# $Z_4 \times (F_2 + uF_2)$ 上的一类循环码

高 健,吕京杰
(山东理工大学理学院,山东淄博 255000)

**摘 要:** 定义了 $Z_4 \times (F_2 + uF_2)$ 上的循环码,明确了一类循环码的生成元结构,给出了该类循环码的极小生成元集. 利用 Gray 映射,构造了一些二元非线性码.

**关键词:** 循环码; 生成元; 极小生成元集; 二元非线性码
**中图分类号:** TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2018)07-1768-06
**电子学报 URL:** http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.07.033

## A Class of Cyclic Codes over $Z_4 \times (F_2 + uF_2)$

GAO Jian, LÜ Jing-jie
(*School of Science, Shandong University of Technology, Zibo, Shandong* 255000, *China*)

**Abstract:** In this paper, we study some of the results on a class of cyclic codes over $Z_4 \times (F_2 + uF_2)$. We give the definition of this class of cyclic codes over $Z_4 \times (F_2 + uF_2)$ first. Then we determine the generators and the minimum generating sets of a type of cyclic codes. Finally, some binary nonlinear codes are constructed by this type of cyclic codes.

**Key words:** cyclic codes; generators; minimum generating sets; binary nonlinear codes

## 1 引言

有限交换环上的编码理论始于上个世纪六十年代. 1994 年 Hammons 等编码学者发现了一些性能良好的二元非线性码可以看作四元有限环 $Z_4$ 上某些循环码的二元象[1]. 这一结果解释了困扰编码学界几十年的问题. 这篇论文也获得了 1995 年 IEEE Transactions on Information Theory 的最佳论文奖. 从此,有限环上的编码理论成为了编码理论中的一个热点研究领域,涌现出了一些很好的理论成果[2~4].

近期,Borges 等编码学者研究了一类纠错码,即 $Z_2Z_4$ - 加性码[5]. 这类纠错码无论在理论上还是在实际应用中都有着重要意义. 随后,国内外的很多编码学者对这一类纠错码进行了更加深入的研究与推广[6,7]. $Z_2Z_4$ - 加性码的码字实际上由两部分组成,前半部分取自 $Z_2$,后半部分取自 $Z_4$. Abualrub 等首次对 $Z_2Z_4$ - 加性循环码做了系统的介绍与研究,并由此得到了一些性能良好的二元非线性码[8].

在本文中,我们研究 $Z_4 \times (F_2 + uF_2)$ 上的一类循环码. 首先,我们给出了 $Z_4 \times (F_2 + uF_2)$ 上循环码的定义. 其次,对于 $Z_4 \times (F_2 + uF_2)$ 上一类特殊的循环码,即 $\tau$ - 循环码,我们给出了这类循环码的生成元表达式以及极小生成元集. 最后,利用 $Z_4 \times (F_2 + uF_2)$ 到有限域 $F_2$ 上的 Gray 映射构造了 $F_2$ 上的二元非线性码.

## 2 $Z_4 \times (F_2 + uF_2)$ 上循环码的定义

设 $R_1 = Z_4, R_2 = F_2 + uF_2$,其中 $u^2 = 0$. 则 $R_1$ 和 $R_2$ 均是 4 元有限链环,它们的理想分别为 $<0> \subseteq <2> \subseteq R_1$ 和 $<0> \subseteq <u> \subseteq R_2$. 环 $R_1$ 和 $R_2$ 具有相似的代数结构,但是由于他们的特征分别是 4 和 2,因此它们具有不同的特点. 根据环 $R_1$ 以及环 $R_2$ 的理想不难看出,$<2>$ 和 $<u>$ 分别是 $R_1$ 和 $R_2$ 的极大理想. 因此,$R_1/<u_1> = R_2/<u_2> = F_2$. 定义映射

$$\phi: R_1 \to R_2$$

其中 $\phi(0) = 0, \phi(1) = 0, \phi(2) = 0$ 以及 $\phi(3) = 1$. 由于 $F_2$ 是 $R_2$ 的子环,则 $\phi$ 是一个同态映射. 对 $R_1$ 中的任意一个元素 $a$ 以及 $R_2$ 中的元素 $b$,定义 $a$ 与 $b$ 的乘法 "$*$" 如下:

$$a * b = \phi(a)b$$

容易验证,环 $R_2$ 在加法和乘法 $*$ 下构成一个 $R_1$ - 模. 我们将这个概念推广到向量空间 $R_1^r \times R_2^s$ 上,其中

$$R_1^r \times R_2^s = \{(e_0, e_1, \cdots, e_{r-1} \mid e_0', e_1', \cdots, e_{s-1}') \mid e_i \in R_1,$$

收稿日期:2017-01-06;修回日期:2017-02-24;任编辑:蓝红杰
基金项目:国家自然科学基金(No. 11626144, No. 11671235)

$e_j^{'}\in R_2, i=0,1,\cdots,r-1, j=0,1,\cdots,s-1\}$. 即,对任意的向量$\boldsymbol{c}=(c_0,c_1,\cdots,c_{r-1}\mid c_0^{'},c_1^{'},\cdots,c_{s-1}^{'})\in R_1^r\times R_2^s$以及$a\in R_1$,有

$$a*\boldsymbol{c}=(ac_0,ac_1,\cdots,ac_{r-1}\mid\phi(a)c_1^{'},\mid\phi(a)c_2^{'},\cdots,\phi(a)c_{s-1}^{'}).$$

因此,向量空间$R_1^r\times R_2^s$关于加法和乘法$*$构成了一个$R_1$-模.

