环 $F_2+uF_2+u^2F_2$ 上的常循环码

丁 健,李红菊,左学武,梁 静
(安徽新华学院公课部,安徽合肥 230088)

摘 要: 常循环码是一类重要的纠错码,本文基于(x^n-1)在 $F_2[x]$上的分解,探讨了环 $R=F_2+uF_2+u^2F_2$ 上任意长度的$(1+\lambda u)$常循环码的极小生成元集(λ 为 R 上的单位).通过分析该环上循环码和常循环码的置换等价性,得到了该环上码长为奇数及码长 $N\equiv 2(\mathrm{mod}\ 4)$时$(1+u^2)$常循环码的生成多项式和极小生成元集.

关键词: 循环码; 常循环码; 极小生成元集; 生成多项式
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2015)01-0145-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.01.023

Constacyclic Codes over the Ring $F_2+uF_2+u^2F_2$

DING Jian, LI Hong-ju, ZUO Xue-wu, LIANG Jing
(*Department of Common Course, Anhui Xinhua University, Hefei, Anhui* 230088, *China*)

Abstract: Constacyclic codes are a kind of important error-correcting codes. In view of the factorization of (x^n-1) in $F_2[x]$, the minimal generating set of $(1+\lambda u)$ constacyclic codes with an arbitrary length N over the ring $R=F_2+uF_2+u^2F_2$ are investigated, where λ is a unit of the ring R. Based on the analysis of the equivalence between cyclic codes and constacyclic codes over the ring R, the generator polynomials and minimal generating set of $(1+u^2)$ constacyclic codes with odd length are obtained, so are the codes with length $N\equiv 2(\mathrm{mod}\ 4)$.

Key words: cyclic codes; constacyclic codes; the minimal generating set; generator polynomials

1 引言

环 F_2+uF_2 是介于环 Z_4 和域 F_4 之间的一种四元环,2006 年,Qian[1]等人讨论了环 F_2+uF_2 上的单根循环码和常循环码的结构,得到该环上单根$(1+u)$常循环码的 Gray 象是距离不变的二元线性循环码,此后此类环上的循环码和常循环码被广泛研究[2~11]. Abular[2,3]等人确定了环 F_2+uF_2 和 $F_2+uF_2+u^2F_2$ 上任意长度的循环码、环 F_2+uF_2 上任意长度的常循环码的结构,得到了其秩和极小生成元集;施敏加[4,5]等人研究了环 F_2+uF_2 上长为 2^e 的循环码和$(1+u)$常循环码、$F_q[u]/<u^k>$上的单根常循环码的秩和极小生成元集;Zhu Shixin[7]等人给出了有限链环上的单根循环码和负循环码的秩;Kai Xiaoshan[8]等人确定了环 $F_p[u]/<u^k>$上的$(1+\lambda u)$常循环码的结构.近来,丁健[9]等人研究了环 $F_{p^m}+uF_{p^m}$常循环码的置换等价性,得到该环上一系列常循环码的结构;胡庆[10]等人探讨了环 $F_q+uF_q+u^2F_q$ 上任意长度的循环码的结构和秩;施敏加[11]确定了环 $F_2[u]/<u^k>$的$(1+\lambda u)$常循环自对偶码存在的充要条件.大量的文章研究了环 $F_q[u]/<u^k>$上的单根循环码、$(1+\lambda u)$单根及重根常循环码的结构、秩和极小生成元集,但是此类环上的其它重根常循环码的理论仍很不完善且单根 α 常循环码的秩、极小生成元集皆是基于$(x^N-\alpha)$的分解.本文利用(x^n-1)在 $F_2[x]$上的分解及环 $F_2+uF_2+u^2F_2$ 上循环码、常循环码间的置换等价性,得到了该环上任意长度的$(1+\lambda u)$常循环码的秩和极小生成元集(λ 为 R 上的单位)、单根$(1+u^2)$常循环及码长 $N\equiv 2(\mathrm{mod}\ 4)$时的$(1+u^2)$常循环码的生成多项式和极小生成元集,对进一步确定该环上常循环码的距离分布、译码有一定的意义.

