几类最优重根循环码的构造

黄素娟[1,2],孙中华[1,2],朱士信[1,2]
(1. 合肥工业大学数学学院,安徽合肥 230601;2. 智能互联系统安徽省实验室,安徽合肥 230009)

摘 要: 本文分析了重根循环码的纠错能力. 利用循环码的代数结构,构造了几类最优的循环码. 构造了一类距离最优的二元重根循环码,并由此派生出一类距离和维数都是最优的二元重根循环码;构造了一类距离和维数都是最优的非二元重根循环码;构造了两类距离最优的非二元循环码.

关键词: 重根循环码; 最优码; Hamming距离
中图分类号: TN911. 22 **文献标识码:** A **文章编号:** 0372-2112(2022)01-0142-07
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20200739

On the Construction of Several Classes of Optimal Repeated-Root Cyclic Codes

HUANG Su-juan[1,2], SUN Zhong-hua[1,2], ZHU Shi-xin[1,2]
(1. *School of Mathematics*, *Hefei University of Technology*, *Hefei*, *Anhui* 230601, *China*;
2. *Intelligent Interconnected Systems Laboratory of Anhui Province* (*Hefei University of Technology*), *Hefei*, *Anhui* 230009, *China*)

Abstract: This paper analyzes the error-correction ability of repeated-root cyclic codes. By using the algebraic structure of cyclic codes, several classes of optimal cyclic codes are constructed. A class of binary repeated-root cyclic codes with optimal distances is constructed, and then a class of binary repeated-root cyclic codes with optimal distances and dimensions is derived; A class of non-binary repeated-root cyclic codes with optimal distances and dimensions is constructed; Two classes of non-binary cyclic codes with optimal distances are constructed.

Key words: repeated-root cyclic codes; optimal codes; Hamming distances

1 引言

循环码是一类重要的线性码,许多高效的纠错码都是循环码,如Golay码和RS码等. 重根循环码作为一类特殊的循环码受到广泛关注. Chen[1]在其博士论文中研究了码长为$2n$(n是奇数)的二元重根循环码的最小距离(相关结论亦可查阅文献[2]). Gastagnoli等人[3]证明了重根循环码的最小距离可以用一组单根循环码的最小距离来表示,并证明了重根循环码是渐进坏的. 基于这一理论,编码学者们确定了几类重根循环码的最小距离(参阅文献[4~6]和它们的引用). van Lint[7]通过$(u|u+v)$构造证明了码长为$2n$(n是奇数)的二元重根循环码可以通过两个码长为n的二元循环码来构造,并构造了参数为$[2^m-2, 2^m-m-3, 4]$的最优二元循环码. 然而,由于重根循环码是渐进坏的,此后关于重根循环码最优性的讨论相对较少.

最新的研究结果表明,重根循环码在量子纠错码和符号对码的构造中有重要作用. 以重根循环码为载体,文献[8~11]构造了几类参数优的量子重根循环码,文献[12]构造了几类参数好的非二元量子同步码. 文献[13]和文献[14],利用重根循环码的代数结构,确定了几类重根循环码的最小对距离,由此构造了几类有最大符号对距离的符号对码,从而说明重根循环码在符号对读信道上有较好的纠错能力. 重根循环码的纠错能力是这两类应用中的一个关键点,因此,分析重根循环码的纠错能力并探讨它的最优性,是一个有趣的问题.

一个p元$[n,k,d]$线性码C称为距离最优的是指不存在参数为$[n,k,\geqslant d+1]$的p元线性码. 码C称为维

收稿日期:2020-07-16;修回日期:2021-01-05;责任编辑:王天慧
基金项目:国家自然科学基金(No.62002093,No.61772168,No.61802102);中央高校基本科研业务费专项资金资助(No.JZ2020HGQA0154,No.JZ2020HGTA0079,No.PA2019GDZC0097)

数最优的是指不存在参数为$[n, \geqslant k+1, d]$的p元线性码. 本文基于循环码的代数的结构,首先,构造了几类最小距离是4的距离最优二元重根循环码,特别地,其中一类距离最优码也是维数最优的线性码;其次,构造了一类最小距离是3的距离和维数都是最优的非二元重根循环码;最后,构造了两类最小距离是4的距离最优非二元循环码. 本文的研究结果表明,重根循环码可以产生小距离的最优线性码.

2 预备知识

设p是一个素数,$\mathbb{F}_p$是p阶有限域. 设n是一个正整数,$\mathbb{F}_p^n$是$\mathbb{F}_p$上n维行向量空间. $\mathbb{F}_p^n$的每个k维子空间称为一个码长为n且维数为k的p元线性码,记作$[n,k]$. 设$\boldsymbol{x}\in\mathbb{F}_p^n$,向量$\boldsymbol{x}$的Hamming重量定义为$\boldsymbol{x}$非零分量的个数,记作$\mathrm{wt}(\boldsymbol{x})$. 设$\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_p^n$,向量$\boldsymbol{x}$和$\boldsymbol{y}$的Hamming距离定义为$\boldsymbol{x}-\boldsymbol{y}$的Hamming重量,记作$\mathrm{dist}(\boldsymbol{x},\boldsymbol{y})$,即$\mathrm{dist}(\boldsymbol{x},\boldsymbol{y})=\mathrm{wt}(\boldsymbol{x}-\boldsymbol{y})$. 一个$p$元$[n,k]$线性码$C$的最小距离定义为

$$\begin{aligned}&\min\{\mathrm{dist}(\boldsymbol{x},\boldsymbol{y})|\boldsymbol{x},\boldsymbol{y}\in C,\boldsymbol{x}\neq\boldsymbol{y}\}\\&=\min\{\mathrm{wt}(\boldsymbol{x})|\boldsymbol{x}\in C,\boldsymbol{x}\neq\boldsymbol{0}\}\end{aligned}$$