**定义 1**　设向量集$\boldsymbol{C}$是$R_1^r\times R_2^s$的一个非空子集,如果$\boldsymbol{C}$关于乘法$*$构成一个$R_1^r\times R_2^s$的一个$R_1$-子模,则称$\boldsymbol{C}$是$R_1\times R_2$上码长为$r+s$的线性码.

在本文中,我们讨论的码都是线性码. 下面,我们给出$R_1\times R_2$上循环码的定义.

**定义 2**　设$\boldsymbol{C}$是$R_1^r\times R_2^s$上码长为$r+s$的线性码,即$\boldsymbol{C}$关于乘法$*$构成$R_1^r\times R_2^s$的一个$R_1$-子模. 若对于$\boldsymbol{C}$中的任意一个码字

$$(c_0,c_1,\cdots,c_{r-1}\mid c_0^{'},c_1^{'},\cdots,c_{s-1}^{'})$$

有

$$(c_{r-1},c_0,c_1,\cdots,c_{r-2}\mid c_{s-1}^{'},c_0^{'},c_1^{'},\cdots,c_{s-2}^{'})$$

仍是线性码$\boldsymbol{C}$中的码字,则称$\boldsymbol{C}$是$R_1+R_2$上码长为$r+s$的循环码.

值得注意的是,定义 2 中我们给出的$R_1\times R_2$上码长为$r+s$的循环码具有 2 个循环块,一个是$R_1$上码长为$r$的循环块,一个是$R_2$上码长为$s$的循环块,从而不同于传统意义上的循环码.

令$R_{r,s}=R_1[x]/<x^r-1>\times R_2[x]/<x^s-1>$. 设$a(x)=a_0+a_1x+\cdots+a_nx^n$是$R_1[x]$中的任意一个元素. 取$R_{r,s}$中的任意一个元素$c(x)=(c_r(x)\mid c_s(x))$,其中

$$c_r(x)=c_0+\cdots+c_{r-1}x^{r-1}\in R_1[x]/<x^r-1>,$$

$$c_s(x)=c_0+\cdots+c_{s-1}x^{s-1}\in R_2[x]/<x^s-1>,$$

定义

$$a(x)*c(x)=(a(x)c_r(x)\mid\phi(a(x))c_s(x)),$$

其中

$$\phi(a(x))=\phi(a_0)+\phi(a_1)x+\cdots+\phi(a_n)x^n.$$

显然,$R_{r,s}$构成一个$R_1[x]$-模. 定义

$$\varphi:R_1^r\times R_2^s\to R_{r,s}$$

$$\boldsymbol{c}=(c_0,c_1,\cdots,c_{r-1}\mid c_0^{'},c_1^{'},\cdots,c_{s-1}^{'})\mapsto c(x)=(c_r(x)\mid c_s(x))$$

其中

$$c_r(x)=c_0+c_1x+\cdots+c_{r-1}x^{r-1}\in R_r,$$

$$c_s(x)=c_0^{'}+c_1^{'}x+\cdots+c_{s-1}^{'}x^{s-1}\in R_s.$$

显然,$\varphi$是一个$R_1$-模同构. 另外,容易证明$\boldsymbol{C}$是$R_1\times R_2$上码长为$r+s$的循环码当且仅当$\phi(\boldsymbol{C})$是$R_{r,s}$的一个$R_1[x]$-子模. 在本文中若没有特殊说明,我们将$\boldsymbol{C}$和$\phi(\boldsymbol{C})$等同.

## 3　两个引理

设$\boldsymbol{C}$是环$R_1$上码长为$n$的线性码,即$\boldsymbol{C}$是$R_1^n$的一个$R_1$-子模. 线性码$\boldsymbol{C}$是循环码当且仅当对$\boldsymbol{C}$中的任意一个码字$(c_0,c_1,\cdots,c_{n-1})$有$(c_{n-1},c_0,\cdots,c_{n-2})$仍是$\boldsymbol{C}$中的一个码字.

设$R_n=R_1[x]/<x^n-1>$,则环$R_1$上的码长为$n$的循环码$\boldsymbol{C}$可以看作$R_n$的一个理想. 设$n$是一个奇数且在$R_1$上有

$$x^n-1=f(x)g(x)h(x),\text{则}$$

$$\begin{aligned}\boldsymbol{C}&=<f(x)h(x),2f(x)g(x)>\\&=<f(x)h(x)+2f(x)>\end{aligned}\tag{1}$$

其中$f(x),g(x),h(x)$是环$R_1$上的首一多项式且$f(x)h(x)+2f(x)$称为循环码的生成多项式[9].

由上述,我们知道环$R_1$上的循环码是$R_n$的理想,即$R_n$的一个$R_1[x]$-子模. 因此$\boldsymbol{C}$也可以看作$R_n$的一个$R_1$-子模. 通过式(1),我们能否给出$\boldsymbol{C}$作为$R_n$的$R_1$-子模的极小生成元集,即循环码$\boldsymbol{C}$作为$R_n$的$R_1$-子模的生成元? 事实上,一旦给出了极小生成元集我们就确定了$\boldsymbol{C}$的生成矩阵.