2 基本概念

令 R 代表环 $F_+uF_2+u^2F_2$,其中 $u^3=0$, $F_2=GF(2)$.在 $F_2[x]$中,令 $x^n-1=f_1(x)f_2(x)\cdots f_j(x)$,其中 n 为奇数且$f_1(x)f_2(x)\cdots f_j(x)$为 $F_2[x]$上两两互素的首一不可约多项式,以下简记为 f_1、f_2、…、f_j.令 C 是

收稿日期:2014-02-13;修回日期:2014-07-01;责任编辑:蓝红杰
基金项目:安徽省教育厅自然科学项目(No.KJ2013B107);安徽新华学院科研及质量工程项目(No.2013tskcx06, No.2013jgkcx09, No.2014Zr009)

环 R 上长为 $N=2^e n$ 的码(e 为非负整数)、$P(C)$是码 C 的多项式表示,则 $P(C)=\{\sum_{i=0}^{N-1} c_i x^i \mid (c_0,c_1,\cdots,c_{N-1}) \in C\}$.

令 V 是从 R^N 到 R^N 的映射:$V(c_0,c_1,\cdots,c_{N-1})=(\alpha c_{N-1},c_0,c_1,\cdots,c_{N-2})$,其中 α 是环 R 上的单位,则 C 是环 R 上的 α 常循环码$\Leftrightarrow V(C)=C$.

显然有如下命题:

命题 1 环 R 上长为 N 的码 C 是 α 常循环码$\Leftrightarrow P(C)$是 $R[x]/<x^N-\alpha>$的理想.

环 R 上循环码、常循环码 C 的基所含元素的个数记为 $rak(C)$,也即码 C 极小生成元集中的元素个数,称之为该环上码 C 的秩.

3 环 R 上任意长度的$(1+\lambda u)$常循环码

在文献[8]的定理 3.4 及推论 4.10 中令 $k=3$ 可得如下引理.

引理 1 设 C 是环 R 上长为 $N=2^e n$ 的$(1+\lambda u)$常循环码(λ 为 R 上的单位),则 $C=<f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}>$,其中 $0\leqslant k_i\leqslant 2^e\cdot 3$, $i=1,2,\cdots,j$, 此时 $|C|=2^{3N-\omega}$, $\omega=\sum_{i=1}^{j} k_i\deg(f_i)$.

由引理 1 易得定理 1.

定理 1 对于环 R 上长为 $N=2^e n$ 的$(1+\lambda u)$常循环码 $C=<f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}>$,当 $\max\{k_1,k_2,\cdots,k_j\}=0$ 时码 $C=<1>$, $rank(C)=N$,其极小生成元集为

$$\beta=\{1,x,x^2,\cdots x^{N-1}\}.$$

定理 2 对于环 R 上长为 $N=2^e n$ 的$(1+\lambda u)$常循环码 $C=<f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}>$,当 $0<\max\{k_1,k_2,\cdots,k_j\}\leqslant 2^e$ 时, $rank(C)=N$. 令 $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=g$, $\deg(g)=r\geq 1$,则 $g\mid(x^N-1)$,此时

(1)若 $\min\{k_1,k_2,\cdots,k_j\}<2^e$,则码 $C=<g>$,其极小生成元集为 $\beta=\{g,xg,\cdots,x^{N-r-1}g,u,ux,\cdots,ux^{r-1}\}$.

(2)若 $\min\{k_1,k_2,\cdots,k_j\}=2^e$ 即 $k_1=k_2=\cdots=k_j=2^e$,则码 $C=<u>$,其极小生成元集为 $\beta=\{u,ux,\cdots,ux^{N-1}\}$.

证明 由 g 的取法易得 $g\mid(x^N-1)$且 $\deg(g)=r\geq 1$.