码长为n、维数为k和最小距离为d的p元线性码,记作$[n,k,d]$. 一个p元$[n,k,d]$线性码的三个参数满足球包界[15]:

$$\sum_{i=0}^{\lfloor(d-1)/2\rfloor}\binom{n}{i}(p-1)^i\leqslant p^{n-k}\tag{1}$$

其中$\lfloor x\rfloor$表示不超过x的最大整数. 对于最小距离是偶数的二元$[n,k,d]$线性码,文献[16]给出了一个改进的界:

$$\sum_{i=0}^{(d-2)/2}\binom{n-1}{i}\leqslant 2^{n-k-1}\tag{2}$$

对于$p>3$元$[n,k,d]$线性码,文献[16]证明

$$\sum_{i=0}^{r}\binom{n-d+1+2r}{i}(p-1)^i\leqslant p^{n-d+1+2r-k}\tag{3}$$

其中$r=\left\lfloor\min\left\{\dfrac{d-1}{2},\dfrac{n-d}{p-2}\right\}\right\rfloor$.

一个码长n的p元线性码C称为循环码是指对任意的$(c_0,c_1,\cdots,c_{n-1})\in C$,有$(c_{n-1},c_0,\cdots,c_{n-2})\in C$. 定义映射

$$\sigma:\mathbb{F}_p^n\to R=\mathbb{F}_p[x]/(x^n-1),$$
$$(c_0,c_1,\cdots,c_{n-1})\mapsto c_0+c_1x+\cdots+c_{n-1}x^{n-1},$$

则码长为n的p元线性码C是循环码当且仅当$\sigma(C)=\{\sigma(\mathbf{c})|\mathbf{c}\in C\}$是商环$R$的理想. 众所周知,商环$R$是主理想环,因此,对于每个码长为$n$的$p$元循环码$C$,存在唯一的多项式$g(x)\in\mathbb{F}_p[x]$使得$g(x)|(x^n-1)$且$C=g(x)R=(g(x))$,$g(x)$称为码$C$的生成多项式,并且码$C$的维数$\dim(C)=n-\deg(g(x))$. 设$n=p^e\ell$,其中$e$和$\ell$是非负整数且$\gcd(\ell,p)=1$. 记$\mathrm{ord}_\ell(p)$为$p$模$\ell$的阶,即使得$p^l\equiv 1(\mathrm{mod}\,\ell)$的最小正整数. 设$\mathrm{ord}_\ell(p)=m$,则在$\mathbb{F}_{p^m}$上存在一个$\ell$次本原单位根$\alpha$. 设$\mathbb{Z}_\ell=\mathbb{Z}/\ell\mathbb{Z}$是整数模$\ell$的剩余类环. 定义$\mathbb{Z}_\ell$上等价关系$\sim$:$i\sim j\Leftrightarrow\exists s\in\mathbb{Z}, ip^s\equiv j(\mathrm{mod}\,n)$. 用$\Lambda$表示等价类构成的集合,则

$$x^\ell-1=\prod_{i\in\Lambda}\prod_{j\in\mathrm{cl}(i)}(x-\alpha^j)\tag{4}$$

其中$\mathrm{cl}(i)$表示i所在的等价类. 对于$0\leqslant i\leqslant n-1$,$\mathbb{F}_p[x]$上以$\alpha^i$为根的次数最低首一多项式称作$\alpha^i$在$\mathbb{F}_p$上的极小多项式. 容易验证,$\alpha^i$在$\mathbb{F}_p$上的极小多项式为$m_i(x)=\prod_{j\in\mathrm{cl}(i)}(x-\alpha^j)\in\mathbb{F}_p[x]$. 进一步可证,式(4)为$x^\ell-1$在$\mathbb{F}_p[x]$上的不可约分解且$x^n-1=(x^\ell-1)^{p^e}=\prod_{i\in\Lambda}m_i(x)^{p^e}$. 当$e=0$时,码长为$n$的$p$元循环码称为单根循环码;当$e\geqslant 1$时,码长为$n$的$p$元循环码称为重根循环码. 对于单根循环码的最小距离有如下著名的界[15].

引理 1 设p是一个素数,n是一个正整数且$\gcd(n,p)=1$. 设α是一个n次本原单位根. 设C是一个码长为n且生成多项式为$g(x)$的p元循环码. 如果存在整数b,c_1,c_2且$\gcd(c_1,n)=\gcd(c_2,n)=1$使得

$$\alpha^{b+i_1c_1+i_2c_2},\ (i_1=0,1,\cdots,\delta-2,i_2=0,1,\cdots,s)$$

是$g(x)$的根,则码C的最小距离$d(C)\geqslant\delta+s$.

当$s=0$时,引理1称为BCH界. 对于重根循环码的最小距离,Gastagnoli等人[3]提出了如下理论.