**引理 1**　设$\boldsymbol{C}$是环$R_1$上码长为$n$的循环码,且

$$\begin{aligned}\boldsymbol{C}&=<f(x)h(x),2f(x)g(x)>\\&=<f(x)h(x)+2f(x)>,\end{aligned}$$

其中$n$是一个奇数,并且在$R_1$上有

$$x^n-1=f(x)g(x)h(x),$$

$f(x),g(x),h(x)$是环$R_1$上的首一多项式. 定义

$$S_1=\{f(x)h(x),xf(x)h(x),\cdots,x^{\deg g(x)-1}f(x)h(x)\},$$

$$S_2=\{2f(x)g(x),2xf(x)g(x),\cdots,2x^{\deg h(x)-1}f(x)g(x)\}.$$

则$S_1\cup S_2$是循环码$\boldsymbol{C}$作为$R_n$的$R_1$-子模的极小生成元集.

**证明**　由于$\boldsymbol{C}=<f(x)h(x),2f(x)g(x)>$,

所以我们分为以下几种情况进行讨论:

(1)当$f(x)=1$,则$x^n-1=g(x)h(x)$且$\boldsymbol{C}=<h(x)>\oplus<2g(x)>$. 显然,$S_1\cup S_2$构成$\boldsymbol{C}$的极小生成元集.

(2) 当$f(x)\neq1$,则

(2-1-1) 当$h(x)=1$,则$x^n-1=f(x)g(x)$且$\boldsymbol{C}=<f(x)>$. 此时,$S_2=\varnothing$. 显然,$S_1\cup S_2$构成$\boldsymbol{C}$的极小生成元集.

(2-1-2) 当$h(x)\neq1$,则$x^n-1=f(x)g(x)h(x)$且$\boldsymbol{C}=<f(x)h(x)>\oplus<2f(x)g(x)>$. 显然,$S_1\cup S_2$构成$\boldsymbol{C}$的极小生成元集.

(2-2-1) 当$g(x)=1$,则$x^n-1=f(x)h(x)$且$\boldsymbol{C}=<2f(x)>$. 此时,$S_1=\varnothing$. 显然,$S_1\cup S_2$构成$\boldsymbol{C}$的极小生成元集.

(2-2-2) 当$g(x)\neq1$,则$x^n-1=f(x)g(x)h(x)$且

$\boldsymbol{C}=<f(x)h(x)>\oplus<2f(x)>$. 显然,$S_1\cup S_2$ 构成 $\boldsymbol{C}$ 的极小生成元集.

由于 $R_1$ 和 $R_2$ 上码长为奇数的循环码具有相同的代数结构[10],因此对于环 $R_2$ 上码长为奇数的循环码我们有类似于引理 1 的结果.

**引理 2** 令 $R_n'=R_2[x]/<x^n-1>$. 设 $\boldsymbol{C}$ 是环 $R_2$ 上码长为 $n$ 的循环码,且

$$\boldsymbol{C}=<\tilde{f}(x)\tilde{h}(x),u\tilde{f}(x)\tilde{g}(x)>=<\tilde{f}(x)\tilde{h}(x)+u\tilde{f}(x)>,$$

其中 $n$ 是一个奇数并且在 $R_2$ 上有 $x^n-1=\tilde{f}(x)\tilde{g}(x)\tilde{h}(x)$,$\tilde{f}(x),\tilde{g}(x),\tilde{h}(x)$ 是环 $R_2$ 上的首一多项式. 定义

$$S_1=\{\tilde{f}(x)\tilde{h}(x),x\tilde{f}(x)\tilde{h}(x),\cdots,x^{\deg\tilde{g}(x)-1}\tilde{f}(x)\tilde{h}(x)\},$$

$$S_2=\{u\tilde{f}(x)\tilde{g}(x),ux\tilde{f}(x)\tilde{g}(x),\cdots,ux^{\deg\tilde{h}(x)-1}\tilde{f}(x)\tilde{g}(x)\}.$$

则 $S_1\cup S_2$ 是循环码 $\boldsymbol{C}$ 作为 $R_n'$ 的 $R_2$ - 子模的极小生成元集.

## 4 $Z_4\times(F_2+uF_2)$ 上循环码的极小生成元集

设 $R_1[x]/<x^r-1>$ 和 $R_2[x]/<x^s-1>$ 是两个主理想环,其中 $r$ 和 $s$ 是两个奇数. 令 $\boldsymbol{C}$ 是 $R_1+R_2$ 上码长为 $r+s$ 的循环码,即 $R_{r,s}=R_1[x]/<x^r-1>\times R_2[x]/<x^s-1>$ 的 $R_1[x]$ - 子模. 定义映射

$$\tau:\boldsymbol{C}\to R_2[x]/<x^s-1>$$
$$(c_1(x)\,|\,c_2(x))\mapsto c_2(x).$$

显然,$\tau$ 是一个 $R_1[x]$ - 模同态. 由于 $\boldsymbol{C}$ 是 $R_{r,s}$ 的一个 $R_1[x]$ - 子模,所以对任意的 $a(x)\in R_1[x]$ 有

$a(x)*(c_1(x)\,|\,c_2(x))=(a(x)c_1(x)\,|\,\varphi(a(x)c_2(x)))\in\boldsymbol{C}$. 因为 $\varphi$ 是一个从 $R_1$ 到 $R_2$ 环同态映射且 $\varphi(R_1)=F_2$ 是 $R_2$ 的一个子环,所以