(1)假设存在 $a_i,b_i,c_i,D_l,E_l\in F_2$, $i=0,1,\cdots,N-r-1$, $l=0,1,\cdots,r-1$ 使得

$$\sum_{i=0}^{N-r-1}(a_i+ub_i+u^2c_i)x^i g+\sum_{l=0}^{r-1}(D_l+uE_l)ux^l=0$$

则

$$g\sum_{i=0}^{N-r-1}a_i x^i+u\sum_{l=0}^{r-1}D_l x^l+ug\sum_{i=0}^{N-r-1}b_i x^i+u^2\sum_{l=0}^{r-1}E_l x^l+u^2 g\sum_{i=0}^{N-r-1}c_i x^i=0 \quad (1)$$

因为 $u\mid 0$、$u\mid u$,所以 $u\mid(g\sum_{i=0}^{N-r-1}a_i x^i)$即$\frac{x^N-1}{g}\mid\sum_{i=0}^{N-r-1}a_i x^i$.

而 $N-r-1<\deg(\frac{x^N-1}{g})=N-r<N$,

故 $a_0=a_1=\cdots=a_{N-r-1}=0$ (2)

所以等式(1)可化为 $u\sum_{i=0}^{r-1}D_l x^l+ug\sum_{i=0}^{N-r-1}b_i x^i+u^2\sum_{i=0}^{r-1}E_l x^l+u^2 g\sum_{i=0}^{N-r-1}c_i x^i=0$.

又因为 $ug\mid 0$、$ug\mid u(\frac{x^N-1}{\lambda})$即 $ug\mid u^2$,所以 $ug\mid(u\sum_{l=0}^{r-1}D_l x^l)$即 $g\mid\sum_{l=0}^{r-1}D_l x^l$.

而 $r-1<\deg(g)=r<N$,

故 $D_0=D_1=\cdots=D_{r-1}=0$. (3)

所以等式(1)可化为 $ug\sum_{i=0}^{N-r-1}b_i x^i+u^2\sum_{l=0}^{r-1}E_l x^l+u^2 g\sum_{i=0}^{N-r-1}c_i x^i=0$.

因为 $u^2\mid 0$、$u^2\mid u^2$,所以 $u^2\mid ug\sum_{i=0}^{N-r-1}b_i x^i$ 即$\frac{x^N-1}{g}\mid\sum_{i=0}^{N-r-1}b_i x^i$.

而 $N-r-1<N-r=\deg(\frac{x^N-1}{g})<N$,

故 $b_0=b_1=\cdots=b_{N-r-1}=0$ (4)

所以等式(1)可化为 $u^2\sum_{l=0}^{r-1}E_l x^l+u^2 g\sum_{i=0}^{N-r-1}c_i x^i=0$. 所以 $u^2 g\mid u^2\sum_{l=0}^{r-1}E_l x^l$ 即 $g\mid\sum_{l=0}^{r-1}E_l x^l$.

而 $r-1<r=\deg(g)<N$,

故 $E_0=E_1=\cdots=E_{r-1}=0$ (5)

所以等式(1)可化为 $u^2\sum_{i=0}^{N-r-1}c_i x^i=0=u^3$,因此$\frac{x^N-1}{g}\mid\sum_{i=0}^{N-r-1}x_i x^i$.

而 $N-r-1<N-r=\deg(\frac{x^N-1}{g})<N$,

故 $c_0=c_1\cdots=c_{N-r-1}=0$ (6)

由等式(1)至(6)可知 $\beta=\{g,xg,\cdots,x^{N-r-1}g,u,ux,\cdots,ux^{r-1}\}$可线性组合成$(2^{N-r})^3\cdot(2^r)^2=2^{3N-r}$个码字,且显然组合成的码字皆在码 $C=<g>$中,又由引理 1 可得$|C|=2^{3N-r}$,故 β 为码$C=<g>$的极小生成元集.

(2)由定理 1 可得.