设$x^\ell-1$在$\mathbb{F}_p[x]$上的不可约分解为$x^\ell-1=m_1(x)m_2(x)\cdots m_r(x)$,则码长为$n$的$p$元循环码$C$的生成多项式可唯一表示为$g(x)=m_1(x)^{s_1}m_2(x)^{s_2}\cdots m_r(x)^{s_r}$,其中$0\leqslant s_i\leqslant p^e$,$i=1,2,\cdots,r$. 对于$0\leqslant t\leqslant p^e-1$,定义

$$\bar{g}_t(x)=\prod_{i=1,s_i>t}^{r}m_i(x).$$

如果$\{i|s_i>t\}=\varnothing$,规定$\bar{g}_t(x)=1$. 设$\bar{C}_t$是码长为ℓ生成多项式为$\bar{g}_t(x)$的p元循环码,记$\bar{C}_t$的最小距离为$d(\bar{C}_t)$. 特别地,当$\bar{g}_t=x^\ell-1$时,规定$d(\bar{C}_t)=\infty$. 进一步,定义t的p-进制展开为$t=t_0+t_1p+\cdots+t_{e-1}p^{e-1}$,其中$0\leqslant t_i\leqslant p-1$,$i=0,1,\cdots,e-1$,并定义$t$的$p$重量为$P_t=(t_0+1)(t_1+1)\cdots(t_{e-1}+1)$. 文献[3]中引理1和定理1证明如下结论成立.

引理 2 码长为n且生成多项式为$g(x)=m_1(x)^{s_1}m_2(x)^{s_2}\cdots m_r(x)^{s_r}$的$p$元重根循环码的最小距离$d(C)=\min\{P_t\cdot d(\bar{C}_t)|0\leqslant t\leqslant p^e-1\}$.

3 主要结果

基于重根循环码的代数结构,本节构造了几类最优码.

3.1 二元最优重根循环码

下面构造最优二元重根循环码. 对任意的正整数 ℓ,记 $v_2(\ell)$ 表示 ℓ 的2-进制展开中非零项的最高次幂,即如果 $v_2(\ell)=i$,则 ℓ 的2-进制展开为 $\ell_0+\ell_1 2+\cdots+\ell_{i-1}2^{i-1}+2^i$.

定理1 设 ℓ 是奇数且 $\ell\geqslant 3$,e 是正整数,则存在参数为 $[2^e\ell, 2^e\ell-2^{e-1}-\mathrm{ord}_\ell(2)-1, 4]$ 的二元重根循环码 $C(e,\ell)$. 当 $v_2(\ell^2)-\mathrm{ord}_\ell(2)\geqslant 2^{e-1}-2e+2$ 时,$C(e,\ell)$ 是距离最优的二元线性码.

证明 设 α 是 $\mathbb{F}_2$ 扩域上的 ℓ 次本原单位根,$m(x)$ 是 α 在 $\mathbb{F}_2$ 上的极小多项式. 设 $C(e,\ell)$ 是码长为 $n=2^e\ell$ 且生成多项式为 $(x+1)^{2^{e-1}+1}m(x)$ 的二元重根循环码,则

$$\dim(C(e,\ell))=n-2^{e-1}-\mathrm{ord}_\ell(2)-1.$$

首先,证明 $d(C(e,\ell))=4$. 设 $\bar{C}_0$ 是码长为 ℓ 且生成多项式为 $(x+1)m(x)$ 的二元循环码. 因为 $\alpha^0,\alpha^1,\alpha^2$ 是 $(x+1)m(x)$ 的零点,由BCH界,$d(\bar{C}_0)\geqslant 4$. 设 $\bar{C}_1$ 是码长为 ℓ 且生成多项式为 $x+1$ 的二元循环码,则 $d(\bar{C}_1)=2$. 容易验证 $P:=\min\{P_t: 2^{e-1}+1\leqslant t\leqslant 2^e-1\}=4$. 由引理2,$d(C(e,\ell))=\min\{d(\bar{C}_0), 2d(\bar{C}_1), P\}=4$.

最后,证明 $C(e,\ell)$ 的最优性. 假设存在参数为 $[2^e\ell, 2^e\ell-2^{e-1}-\mathrm{ord}_\ell(2)-1, \geqslant 5]$ 的二元码,由球包界(1),

$$1+n+\frac{n(n-1)}{2}\leqslant 2^{n-\dim(C)}=2^{\mathrm{ord}_\ell(2)+2^{e-1}+1},$$

而不等式左端

$$1+n+\frac{n(n-1)}{2}=2^{2e-1}\ell^2+2^{e-1}\ell+1>2^{v_2(\ell^2)+2e-1}\geqslant 2^{\mathrm{ord}_\ell(2)+2^{e-1}+1},$$

矛盾. 因此,$C(e,\ell)$ 是距离最优的二元线性码.

注1 定理1的距离最优约束条件是充分的. 通过计算机搜索,定理1可以产生39个码长不超过256的距离最优二元重根循环码,其中36个码长满足定理1中的约束条件,与码表[17]比较,36个距离最优二元码中有11个码是维数最优的. 详见表1. 其中带#的码表示不满足约束条件的最优码,带*的码表示维数最优码. 由此可以看出,尽管重根循环码是渐近坏的,但仍存在小距离的最优重根循环码.

