.006

[26] Wu, T.T., Zhu, S.X, Liu, L. and Li, L.Q. (2024) Optimal Quinary Cyclic Codes with Three Zeros. *Cryptography and Communications*, **16**, 801-823. https://doi.org/10.1007/s12095-024-00703-4

[27] Liao, D.C., Kai, X.S., Zhu, S.X. and Li, P. (2019) A Class of Optimal Cyclic Codes with Two Zeros. *IEEE Communications Letters*, **23**, 1293-1296. https://doi.org/10.1109/lcomm.2019.2921330

[28] Liu, Y. and Cao, X.W. (2020) Four Classes of Optimal Quinary Cyclic Codes. *IEEE Communications Letters*, **24**, 1387-1390. https://doi.org/10.1109/lcomm.2020.2983373

[29] Liu, Y., Cao, X.W. and Zha, Z.B. (2023) More Classes of Optimal Quinary Cyclic Codes of Form $\mathcal{C}_{(1,e,s)}$. *Applicable Algebra in Engineering, Communication and Computing*, **36**, 327-339. https://doi.org/10.1007/s00200-023-00604-8

[30] Liu, Q., Huang, J.H., Zheng, D.B., Jiang, R and Zhang L.P. (2025) Several Classes of Optimal Quinary Cyclic Codes with Minimum Distance Four. *Cryptography and Communications*, **17**, 1521-1542. https://doi.org/10.1007/s12095-025-00814-6

[31] Liu, Y. and Cao, X.W. (2025) Three New Classes of Optimal Quinary Cyclic Codes with Minimum Distance Four. *Applicable Algebra in Engineering*, *Communication and Computing*, **36**, 493-501. https://doi.org/10.1007/s00200-023-00621-7

[32] Wu, T.T., Liu, L. and Li, L.Q. (2025) Several Classes of Optimal Cyclic Codes with Three Zeros. *Applicable Algebra in Engineering*, *Communication and Computing*, **36**, 743-767. https://doi.org/10.1007/s00200-023-00636-0