定理 3 对于环 R 上长为 $N=2^e n$ 的$(1+\lambda u)$常循环码 $C=<f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}>$,当 $2^e<\max\{k_1,k_2,\cdots,k_j\}\leqslant$

2^{e+1}时,$rank(C)=N$,此时

(1)若 $\min\{k_1,k_2,\cdots,k_j\}<2^e$,则必存在 $F_2[x]$上的首一多项式 f 和满足条件 $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=fg$、$f\mid g\mid(x^N-1)$的次数最高的首一多项式 g.令 $\deg(g)=r,\deg(f)=s\geq 1$.

①当 $r>s$ 时,码 $C=<fg>$,其极小生成元集为 $\beta=\{fg,xfg,\cdots,x^{N-r-1}fg,uf,uxf,\cdots,ux^{r-s-1}f,u^2,u^2x,\cdots,u^2x^{s-1}\}$.

②当 $r=s$ 即 $f=g$ 时,码 $C=<g^2>$,其极小生成元集为 $\beta=\{g^2,xg^2,\cdots,x^{N-r-1}g^2,u^2,u^2x,\cdots,u^2x^{r-1}\}$.

(2)若 $2^e\leqslant\min\{k_1,k_2,\cdots,k_j\}<2^{e+1}$,则必存在 $F_2[x]$上的首一多项式 $g=f_1^{k_1-2^e}f_2^{k_2-2^e}\cdots f_j^{k_j-2^e}$ 使得码 $C=<ug>$且 $g\mid(x^N-1)$.令 $\deg(g)=r\geq 1$,则该码的极小生成元集为 $\beta=\{ug,uxg,\cdots,ux^{N-r-1}g,u^2,u^2x,\cdots,u^2x^{r-1}\}$.

(3)若 $\min\{k_1,k_2,\cdots,k_j\}=2^{e+1}$即 $k_1=k_2=\cdots=k_j=2^{e+1}$,则码 $C=<u^2>$,其极小生成元集为 $\beta=\{u^2,xu^2,\cdots x^{N-1}u^2\}$.

证明　(1)若 $\min\{k_1,k_2,\cdots,k_j\}<2^e$,易知必存在 $F_2[x]$上的首一多项式 f 和满足条件 $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=fg$、$f\mid g\mid(x^N-1)$的次数最高的首一多项式 g.令 $\deg(g)=r,\deg(f)=s\geq 1$.

①当 $r>s$ 时,假设存在 $a_i,b_i,c_i,a_l',b_l',D_m\in F_2$,$i=0,1,\cdots,N-r-1$,$l=0,1,\cdots,r-s-1$,$m=0,1,\cdots,s-1$ 使得 $\sum_{i=0}^{N-r-1}(a_i+ub_i+u^2c_i)x^ifg+\sum_{l=0}^{r-s-1}(a_l'+ub_l')ux^lf+\sum_{m=0}^{s-1}D_mu^2x^m=0$,则

$$fg\sum_{i=0}^{N-r-1}a_ix^i+uf\sum_{l=0}^{r-s-1}a_l'x^l+ufg\sum_{i=0}^{N-r-1}b_ix^i+u^2\sum_{m=0}^{s-1}D_mx^m+u^2f\sum_{l=0}^{r-s-1}b_l'x^l+u^2fg\sum_{i=0}^{N-r-1}c_ix^i=0\tag{7}$$

由 f,g 的取法可知$\frac{x^N-1}{g}$与 f 互素即$(\frac{x^N-1}{g},f)=1$,类似定理 2(1)可证得 $a_i=b_i=c_i=a_i'=b_i'=D_m=0$,即表示 $\beta=\{fg,xfg,\cdots,x^{N-r-1}fg,uf,uxf,\cdots,ux^{r-s-1}f,u^2,u^2x,\cdots,u^2x^{s-1}\}$ 可线性组合成$(2^{N-r})^3\cdot(2^{r-s})^2\cdot 2^s=2^{3N-(r+s)}$个码字,且显然组合成的码字皆在码 C 中,又由引理 1 可得$|C|=2^{3N-(r+s)}$,故 β 为码 $C=<fg>$ 的极小生成元集.

②当 $r=s$ 时,码 $C=<g^2>$,类似①可证得其极小生成元集.