表1 最小距离是4的最优二元重根循环码

生成多项式	参 数	生成多项式	参 数
x^4+x^3+x+1	[6, 2]*	x^6+x^5+x+1	[10, 4]#
$x^5+x^3+x^2+1$	[12, 7]*	x^5+x^2+x+1	[14, 9]*
$x^8+x^6+x^5+x^3+x^2+1$	[18, 10]#	$x^7+x^5+x^2+1$	[20, 13]
$x^7+x^4+x^3+1$	[24, 17]	$x^6+x^5+x^3+1$	[28, 22]*
$x^6+x^4+x^3+x^2+x+1$	[30, 24]*	$x^{10}+x^9+x^7+x^3+x+1$	[34, 24]#
$x^9+x^8+x^7+x^5+x^4+x^2+x+1$	[36, 27]	$x^9+x^5+x^4+1$	[40, 31]
$x^8+x^7+x^5+1$	[42, 34]	$x^8+x^7+x^6+x^3+x^2+1$	[56, 48]
$x^7+x^6+x^5+1$	[60, 53]*	$x^7+x^5+x^4+1$	[62, 55]*
$x^{11}+x^9+x^8+x^7+x^4+x^3+x^2+1$	[68, 57]	$x^{11}+x^{10}+x^8+x^6+x^5+x^3+x+1$	[72, 61]
$x^9+x^7+x^6+x^5+x+1$	[84, 75]	$x^{10}+x^9+x^5+x^4+x^3+x^2+x+1$	[102, 92]
$x^{12}+x^{11}+x^{10}+x^8+x^4+x^3+x^2+1$	[112, 100]	$x^9+x^8+x^6+x^5+x^2+1$	[120, 111]
$x^8+x^7+x^6+x^4+x+1$	[124, 116]*	$x^8+x^5+x^4+x^2+x+1$	[126, 118]*
$x^{13}+x^{12}+x^{11}+x^9+x^4+x^2+x+1$	[132, 119]	$x^{13}+x^{10}+x^8+x^7+x^6+x^5+x^3+1$	[136, 123]
$x^{11}+x^7+x^6+x^5+x^4+x^3+x^2+1$	[146, 135]	$x^{11}+x^8+x^6+x^5+x^3+x^2+x+1$	[168, 157]
$x^{10}+x^7+x^5+x^3+x+1$	[170, 160]	$x^{13}+x^{11}+x^{10}+x^9+x^6+x^4+x+1$	[178, 165]
$x^{14}+x^{11}+x^{10}+x^9+x^3+x^2+x+1$	[182, 168]	$x^{12}+x^{11}+x^{10}+x^5+x^4+x^3+x+1$	[186, 174]
$x^{11}+x^9+x^6+1$	[204, 193	$x^{14}+x^{11}+x^{10}+x^8+x^7+x^4+x^2+1$	[210, 196]
$x^{14}+x^{11}+x^9+x^8+x^5+x^2+x+1$	[234, 220]	$x^{13}+x^{12}+x^{10}+x^8+x^5+x^4+x^2+1$	[240, 193]
$x^{10}+x^9+x^7+x^4+x^3+x^2+x+1$	[248, 238]	$x^9+x^8+x^6+x^4+x^3+1$	[252, 243]*
$x^9+x^7+x^3+x^2+x+1$	[254, 245]*		

由定理1,可以得到一系列最小距离是4的最优二元线性码. 下面给出几类具体的最优二元重根循环码.

推论1 设 m,e 是正整数且 $m\geqslant\max\{2^{e-1}-2e+3, 2\}$,则存在参数为 $[2^{m+e}-2^e, 2^{m+e}-3\cdot 2^{e-1}-m-1, 4]$ 的距离最优二元重根循环码. 特别地,当 $e\in\{1,2\}$ 时,参数为 $[2^{m+e}-2^e, 2^{m+e}-3\cdot 2^{e-1}-m-1, 4]$ 的二元重根循环码也是维数最优码.

证明 设 $\ell=2^m-1$,则 $v_2(\ell^2)=2m-1$ 且 $\mathrm{ord}_\ell(2)=m$. 由定理1,存在参数为 $[2^{m+e}-2^e, 2^{m+e}-3\cdot 2^{e-1}-m-1, 4]$ 的距离最优二元重根循环码.

假设存在参数为 $[2^{m+e}-2^e, k\geqslant 2^{m+e}-3\cdot 2^{e-1}-m, 4]$ 的二元线性码. 由界(2),$1+n-1\leqslant 2^{n-k-1}$,即

$2^m-1\leqslant 2^{n-1-e-k}\leqslant 2^{m+2^{e-1}-e-1}$. 当 $e\in\{1,2\}$ 时，$m+2^{e-1}-e-1=m-1$,所以 $2^m-1\leqslant 2^{m-1}$,矛盾. 故参数为 $[2^{m+e}-2^e, 2^{m+e}-3\cdot 2^{e-1}-m-1, 4]$ 的距离最优码也是维数最优码.

推论 2　设 e 是正整数,m 是偶数且 $m\geqslant 2^{e-1}-2e+6$,则存在参数为

$$\left[\frac{2^{m+e}-2^e}{3}, \frac{2^{m+e}-5\cdot 2^{e-1}-3}{3}-m, 4\right]$$

的距离最优二元重根循环码.

证明　设 $\ell=\dfrac{2^m-1}{3}$,则 $\mathrm{ord}_\ell(2)=m$. 因为

$$2^{2m-4}<\ell^2=\frac{2^{2m}-2^{m+1}+1}{9}<2^{2m-3}$$

所以 $v_2(\ell^2)=2m-4$. 由定理 1,结论成立.

推论 3　设 m 是正偶数且 $e\in\{1,2,3,4\}$,则存在参数为 $\left[3(2^{m+e}+2^e), 3\cdot 2^{m+e}+5\cdot 2^{e-1}-2m-1, 4\right]$ 的距离最优二元重根循环码.

证明　设 $\ell=3(2^m+1)$,则 $\mathrm{ord}_\ell(2)=2m$ 且 $v_2(\ell^2)=2m+3$. 当 $e\in\{1,2,3,4\}$ 时,

$$v_2(\ell^2)-\mathrm{ord}_\ell(2)\geqslant 2^{e-1}-2e+2$$

由定理 1,结论成立.

推论 4　设 $m\geqslant 3$ 是正奇数且 $e\in\{1,2,3,4\}$,则存在参数为 $\left[3(2^{m+e}-2^e), 3\cdot 2^{m+e}-7\cdot 2^{e-1}-2m-1, 4\right]$ 的距离最优二元重根循环码.