$\varphi(R_1[x])=F_2[x]$ 是 $R_2[x]$ 的一个子环. 因此,$\tau(\boldsymbol{C})$ 是商环 $R_2[x]/<x^s-1>$ 的一个 $F_2[x]$ - 子模. 故,$\tau(\boldsymbol{C})$ 是 $R_2[x]/<x^s-1>$ 的理想当且仅当 $\tau(\boldsymbol{C})=<u\tilde{f}(x)>$,其中 $\tilde{f}(x)$ 是多项式 $x^s-1$ 的首一因式. 此时,我们称 $\boldsymbol{C}$ 为 $R_1\times R_2$ 上的 $\tau$ - 循环码. 在本部分,我们首先给出 $R_1\times R_2$ 上 $\tau$ - 循环码的生成元的表达式.

**定理 1** 设 $\boldsymbol{C}$ 是 $R_1\times R_2$ 上码长为 $r+s$ 的 $\tau$ - 循环码,则

$$\boldsymbol{C}=<(f(x)h(x)+2f(x)\,|\,0),(l(x)\,|\,u\tilde{f}(x))>$$

其中,$f(x)$、$g(x)$、$h(x)$ 是环 $R_1$ 上的首一多项式且满足 $f(x)g(x)h(x)=x^r-1$;$\tilde{f}(x)$ 是环 $R_2$ 上 $x^s-1$ 的首一因式;$l(x)\in R_1[x]/<x^r-1>$.

**证明** 因为 $\boldsymbol{C}$ 是 $\tau$ - 循环码,所以 $\tau(\boldsymbol{C})=<u\tilde{f}(x)>$,其中 $\tilde{f}(x)$ 是 $x^s-1$ 的首一因式. 另外,

$$\mathrm{Ker}(\tau)=\{(c_1(x)\,|\,0)\in\boldsymbol{C}\,|\,c_1(x)\in R_1[x]/<x^r-1>\}.$$

定义集合

$$D=\{c_1(x)\in R_1[x]/<x^r-1>\,|\,(c_1(x)\,|\,0)\in\mathrm{Ker}(\tau)\}.$$

显然,$D$ 是商环 $R_1[x]/<x^r-1>$ 的理想. 因此,在 $R_1[x]$ 中存在首一多项式 $f(x)$、$g(x)$、$h(x)$ 使得 $x^r-1=f(x)g(x)h(x)$ 且 $D=<f(x)h(x)+2f(x)>$. 因此,对任意的 $(c_1(x)\,|\,0)\in\mathrm{Ker}(\tau)$,我们有 $c_1(x)\in D$. 故,在 $R_1[x]$ 中存在多项式 $m(x)$ 使得 $c_1(x)=m(x)(f(x)h(x)+2f(x))$. 所以,

$$(c_1(x)\,|\,0)=m(x)*(f(x)h(x)+2f(x)\,|\,0).$$

即,$\mathrm{Ker}(\tau)$ 是由 $(f(x)h(x)+2f(x)\,|\,0)$ 生成的 $R_1[x]$ - 子模. 因此,由模同态基本定理,我们有

$$\boldsymbol{C}/\mathrm{Ker}(\tau)\cong\tau(\boldsymbol{C})=<u\tilde{f}(x)>.$$

设 $(l(x)\,|\,u\tilde{f}(x))\in\boldsymbol{C}$,其中 $\tau((l(x)\,|\,u\tilde{f}(x)))=u\tilde{f}(x)$ 且 $l(x)\in R_1[x]/<x^r-1>$. 则作为 $R_{r,s}$ 的 $R_1[x]$ - 子模的循环码可以由 $(f(x)h(x)+2f(x)\,|\,0)$ 和 $(l(x)\,|\,u\tilde{f}(x))$ 生成.

**引理 3** 设 $\boldsymbol{C}=<(f(x)h(x)+2f(x)\,|\,0),(l(x)\,|\,u\tilde{f}(x))>$ 是 $R_1\times R_2$ 上码长为 $r+s$ 的 $\tau$ - 循环码,如果 $f(x)h(x)+2f(x)$ 或 $2f(x)-f(x)h(x)$ 是 $R_1$ 上的首一多项式,则

$$\deg(l(x))<\deg(f(x)h(x)+2f(x)).$$

**证明** 设 $\boldsymbol{C}=<(f(x)h(x)+2f(x)\,|\,0),(l(x)\,|\,u\tilde{f}(x))>$. 若 $\deg(l(x))\geqslant\deg(f(x)h(x)+2f(x))$. 令 $i=\deg(l(x))-\deg(f(x)h(x)+2f(x))$. 考虑

$$\boldsymbol{C}'=<(f(x)h(x)+2f(x)\,|\,0),l(x)-ax^i(f(x)h(x)+2f(x))\,|\,u\tilde{f}(x)>$$

其中 $a$ 是 $l(x)$ 的首项系数. 显然,$\boldsymbol{C}\subseteq\boldsymbol{C}'$. 另外,

$$(l(x)\,|\,u\tilde{f}(x))=(l(x)-ax^i(f(x)h(x)+2f(x))\,|\,u\tilde{f}(x))+ax^i*(f(x)h(x)+2f(x)\,|\,0).$$

所以 $(l(x)\,|\,u\tilde{f}(x))\in\boldsymbol{C}'$. 故,$\boldsymbol{C}=\boldsymbol{C}'$.