(2)类似定理 2(1)可证.

(3)由定理 1 易得.

定理 4　对于环 R 上长为 $N=2^en$ 的$(1+\lambda u)$常循环码 $C=<f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}>$,当 $2^{e+1}<\max\{k_1,k_2,\cdots,k_j\}\leqslant 2^e\cdot 3$ 时,

(1)若 $\min\{k_1,k_2,\cdots,k_j\}<2^e$,则必存在 $F_2[x]$上的首一多项式 f,g,h 使得 $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=fgh$,$h\mid f\mid g\mid(x^N-1)$,$g$ 是满足条件的次数最高的多项式,在 g 确定后,f 是满足条件的次数最高的多项式.$\deg(g)=r,\deg(f)=s,\deg(h)=t\geq 1$.

①当 $r>s>t$ 时码 $C=<fgh>$,$rank(C)=N-t$,其极小生成元集为 $\beta=\{hfg,xhfg,\cdots,x^{N-r-1}hfg,uhf,uxhf,\cdots,ux^{r-s-1}hf,u^2h,u^2xh,\cdots,u^2x^{s-t-1}h\}$.

②当 $r=s>t$ 即 $f=g$ 时码 $C=<hg^2>$,$rank(C)=N-t$,其极小生成元集为 $\beta=\{hg^2,xhg^2,\cdots,x^{N-r-1}hg^2,u^2h,u^2xh,\cdots,u^2x^{r-t-1}h\}$.

③当 $r>s=t$ 即 $f=h$ 时码 $C=<f^2g>$,$rank(C)=N-s$,其极小生成元集为 $\beta=\{f^2g,xf^2g,\cdots,x^{N-r-1}f^2g,uf^2,uxf^2,\cdots,ux^{r-s-1}f^2\}$.

④当 $r=s=t$ 即 $g=f=h$ 时码 $C=<g^3>$,$rank(C)=N$,其极小生成元集为 $\beta=\{g^3,xg^3,\cdots,x^{N-r-1}g^3\}$.

(2)若 $2^e\leqslant\min\{k_1,k_2,\cdots,k_j\}<2^{e+1}$,则必存在 $F_2[x]$上的首一多项式 f、g 使得 $fg=f_1^{k_1-2^e}f_2^{k_2-2^e}\cdots f_j^{k_j-2^e}$,$f\mid g\mid(x^N-1)$,$g$ 是满足条件的次数最高的多项式.令 $\deg(g)=r,\deg(f)=s\geq 1$.

①当 $r>s$ 时码 $C=<ufg>$,$rank(C)=N-s$,其极小生成元集为 $\beta=\{ufg,xufg,\cdots,x^{N-r-1}ufg,u^2f,u^2xf,\cdots,u^2x^{r-s-1}f\}$.

②当 $r=s$ 即 $f=g$ 时码 $C=<ug^2>$,$rank(C)=N-r$,其极小生成元集为 $\beta=\{ug^2,uxg^2,\cdots,ux^{N-r-1}g^2\}$.

(3)若 $2^{e+1}\leqslant\min\{k_1,k_2,\cdots,k_j\}<2^e\cdot 3$,则必存在 $F_2[x]$上的首一多项式 $g=f_1^{k_1-2^{e+1}}f_2^{k_2-2^{e+1}}\cdots f_j^{k_j-2^{e+1}}$ 使得码 $C=<u^2g>$且 $g\mid(x^N-1)$.令 $\deg(g)=r\geq 1$,码 $C=<u^2g>$的秩 $rank(C)=N-r$,极小生成元集为 $\beta=\{u^2g,u^2xg,\cdots,u^2x^{N-r-1}g\}$.

(4)若 $\min\{k_1,k_2,\cdots,k_j\}=2^e\cdot 3$ 即 $k_1=k_2=\cdots=k_j=2^e\cdot 3$,则码 $C=<u^3>=<0>$.