证明　设 $\ell=3(2^m-1)$,则 $\mathrm{ord}_\ell(2)=2m$. 当 $m=3$ 时,$v_2(\ell^2)=8$;当 $m\geqslant 5$ 时,$v_2(\ell^2)=2m+3$. 容易验证,当 $e\in\{1,2,3,4\}$ 时，$v_2(\ell^2)-\mathrm{ord}_\ell(2)\geqslant 2^{e-1}-2e+2$. 由定理 1,结论成立.

推论 5　设 m 是正整数且 $e\in\{2,3\}$,则存在参数为 $\left[2^{m+e}+2^e, 2^{m+e}+2^{e-1}-2m-1, 4\right]$ 的距离最优二元重根循环码.

证明　设 $\ell=2^m+1$，则 $\mathrm{ord}_\ell(2)=2m$ 且 $v_2(\ell^2)=2m$. 当 $e\in\{2,3\}$ 时，$v_2(\ell^2)-\mathrm{ord}_\ell(2)\geqslant 2^{e-1}-2e+2$.由定理 1,结论成立.

3.2　非二元最优循环码

本小节将构造几类非二元最优码.

定理 2　设 p 是一个奇素数,m 是一个正整数,$\lambda\geqslant 2$ 且 $\lambda\mid(p-1)$,则存在参数为

$$\left[\frac{(p^{m+1}-p)\lambda}{p-1}, \frac{(p^{m+1}-p)\lambda}{p-1}-2-m, 3\right]$$

的距离和维数都是最优的 p 元重根循环码.

证明　设 $\ell=\dfrac{(p^m-1)\lambda}{p-1}$,$\alpha$ 是 $\mathbb{F}_p$ 扩域上的 ℓ 次本原单位根,$m(x)$ 是 α 在 $\mathbb{F}_p$ 上的极小多项式. 设 C 是码长为 $n=p\ell$ 且生成多项式为 $(x-1)^2m(x)$ 的 p 元重根循环码,则 $\dim(C)=n-2-m$.

设 $\bar{C}_0$ 是码长为 ℓ 且生成多项式为 $(x-1)m(x)$ 的 p 元循环码. 因为 α^0 和 α^1 是 $(x-1)m(x)$ 的零点,由 BCH 界,$d(\bar{C}_0)\geqslant 3$. 设 $\bar{C}_1$ 是码长为 ℓ 且生成多项式为 $x-1$ 的 p 元循环码,则 $d(\bar{C}_1)=2$. 容易验证,

$$P:=\min\{P_t: 2\leqslant t\leqslant p-1\}=3.$$

由引理 2,$d(C)=\min\{d(\bar{C}_0), 2d(\bar{C}_1), P\}=3$.

下面讨论码 C 的最优性. 由球包界(1)推出,不存在参数为 $[p\ell, p\ell-2-m, \geqslant 5]$ 的 p 元线性码. 假设存在参数为 $[p\ell, p\ell-2-m, 4]$ 的 p 元线性码,由界(3),$1+(n-1)(p-1)\leqslant p^{n-1-\dim(C)}=p^{m+1}$,矛盾. 因此,$C$ 是距离最优的 p 元循环码. 同理,假设存在参数为 $[p\ell, k\geqslant p\ell-1-m, 3]$ 的 p 元线性码,由球包界(1),$1+n(p-1)\leqslant p^{n-k}\leqslant p^{m+1}$,矛盾. 因此,码 C 是维数最优的 p 元循环码.

由定理 2 推出,存在如下最优的 p 元重根循环码.

推论 6　设 p 是一个奇素数且 m 是正整数,则

(i) 存在参数为 $[p^{m+1}-p, p^{m+1}-p-2-m, 3]$ 的距离和维数都是最优的 p 元重根循环码;

(ii) 存在参数为

$$\left[\frac{2(p^{m+1}-p)}{p-1}, \frac{2(p^{m+1}-p)}{p-1}-2-m, 3\right]$$

的距离和维数都是最优的 p 元重根循环码;

(iii) 如果 $p\geqslant 5$,存在参数为

$$\left[\frac{p^{m+1}-p}{2}, \frac{p^{m+1}-p}{2}-2-m, 3\right]$$

的距离和维数都是最优的 p 元重根循环码.

例 1　当 $p=3$ 时,定理 2 构造了一类参数为 $[3^{m+1}-3, 3^{m+1}-5-m, 3]$ 的最优三元循环码. 对于短码长,表 2 给出了它们的生成多项式,与码表[17]比较,定理 2 证明存在最优重根循环码.

例 2　当 $p=5$ 时,定理 2 构造了两类最优五元循环码,它们的参数分别为 $[5^{m+1}-5, 5^{m+1}-7-m, 3]$ 和 $\left[\dfrac{5^{m+1}-5}{2}, \dfrac{5^{m+1}-9}{2}-m, 3\right]$. 对于短码长,表 3 给出了它们的生成多项式,与码表[17]比较,定理 2 证明存在最优重根循环码.

下面构造最小距离是 4 的最优 p 元循环码.

定理 3　设 p 是一个奇素数,m 和 n 是正整数,$n\mid(p^{2m}-1)$ 且 $n>p^m+1$. 设 $\gcd(p^m+1, n)=\tau$,$\lambda=n/\tau$ 且 $\mathrm{ord}_\lambda(p)=s$,当

$$n>\frac{(p-3)+\sqrt{(p-3)^2+8(p^{2m+s+1}-1)}}{2(p-1)}$$

时,存在参数为 $[n, n-1-2m-s, 4]$ 的距离最优 p 元循环码.