**引理 4** 设 $\boldsymbol{C}=<(f(x)h(x)+2f(x)\,|\,0),(l(x)\,|\,u\tilde{f}(x))>$ 是 $R_1\times R_2$ 上码长为 $r+s$ 的 $\tau$ - 循环码,则

$$(f(x)h(x)+2f(x))\,\Big|\,\frac{x^s-1}{\tilde{f}(x)}l(x).$$

**证明** 由于 $F_2$ 是环 $R_2$ 的子环,因此 $x^s-1$ 在 $R_2$ 上的分解可以看作在 $F_2$ 上分解. 所以,$\phi(\frac{x^s-1}{\tilde{f}(x)})=\frac{x^s-1}{\tilde{f}(x)}$. 因为

$$\frac{x^s-1}{\tilde{f}(x)}*(l(x)\,|\,u\tilde{f}(x))=(\frac{x^s-1}{\tilde{f}(x)}l(x)\,|\,0),$$

所以 $\tau(\frac{x^s-1}{\tilde{f}(x)}*(l(x)\,|\,u\tilde{f}(x)))=0$. 因此,$(\frac{x^s-1}{\tilde{f}(x)}l(x)\,|\,0)\in\mathrm{Ker}(\tau)\subseteq\boldsymbol{C}$. 故,

$$(f(x)h(x)+2f(x))\left|\frac{x^s-1}{\tilde{f}(x)}l(x).\right.$$

根据引理4,如果$\tau$-循环码$\boldsymbol{C}$只有$(l(x)\mid u\tilde{f}(x))$一个生成元生成,则

$$(x^r-1)\left|\frac{x^s-1}{\tilde{f}(x)}l(x).\right.$$

因此,由定理1、引理3、引理4,我们可以将$\tau$-循环码进行如下分类.

**推论1**　设$\boldsymbol{C}$是$R_1\times R_2$上码长为$r+s$的$\tau$-循环码,则$\boldsymbol{C}$可进行如下分类:

(i)$\boldsymbol{C}=<f(x)h(x)+2f(x)\mid 0>$,其中$f(x)$、$g(x)$、$h(x)$是$R_1$上的首一多项式且$f(x)g(x)h(x)=x^r-1$.

(ii)$\boldsymbol{C}=<(l(x)\mid u\tilde{f}(x))>$,其中$\tilde{f}(x)$是$x^s-1$的首一因式,且$(x^r-1)\left|\frac{x^s-1}{\tilde{f}(x)}l(x).\right.$

(iii)$\boldsymbol{C}=<(f(x)h(x)+2f(x)\mid 0),(l(x)\mid u\tilde{f}(x))>$,其中$f(x)h(x)+2f(x)$的首项系数为1或3;$f(x)$、$g(x)$、$h(x)$是$R_1$上的首一多项式且$f(x)g(x)h(x)=x^r-1$;

$\deg(l(x))<\deg(f(x)h(x)+2f(x))$;$(f(x)h(x)+2f(x))\left|\frac{x^s-1}{\tilde{f}(x)}l(x)\right.$;$\tilde{f}(x)$是$x^s-1$的首一因式.

(iv)$\boldsymbol{C}=<2f(x)\mid 0),(l(x)\mid u\tilde{f}(x))>$,

其中$f(x)$是$x^r-1$的首一因式;

$2f(x)\left|\frac{x^s-1}{\tilde{f}(x)}l(x)\right.$;$\tilde{f}(x)$是$x^s-1$的首一因式.

$R_1\times R_2$上码长为$r+s$的$\tau$-循环码$\boldsymbol{C}$是$R_{r,s}$的一个$R_1[x]$-子模,当然也是$R_{r,s}$的一个$R_1$-子模. 下面,我们给出了$\tau$-循环码$\boldsymbol{C}$作为$R_{r,s}$的$R_1$-子模的极小生成元集.

**定理2**　设$\boldsymbol{C}=<(f(x)h(x)+2f(x)\mid 0),(l(x)\mid u\tilde{f}(x))>$是$R_1\times R_2$上码长为$r+s$的$\tau$-循环码,其中$f(x)$、$g(x)$、$h(x)$是$R_1$上的首一多项式且$f(x)g(x)h(x)=x^r-1$;$\tilde{f}(x)$是$x^s-1$的首一因式. 令$\deg(g(x))=t$,$\deg(h(x))=k$,

$\deg(\tilde{f}(x))=s-l$. 设

$$\begin{aligned}S_1&=\{(f(x)h(x)+2f(x)\mid 0),x*(f(x)h(x)+2f(x)\mid 0),\cdots,x^{t-1}*(f(x)h(x)+2f(x)\mid 0)\},\\S_2&=\{(2f(x)g(x)\mid 0),x*(2f(x)g(x)\mid 0),\cdots,x^{k-1}*(2f(x)g(x)\mid 0)\},\\S_3&=\{(l(x)\mid u\tilde{f}(x)),x*(l(x)\mid u\tilde{f}(x)),\cdots,x^{l-1}*(l(x)\mid u\tilde{f}(x))\}.\end{aligned}$$

则$S_1\cup S_2\cup S_3$是$\boldsymbol{C}$作为$R_{r,s}$的$R_1$-子模的极小生成元集. 因此,$\tau$-循环码$\boldsymbol{C}$的码字个数为$4^t2^k2^l=4^t2^{k+l}$.