证明　(1)若 $\min\{k_1,k_2,\cdots,k_j\}<2^e$,则易知必存在 $F_2[x]$上的首一多项式 f,g,h 使得 $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=fgh$,$h\mid f\mid g\mid(x^N-1)$,$g$ 是满足条件的次数最高的多项式,在 g 确定后,f 是满足条件的次数最高的多项式.令 $\deg(g)=r,\deg(f)=s,\deg(h)=t\geq 1$.

①当 $r>s>t$ 时,码 $C=<fgh>$,假设存在 $a_i,b_i,c_i,a_i',b_i',D_m\in F_2$,$i=0,1,\cdots,N-r-1$,$l=0,1,\cdots,r-s-1$,$m=0,1,\cdots,s-t-1$ 使得

$$\sum_{i=0}^{N-r-1}(a_i+ub_i+u^2c_i)x^ihfg+\sum_{l=0}^{r-s-1}(a_l'+ub_l')ux^lhf+\sum_{m=0}^{s-t-1}D_mu^2x^mh=0,$$

则 $$hfg\sum_{i=0}^{N-r-1}a_ix^i+uhf\sum_{l=0}^{r-s-1}a_l'x^l+uhfg\sum_{i=0}^{N-r-1}b_ix^i+u^2h\sum_{m=0}^{s-t-1}D_mx^m+u^2hf\sum_{l=0}^{r-s-1}b_l'x^l+u^2hfg\sum_{i=0}^{N-r-1}c_ix^i=0 \quad (8)$$

而$(\frac{x^n-1}{g},f)=1,(\frac{x^n-1}{g},h)=1$,故类似定理 3(1)可证得 $a_i=b_i=c_i=a_l'=b_l'=D_m=0$,

即表示 $\beta=\{hfg,xhfg,\cdots,x^{N-r-1}hfg,uhf,uxhf,\cdots,ux^{r-s-1}hf,u^2h,u^2xh,\cdots,u^2x^{s-t-1}h\}$ 可线性组合成 $(2^{N-r})^3\cdot(2^{r-s})^2\cdot2^{s-t}=2^{3N-(r+s+t)}$ 个码字,且显然组合成的码字皆在码 $C=<fgh>$ 中,又由引理 1 可得 $|C|=2^{3N-(r+s+t)}$,故 β 为码 $C=<fgh>$ 的极小生成元集.

②、③、④可类似证明.

(2)类似定理 3(1)可证得.

(3)类似定理 2(1)可证得.

(4)显然成立.

4 环 R 上的$(1+u^2)$常循环码

4.1 环 R 上码长$N\equiv1(\mathrm{mod}\ 4)$时的$(1+u^2)$常循环码

当码长 $N\equiv1(\mathrm{mod}\ 4)$时,必存在非负整数 k 使得 $N\equiv4k+1$.令 $\xi_1=1+u+u^2$,构造映射 $\varphi_1:R[x]/<x^N-(1+u)>\to R[x]/<x^N-(1+u^2)>$,$c(x)\to c(\xi_1x)$

引理 2 如上构造的映射 φ_1 为同构映射.

证明 对于任意 $f(x),g(x)\in R[x]$,$f(x)\equiv g(x)(\mathrm{mod}(x^N-(1+u)))$

$\Leftrightarrow$存在 $h(x)\in R[x]$使得 $f(x)-g(x)=h(x)[x^N-(1+u)]$

$\Leftrightarrow f(\xi_1x)-g(\xi_1x)=h(\xi_1x)[\xi_1{}^Nx^N-(1+u)]$

$\Leftrightarrow f(\xi_1x)-g(\xi_1x)=h(\xi_1x)\xi_1{}^N[x^N-(1+u^2)]$

$\Leftrightarrow f(\xi_1x)\equiv g(\xi_1x)\mathrm{mod}[x^N-(1+u^2)]$

所以映射 φ_1 是从 $R[x]/<x^N-(1+u)>$ 到 $R[x]/<x^N-(1+u^2)>$ 的一一映射.