证明　因为 $n\mid(p^{2m}-1)$ 且 $n>p^m+1$,则 $\mathrm{ord}_n(p)=$

表2 最小距离是3的最优三元重根循环码

生成多项式	参 数	生成多项式	参 数
x^3+2x^2+2x+1	[6, 3]	x^4+2x^2+x+2	[24, 20]
x^5+x^4+1	[78, 73]	$x^6+2x^3+2x^2+2x+2$	[240, 234]
$x^7+x^6+x^5+2x^3+1$	[726, 719]	$x^8+x^7+2x^5+2x^2+x+2$	[2184, 13]
$x^9+x^8+x^7+2x^4+2x^3+x+1$	[6558, 6549]	$x^{10}+x^9+x^8+2x^7+x^3+x+2$	[19680, 19670]

表3 最小距离是3的最优五元重根循环码

生成多项式	参 数	生成多项式	参 数
x^3+4x^2+4x+1	[10, 7]	x^3+x^2+3	[20, 17]
$x^4+x^3+4x^2+4$	[60, 56]	x^4+2x^3+2	[120, 116]
$x^5+4x^4+3x^3+4x^2+2x+1$	[310, 305]	$x^5+3x^4+4x^3+2x^2+2x+3$	[620, 615]
$x^6+x^5+3x^3+4x^2+2x+4$	[1560, 1554]	$x^6+3x^5+x^3+3x^2+2$	[3120, 3114]

$2m$. 设$\alpha\in\mathbb{F}_{p^{2m}}$是一个$n$次本原单位根，$m(x)$是$\alpha$在$\mathbb{F}_p$上的极小多项式，则$\deg(m(x))=2m$. 设$m_{p^m+1}(x)$是$\alpha^{p^m+1}$在$\mathbb{F}_p$上的极小多项式，下证$\deg(m_{p^m+1}(x))=s$. 显然，$\deg(m_{p^m+1}(x))$是使$(p^m+1)(p^l-1)\equiv 0(\bmod n)$成立的最小正整数. 注意到

$$(p^m+1)(p^l-1)\equiv 0(\bmod n)\Leftrightarrow p^l\equiv 1(\bmod \lambda),$$

于是$\deg(m_{p^m+1}(x))=s$. 设C是码长为n且生成多项式为$g(x)=(x-1)m(x)m_{p^m+1}(x)$的$p$元循环码，则$\dim(C)=n-1-2m-s$.

一方面，因为$\alpha^0,\alpha^1,\alpha^{p^m},\alpha^{p^m+1}$是$g(x)$的零点，由引理1，$d(C)\geqslant 4$. 另一方面，假设存在参数为$[n,n-1-2m-s,\geqslant 5]$的$p$元线性码. 由球包界(1)，

$$1+n(p-1)+\frac{n(n-1)}{2}(p-1)^2\leqslant p^{2m+s+1}$$

由此推出

$$n\leqslant\frac{(p-3)+\sqrt{(p-3)^2+8(p^{2m+s+1}-1)}}{2(p-1)}$$

矛盾. 因此，C是最小距离为4的最优p元循环码.

由定理3推出，存在如下最优的p元循环码.

推论7 设p是一个奇素数且m是一个正整数，则

(i) 对任意的$n|(p^2-1)$且$n>p+1$，存在参数为$[n,n-4,4]$的距离最优p元循环码；

(ii) 如果$m\geqslant 2$，对任意的$e|(p-1)$，$s\geqslant 2$且$s|m$，存在参数为

$$\left[\frac{(p^m+1)(p^s-1)}{e},\frac{(p^m+1)(p^s-1)}{e}-1-2m-s,4\right]$$

的距离最优p元循环码；

(iii) 对任意的$\ell|(p^2-1)$且$\ell\geqslant p+1$，存在参数为$[(p^2+1)\ell,(p^2+1)\ell-7,4]$的距离最优$p$元循环码；

(iv) 对任意的$e|(p^2-1)$且$e<p^2-1$，存在参数为

$$\left[\frac{p^6-1}{e},\frac{p^6-1}{e}-10,4\right]$$

的距离最优p元循环码；

(v) 如果$p\geqslant 5$且$m\geqslant 4$，对任意的$e|(p^2-1)$，存在参数为$\left[\frac{p^{2m}-1}{e},\frac{p^{2m}-1}{e}-1-3m,4\right]$的距离最优$p$元循环码；

(vi) 如果$m\geqslant 3$，存在参数为

$$\left[\frac{3^{2m}-1}{4},\frac{3^{2m}-1}{4}-1-3m,4\right]$$

的距离最优三元循环码；

(vii) 如果$m\geqslant 5$，存在参数为

$$\left[\frac{3^{2m}-1}{8},\frac{3^{2m}-1}{8}-1-3m,4\right]$$

的距离最优三元循环码；

(viii) 如果$p\geqslant 5$，对任意的$\ell|(p-1)$且$\ell\geqslant 2$，存在参数为$[(p^m+1)\ell,(p^m+1)\ell-2-2m,4]$的距离最优$p$元循环码.

证明 (i)~(viii)的证明类似，下面仅给出(v)的证明，其余略去.

(v) 设$n=\frac{p^{2m}-1}{e}$，其中$m\geqslant 4$且$e|(p^2-1)$. 显然，$n>p^m+1$. 下证$s=\deg(m_{p^m+1}(x))=m$，即证m是使得$(p^m+1)(p^s-1)\equiv 0(\bmod n)$成立的最小正整数. 因为$s|m$且$n>(p^m+1)(p^{\frac{m}{2}}-1)$，所以$s=m$. 直接计算可得

$$[2(p-1)n-(p-3)]^2>\frac{(2p^{2m}-p^2)^2}{(p+1)^2}>(p-3)^2+8(p^{3m+1}-1),$$

即

$$n>\frac{(p-3)+\sqrt{(p-3)^2+8(p^{3m+1}-1)}}{2(p-1)}$$

由定理3，存在参数为$[n,n-1-3m,4]$的距离最优p元循环码.