**证明**　设$c(x)$是$\tau$-循环码$\boldsymbol{C}$中的任意一个码字,则存在$R_1[x]$中的多项式$p(x)$和$q(x)$使得

$$c(x)=p(x)*(f(x)h(x)+2f(x)\mid 0)+q(x)*(l(x)\mid u\tilde{f}(x)).$$

如果$\deg(p(x))\leqslant t-1$,则

$p(x)*(f(x)h(x)+2f(x)\mid 0)\in\mathrm{Span}(S_1\cup S_2)$,其中$\mathrm{Span}(S_1\cup S_2)$表示由$S_1\cup S_2$生成的$R_{r,s}$的$R_1[x]$-子模. 否则,存在$R_1[x]$中的多项式$p_1(x)$以及$q_1(x)$使得

$$p(x)=p_1(x)g(x)+q_1(x),$$

其中$q_1(x)=0$或$\deg(q_1(x))\leqslant t-1$. 因此$p(x)*(f(x)h(x)+2f(x)\mid 0)=(q_1(x)f(x)h(x)+2q_1(x)f(x)\mid 0)+(2p_1(x)f(x)g(x)\mid 0)$.

如果$\deg(p_1(x))\leqslant k-1$,则

$p(x)*(f(x)h(x)+2f(x)\mid 0)\in\mathrm{Span}(S_1\cup S_2)$.

否则,在$R_1[x]$中存在多项式$p_2(x)$以及$q_2(x)$使得

$$p_1(x)=h(x)p_2(x)+q_2(x),$$

其中$q_2(x)=0$或$\deg(q_2(x))\leqslant k-1$. 因此,

$$(2p_1(x)f(x)g(x)\mid 0)=(2q_2(x)f(x)g(x)\mid 0)\in\mathrm{Span}(S_2).$$

因此,

$p(x)*(f(x)h(x)+2f(x)\mid 0)\in\mathrm{Span}(S_1\cup S_2)$.

如果$\deg(q(x))\leqslant l-1$,则

$q(x)*(l(x)\mid u\tilde{f}(x))=(q(x)l(x)\mid u\phi(q(x))\tilde{f}(x))\}\in\mathrm{Span}(S_3)$.

否则,存在$R_1[x]$中存在多项式$r_1(x)$以及$s_1(x)$使得

$$q(x)=r_1(x)\frac{x^s-1}{\tilde{f}(x)}+s_1(x),$$

其中$s_1(x)=0$或$\deg(s_1(x))\leqslant l-1$. 因此,

$$q(x)*(l(x)\mid u\tilde{f}(x))=r_1(x)\frac{x^r-1}{\tilde{f}(x)}*(l(x)\mid u\tilde{f}(x))+s_1(x)*(l(x)\mid u\tilde{f}(x)).$$

注意到$s_1(x)*(l(x)\mid u\tilde{f}(x))\in\mathrm{Span}(S_3)$. 另外,因为$(f(x)h(x)+2f(x))\left|\frac{x^s-1}{\tilde{f}(x)}l(x)\right.$,

所以

$$(r_1(x)\frac{x^r-1}{\tilde{f}(x)}l(x)\mid 0)\in\mathrm{Span}(S_1\cup S_2).$$

故,

$$c(x)\in\mathrm{Span}(S_1\cup S_2\cup S_3).$$

显然,$S_1\cup S_2\cup S_3$中的元素都是$R_1$-线性无关的,所以$S_1\cup S_2\cup S_3$是$C$的$R_1$-极小生成元集.

在本文的最后,我们利用$R_1\times R_2$上的$\tau$-循环码

构造有限域 $F_2$ 上的非线性码. 首先,我们给出 $R_1\times R_2$ 到有限域 $F_2$ 上的 Gray 映射如下

$$f:R_1\times R_2\to F_2^2\times F_2^2$$
$$r=(a+2b\,|\,c+ud)\mapsto(b,a+b,d,c+d),$$

其中 $a,b,c,d\in F_2$. 显然,$f$ 是一个双射. $R_1\times R_2$ 中元素 $r$ 的 Gray 重量定义为 $f(r)$ 的 Hamming 重量. $f$ 可以自然的推广到 $R_1^r\times R_1^s$ 上. $R_1^r\times R_1^s$ 中元素的 Gray 重量定义为每个分量的 Gray 重量之和. 令 $\boldsymbol{C}$ 是 $R_1\times R_2$ 上码长为 $r+s$ 的线性码,则 $\boldsymbol{C}$ 的极小 Gray 距离等于 $\boldsymbol{C}$ 中非零码字的极小 Gray 重量. 另外,由 Gray 映射的定义知 $f$ 是一个从 $\boldsymbol{C}$ 的 Gray 距离到 $f(\boldsymbol{C})$ 的保距映射,即 $\boldsymbol{C}$ 的极小 Gray 距离等于 $f(\boldsymbol{C})$ 的极小 Hamming 距离. 值得注意的是,$f$ 一般情况下不是一个 $F_2$ - 线性映射. 因此若 $\boldsymbol{C}$ 是 $R_1\times R_2$ 上码长为 $r+s$ 的线性码,则 $f(\boldsymbol{C})$ 一般情况下是一个码长为 $2r+2s$ 的二元非线性码.

**例 1** 令 $\boldsymbol{C}$ 是 $R_1\times R_2$ 上码长为 15 的 $\tau$ - 循环码,其中 $r=12,s=3$. 在 $R_1$ 上我们有

$$x^{12}-1=(x+1)(x+3)(x^2+1)(x^2+x+1)(x^2+3x+1)(x^4+3x^2+1).$$
$$f(x)=(x+3)(x^2+1),$$
$$g(x)=(x+1)(x^2+3x+1)(x^4+3x^2+1),$$
$$h(x)=x^2+x+1.$$

另外,在 $R_2$ 上我们有

$$x^3-1=(x+1)(x^2+x+1).$$

不妨令 $\tilde{f}(x)=x^2+x+1$. 令 $l(x)=0$,则由定理 2,我们可以得到 $\tau$ - 循环码 $\boldsymbol{C}$ 具有如下的极小生成元集

$$S_1=\{(x^5+3x^3+x^2+2x+1\,|\,0),(x^6+3x^4+x^3+2x^2+x\,|\,0),\cdots,(x^{11}+3x^9+x^8+2x^7+x^6\,|\,0)\},$$
$$S_2=\{(2x^{10}+2x^9+2x^7+2x^6+2x^4+2x^3+2x+2\,|\,0),(2x^{11}+2x^{10}+2x^8+2x^7+2x^5+2x^4+2x^2+2x\,|\,0)\},$$
$$S_3=\{0\,|\,ux^2+ux+u\}.$$

由极小生成元集,我们可以给出码 $\boldsymbol{C}$ 的一个 $Z_4$ - 生成矩阵 $\boldsymbol{G}$,其中

$$\boldsymbol{G}=\begin{pmatrix}
1&2&1&3&0&1&0&0&0&0&0&0&0&0&0\\
0&1&2&1&3&0&1&0&0&0&0&0&0&0&0\\
0&0&1&2&1&3&0&1&0&0&0&0&0&0&0\\
0&0&0&1&2&1&3&0&1&0&0&0&0&0&0\\
0&0&0&0&1&2&1&3&0&1&0&0&0&0&0\\
0&0&0&0&0&1&2&1&3&0&1&0&0&0&0\\
0&0&0&0&0&0&1&2&1&3&0&1&0&0&0\\
2&2&0&2&2&0&2&2&0&2&2&0&0&0&0\\
0&2&2&0&2&2&0&2&2&0&2&2&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&u&u&u
\end{pmatrix}$$

码 $\boldsymbol{C}$ 的码字个数是 $2^{17}$,极小 Gray 距离是 4. 利用 Gray 映射,我们可以构造出一个参数为 $(30,2^{17},4)$ 的二元非线性码.

**例 2** 令 $r=35,s=5$,码 $\boldsymbol{C}$ 是 $R_1\times R_2$ 上码长为 40 的 $\tau$ - 循环码. 在 $R_1$ 上我们有

$$\begin{aligned}x^{35}-1=&(x+3)(x^3+2x^2+x+3)(x^3+3x^2+2x+3)(x^4+x^3+x^2+x+1)(x^{12}+2x^{11}+3x^{10}+x^9+x^8+3x^7+2x^6+2x^5+x^4+2x^3+3x^2+x+1)\\&(x^{12}+x^{11}+3x^{10}+2x^9+x^8+2x^7+2x^6+3x^5+x^4+x^3+3x^2+2x+1).\end{aligned}$$

不妨令

$$f(x)=x^4+x^3+x^2+x+1,$$
$$g(x)=(x^3+2x^2+x+3)(x^3+3x^2+2x+3),$$
$$\begin{aligned}h(x)=&(x+3)(x^{12}+2x^{11}+3x^{10}+x^9+x^8+3x^7+2x^6+2x^5+x^4+2x^3+3x^2+x+1)\\&(x^{12}+x^{11}+3x^{10}+2x^9+x^8+2x^7+2x^6+3x^5+x^4+x^3+3x^2+2x+1).\end{aligned}$$

另外,在 $R_2$ 上我们有

$$x^5-1=(x+1)(x^4+x^3+x^2+x+1).$$

不妨令 $\tilde{f}(x)=x^4+x^3+x^2+x+1$.

设 $l(x)=0$,则 $\tau$ - 循环码 $\boldsymbol{C}$ 的极小生成元集

$$S_1=\{(x^{29}+3x^{28}+x^{22}+3x^{21}+x^{15}+3x^{14}+x^8+3x^7+2x^4+2x^3+2x^2+3x+1\,|\,0),\cdots,(x^{34}+3x^{33}+x^{27}+3x^{26}+x^{20}+3x^{19}+x^{13}+3x^{12}+2x^9+2x^8+2x^7+3x^6+x^5\,|\,0)\},$$
$$S_2=\{(2x^{10}+2x^8+2x^6+2x^5+2x^4+2x^2+2\,|\,0),\cdots,(2x^{34}+2x^{32}+2x^{30}+2x^{29}+2x^{28}+2x^{26}+2x^{24}\,|\,0)\},$$
$$S_3=\{(0\,|\,ux^4+ux^3+ux^2+ux+u)\}.$$