下面构造最小距离是4的最优p元重根循环码.

定理4 设p是一个奇素数，m和ℓ是正整数，

$\ell | (p^{2m}-1)$ 且 $\ell > p^m+1$. 设 $\gcd(p^m+1,\ell)=\tau$, $\lambda=\ell/\tau$ 且 $\mathrm{ord}_\lambda(p)=s$, 当

$$\ell > \frac{(p-3)+\sqrt{(p-3)^2+8(p^{2m+s+3}-1)}}{2p(p-1)}$$

时, 存在参数为 $[p\ell, p\ell-2m-s-3, 4]$ 的距离最优 p 元重根循环码.

证明 与定理3类似, 可证 $\mathrm{ord}_\ell(p)=2m$. 设 $\alpha\in\mathbb{F}_{p^{2m}}$ 是一个 ℓ 次本原单位根, $m(x)$ 是 α 在 $\mathbb{F}_p$ 上的极小多项式, 且 $m_{p^m+1}(x)$ 是 α^{p^m+1} 在 $\mathbb{F}_p$ 上的极小多项式, 则 $\deg(m(x))=2m$ 且 $\deg(m_{p^m+1}(x))=s$. 设 C 是码长为 $p\ell$ 且生成多项式为 $(x-1)^3 m(x) m_{p^m+1}(x)$ 的 p 元循环码, 则 $\dim(C)=n-3-2m-s$. 与定理3类似可证, C 是参数为 $[p\ell, p\ell-2m-s-3, 4]$ 的距离最优 p 元线性码.

由定理4推出, 存在如下最优的 p 元重根循环码.

推论8 设 p 是一个奇素数且 m 是一个正整数, 则

(i) 对任意的 $\ell | (p^2-1)$ 且 $\ell \geqslant \frac{3}{2}(p+1)$, 存在参数为 $[p\ell, p\ell-6, 4]$ 的距离最优 p 元重根循环码;

(ii) 如果 $m\geqslant 2$, 对任意的 $e|(p-1)$, $s\geqslant 2$ 且 $s|m$, 存在参数为

$$\left[\frac{(p^{m+1}+p)(p^s-1)}{e}, \frac{(p^{m+1}+p)(p^s-1)}{e}-3-2m-s, 4\right]$$

的距离最优 p 元重根循环码;

(iii) 对任意的 $\ell | (p^2-1)$ 且 $\ell \geqslant p+1$, 存在参数为 $[(p^3+p)\ell, (p^3+p)\ell-9, 4]$ 的距离最优 p 元重根循环码;

(iv) 对任意的 $e|(p^2-1)$ 且 $e<p^2-1$, 存在参数为 $\left[\frac{p^7-p}{e}, \frac{p^7-p}{e}-12, 4\right]$ 的距离最优 p 元重根循环码;

(v) 如果 $p\geqslant 5$ 且 $m\geqslant 4$, 对任意的 $e|(p^2-1)$, 存在参数为 $\left[\frac{p^{2m+1}-p}{e}, \frac{p^{2m+1}-p}{e}-3-3m, 4\right]$ 的距离最优 p 元重根循环码;

(vi) 如果 $m\geqslant 3$, 存在参数为

$$\left[\frac{3^{2m+1}-3}{4}, \frac{3^{2m+1}-3}{4}-3-3m, 4\right]$$

的距离最优三元重根循环码;

(vii) 如果 $m\geqslant 5$, 存在参数为

$$\left[\frac{3^{2m+1}-3}{8}, \frac{3^{2m+1}-3}{8}-3-3m, 4\right]$$

的距离最优三元重根循环码;

(viii) 如果 $p\geqslant 5$, 对任意的 $\ell | (p-1)$ 且 $\ell\geqslant 2$, 存在参数为 $[(p^{m+1}+p)\ell, (p^{m+1}+p)\ell-4-2m, 4]$ 的距离最优 p 元重根循环码.

注2 定理3和定理4构造了两大类最小距离是4的最优 p 元循环码, 其中定理4构造了距离最优的重根循环码, 从而说明重根循环码可以产生小距离的最优码. 通过计算机搜索, 本文构造了9个码长不超243的距离最优三元码, 其中3个码是维数最优码, 详见表4, 其中带*的码表示维数最优码. 与码表[17]比较, 本文构造了最优循环码.

表4　最小距离是4的最优三元循环码

生成多项式	参　数	生成多项式	参　数
$x^4+2x^3+x^2+x+1$	[8, 4]*	$x^6+x^5+2x^4+x^3+x^2+x+2$	[20, 14]
$x^6+x^4+x^3+2x+1$	[24, 18]*	$x^7+x^6+x^2+x+2$	[40, 33]
$x^8+2x^7+x^6+x^5+x^4+x^2+2$	[60, 52]	$x^7+2x^5+x^4+x^3+2x^2+2$	[80, 73]*
$x^9+2x^8+2x^7+x^6+x^4+2x^3+x^2+2$	[120, 111]	$x^9+x^8+x^5+x^4+x^2+2x+2$	[240, 231]
$x^{10}+2x^9+x^8+x^7+2x^5+2x^4+x^3+2x^2+2x+1$	[182, 172]		

注3 当定理3和定理4的最优约束条件不满足时, 仍可以构造达到码表[17]的最优码, 下面举例说明.