由极小生成元集,我们可以给出码 $\boldsymbol{C}$ 的一个 $Z_4$ - 生成矩阵 $\boldsymbol{G}$,其中

$$\boldsymbol{G}=\begin{pmatrix}
1&3&2&2&2&0&0&3&1&0&0&0&0&0&3&1&0&0&0&0\\
\vdots&&&&&&&&&&&&&&&&&&&\vdots\\
0&0&0&0&0&1&3&2&2&2&0&0&3&1&0&0&0&0&0&3\\
2&0&2&0&2&2&2&0&2&0&2&0&0&0&0&0&0&0&0&0\\
\vdots&&&&&&&&&&&&&&&&&&&\vdots\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

$$\begin{pmatrix}
0&3&1&0&0&0&0&0&3&1&0&0&0&0&0&0&0&0&0\\
&&&&&&&&&&&&&&&\vdots&&\\
1&0&0&0&0&0&3&1&0&0&0&0&0&3&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
&&&&&&&&&&&&&&&\vdots&&\\
0&0&0&0&2&0&2&0&2&2&2&0&2&0&2&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&u&u&u&u
\end{pmatrix}$$

码 $\boldsymbol{C}$ 中的码字个数是 $2^{38}$,极小 Gray 距离是 8. 利用 Gray 映射,我们可以构造出一个参数为 $(80,2^{38},8)$ 的二元非线性码. 通过对比二元非线性码表[11],该码是一个新的二元非线性码.

## 5　结论

本文中我们研究了 $Z_4 \times (F_2 + uF_2)$ 上的一类循环码的代数结构,明确了其生成元结构并由此构造了二元非线性码. 若 $R_1$ 和 $R_2$ 是两个任意的有限链环,能否给出 $R_1 \times R_2$ 上某几类循环码的代数结构并明确其生成元? 近期,Borgers 等编码组在文献[12]中声称解决了该问题. 文[12]中的大部分结果依赖于 $R_1$ 到 $R_2$ 的满同态映射. 但是,需要指出的是环 $R_1$ 到 $R_2$ 不一定存在同态满射. 本文作者已同 Borgers 等联系,他们承认了文[12]中的关键失误并声明 $R_1 \times R_2$ 上循环码的代数结构仍是一个有待解决的问题.

### 参考文献


[1] Hammons A ,Kumar P,Calderbank A,Sloane N,Solé P. The $Z_4$-linearity of Kerdock,Preparata,Goethals,and related codes[J]. IEEE Trans Inform Theory,1994,40(2):301 – 319.

[2] 施敏加,杨善林,朱士信. 环 $F_2 + uF_2$ 上长度为 $2^e$ 的循环码的距离[J]. 电子学报,2011,39 (1):29 – 34.
Shi M,Yang S,Zhu S. The distance of cyclic codes with the length $2^e$ over the ring $F_2 + uF_2$[J]. Acta Electronica Sinica,2011,39(1):29 – 34. (in Chinese)

[3] 施敏加. 环 $F_2 + uF_2 + \cdots + u^{m-1}F_2$ 上常循环自对偶码[J]. 电子学报,2013,41(6):1088 – 1092.
Shi M. The self-dual constacyclic codes over the ring $F_2 + uF_2 + \cdots + u^{m-1}F_2$[J]. Acta Electronica Sinica,2013,41(6):1088 – 1092. (in Chinese)

[4] Shi M,Qian L,Audin N,Solé P. On constacycylic code over $Z_4[u]/<u^2 - 1>$[J]. Finite Field Appl,2017,45(1):86 – 95.

[5] Borges J,Fernández-Córdoba C,Pujol J,Rifà J. $Z_2Z_4$-linear codes:Generator matrices and duality[J]. Des Codes Cryptogr,2010,54(2):167 – 179.

[6] Dougherty S T,Fernández-Córdoba C. $Z_2Z_4$-Additive formally self-dual codes[J]. Des Codes Cryptogr,2014,72(2):435 – 453.

[7] Fernández-Córdoba C,Pujol J,Villanueva M. $Z_2Z_4$-linear codes:rank and kernel[J]. Des Codes Cryptogr,2010,56(1):43 – 59.

[8] Abualrub T,Siap I,Aydin N. $Z_2Z_4$-additive codes[J]. IEEE Trans Inform Theory,2014,60(3):1508 – 1514.

[9] Wan Z-X. Quaternary Codes[M]. Pte Ltd:World Scientific Publishing Company,1997.

[10] Dinh H,López-permouth S. Cyclic and negacyclic codes over finite chain rings[J]. IEEE Trans Inform Theory,2004,50(8):728 – 1743.

[11] Litsyn S,Rains E M,Sloane N J A. Tables of nonlinear binary codes[DB/OL]. http://www.eng.tau.ac.il/lisyn/tableand/index.html,2016-11-20.

[12] Borges J,Fernández Córdoba C,Ten-Valls R. Linear and cyclic codes over direct product of finite chain rings[A]. Processing of the 16th International Conference on Computational and Mathematical Method in Science and Engineering CMMSE 2016[C]. Cádiz,Rota,2016. 4 – 8.


### 作者简介


**高　健**　男,1987 年生于山东德州. 博士、讲师,研究方向为编码理论及其应用.
E-mail:dezhougaojian@163.com



**吕京杰**　男,1993 年生于山东日照. 硕士研究生,研究方向为编码理论及其应用.
E-mail:juxianljj@163.com