例3 设 α 是 $\mathbb{F}_3$ 上不可约多项式 x^6+2x^5+2x+2 的根, 则 α 是一个56次本原单位根. 设 $\eta=\alpha^{28}$, 则 η 在 $\mathbb{F}_3$ 上的不可约多项式为 $x+1$. 设 C_1 是码长为56且生成多项式为 $(x-1)(x+1)(x^6+2x^5+2x+2)$ 的三元循环码, 由定理3的证明可得, C_1 是一个参数为 $[56, 48, \geqslant 4]$ 的三元循环码. 由 Magma 计算得, $d(C_1)=4$. 与码表[17]比较, C_1 是目前已知的最优三元线性码. 设 C_2 是码长为168且生成多项式为 $(x-1)^3(x+1)(x^6+2x^5+2x+2)$ 的三元重根循环码, 由定理4的证明可得, C_2 是一个参数为 $[168, 154, 4]$ 的三元重根循环码. 与码表[17]比较, C_2 是目前已知的最优三元线性码.

4　结论

本文主要研究了重根循环码的纠错性能, 并基于重根循环码构造了一系列最优的线性码. 主要结果如下: (1)构造了几类最小距离是4的最优二元重根循环码, 特别地, 构造了一类维数和距离都是最优的二元重根循环码, 这一结果可以视作文献[7]中例3的推广;

(2)构造了一类最小距离是3的距离和维数都是最优的非二元重根循环码;(3)构造了两大类最小距离是4的距离最优的非二元循环码. 这些研究结果表明:重根循环码中存在小距离的最优线性码. 自然地,是否存在最小距离大于4的最优重根循环码是一个值得进一步研究的问题. 文献[13]和文献[14]基于重根循环码的代数结构和最小Hamming距离,确定了几类循环码的对距离,构造了几类极大距离可分符号对码,从而说明重根循环码有较好的纠正错误的能力. 下一步将研究本文构造的最优码的对距离,从而构造参数优的符号对码.

参考文献

[1] CHEN C L. Some results on algebraically structured error-correcting codes[D]. USA Hawaii: University of Hawaii, 1969.

[2] MORELOS-ZARAGOZA R. A note on repeated-root cyclic codes[J]. IEEE Transactions on Information Theory, 2002, 37(6):1736-1737.

[3] CASTAGNOLI G, MASSEY J L, SCHOELLER P A, et al. On repeated-root cyclic codes[J]. IEEE Transactions on Information Theory, 1991, 37(2): 337-342.

[4] DINH H Q. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions[J]. Finite Fields and Their Applications, 2008, 14(1):22-40.

[5] ÖZADAM H, ÖZBUDAK F. The minimum Hamming distance of cyclic codes of length $2p^s$[C]//International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. Berlin, Heidelberg, GER: Springer, 2009: 92-100.

[6] LI X, YUE Q. The Hamming distance of repeated-root cyclic codes of length $5p^s$[J]. Discrete Applied Mathematics, 2020, 284: 29-41.

[7] VAN LINT J H. Repeated-root cyclic codes[J]. IEEE Transactions on Information Theory, 1991, 37(2): 343-345.

[8] LI R H, LI X L. Quantum codes constructed from binary cyclic codes[J]. International Journal of Quantum Information, 2004, 2(2):265-272.

[9] QIAN J F, ZHANG L. Nonbinary quantum codes derived from repeated-root cyclic codes[J]. Modern Physics Letters B, 2013, 27(8): 1350053.

[10] WANG L Q, ZHU S X. On non-binary quantum repeated-root cyclic codes[J]. International Journal of Quantum Information, 2014, 12(3):1450010.

[11] LI R H, SONG H, MA Y N, LV L D. Quantum codes constructed from repeated-root cyclic codes[J]. Journal of Physics: Conference Series, 2018, 1069(1): 012078.

[12] LUO L, MA Z. Non-binary quantum synchronizable codes from repeated-root cyclic codes[J]. IEEE Transactions on Information Theory, 2018, 64(3): 1461-1470.

[13] CHEN B C, LIN L R, LIU H W. Constacyclic symbol-pair codes: lower bounds and optimal constructions[J]. IEEE Transactions on Information Theory, 2017, 63(12): 7661-7666.

[14] KAI X S, ZHU S X, ZHAO Y S, et al. New MDS symbol-pair codes from repeated-root codes[J]. IEEE Communications Letters, 2018, 22(3): 462-465.

[15] MACWILLIAMS F J, SLOANE N J A. The Theory of Error-Correcting Codes[M]. Amsterdam, Netherlands: North-Holland Pub. CO., 1977.

[16] ROUAYHEB S Y E, GEORGHIADES C N, SOLJANIN E, et al. Bounds on codes based on graph theory[C]// 2007 IEEE International Symposium on Information Theory. Nice, France: IEEE, 2007: 1876-1879.

[17] GRASSL M. Code Tables: Bound on the parameters of various types of codes[J/OL]. [2020-01-12]. http://www.codetables.de.

作者简介

黄素娟 女,1989年生,安徽无为人. 合肥工业大学计算机与信息学院博士研究生. 研究方向为代数编码.

E-mail:huangsujuan1019@163.com

孙中华(通信作者) 男,1989年生,安徽肥西人. 合肥工业大学数学学院讲师,硕士生导师. 研究方向为代数编码.

E-mail:sunzhonghuas@163.com

朱士信 男,1962年生,安徽枞阳人. 合肥工业大学数学学院教授,博士生导师. 研究方向为代数编码、序列密码与信息安全研究.

E-mail:zhushixin@hfut.edu.cn