由于 $\varphi_1(f(x)+g(x))=f(\xi_1x)+g(\xi_1x)=\varphi_1(f(x))+\varphi_1(g(x))$

$\varphi_1(f(x)g(x))=f(\xi_1x)g(\xi_1x)=\varphi_1(f(x))\varphi_1(g(x))$

所以映射 φ_1 是从 $R[x]/<x^N-(1+u)>$ 到 $R[x]/<x^N-(1+u^2)>$ 的环同构映射.

由引理 1、引理 2 易得如下定理.

定理 5 设 C 是环 R 上码长 $N\equiv1(\mathrm{mod}\ 4)$的$(1+u^2)$常循环码,则 $C=<f_1^{k_1}(\xi_1x)f_2^{k_2}(\xi_1x)\cdots f_j^{k_j}(\xi_1x)>$,其中 $0\leqslant k_i\leqslant3,i=1,2,\cdots,j$,$x^N-1=f_1(x)f_2(x)\cdots f_j(x)$,其中 $f_1(x),f_2(x),\cdots,f_j(x)$ 为 $F_2[x]$上两两互素的首一不可约多项式,此时 $|C|=2^{3N-\omega}$,$\omega=\sum_{i=1}^{j}k_i\deg(f_i)$.

由引理 2 和定理 1 至定理 5,易得如下定理.

定理 6 对于环 R 上码长 $N\equiv1(\mathrm{mod}\ 4)$的$(1+u^2)$常循环码 $C=<f_1^{k_1}(\xi_1x)f_2^{k_2}(\xi_1x)\cdots f_j^{k_j}(\xi_1x)>$,当 $\max\{k_1,k_2,\cdots,k_j\}=0$ 时码 $C=<1>$,$rank(C)=N$,其极小生成元集为 $\beta=\{1,x,x^2,\cdots x^{N-1}\}$.

定理 7 对于环 R 上码长 $N\equiv1(\mathrm{mod}\ 4)$的$(1+u^2)$常循环码 $C=<f_1^{k_1}c(\xi_1x)f_2^{k_2}(\xi_1x)\cdots f_j^{k_j}(\xi_1x)>$,当 $\max\{k_1,k_2,\cdots,k_j\}=1$ 时,$rank(C)=N$.令 $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=g$,$\deg(g)=r\geq1$,则 $g|(x^N-1)$,此时

(1)若 $\min\{k_1,k_2,\cdots,k_j\}=0$,则码 $C=<g(\xi_1x)>$,其极小生成元集为 $\beta=\{g(\xi_1x),xg(\xi_1x),\cdots,x^{N-r-1}g(\xi_1x),u,ux,\cdots,ux^{r-1}\}$.

(2)若 $\min\{k_1,k_2,\cdots,k_j\}=1$ 即 $k_1=k_2=\cdots=k_j=1$,则码 $C=<u>$,其极小生成元集为 $\beta=\{u,ux,\cdots,ux^{N-1}\}$.

定理 8 对于环 R 上码长 $N\equiv1(\mathrm{mod}\ 4)$的$(1+u^2)$常循环码 $C=<f_1^{k_1}(\xi_1x)f_2^{k_2}(\xi_1x)\cdots f_j^{k_j}(\xi_1x)>$,当 $\max\{k_1,k_2,\cdots,k_j\}=2$时,$rank(C)=N$.

(1)若 $\min\{k_1,k_2,\cdots,k_j\}=0$,则必存在 $F_2[x]$上的首一多项式 f 和满足条件 $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=fg$,$f|g|(x^N-1)$的次数最高的首一多项式 g.令 $\deg(g)=r$,$\deg(f)=s\geq1$.

①当 $r>s$ 时,码 $C=<f(\xi_1x)g(\xi_1x)>$,其极小生成元集为 $\beta=\{f(\xi_1x)g(\xi_1x),xf(\xi_1x)g(\xi_1x),\cdots,x^{N-r-1}f(\xi_1x)g(\xi_1x),uf(\xi_1x),uxf(\xi_1x),\cdots,ux^{r-s-1}f(\xi_1x),u^2,u^2x,\cdots,u^2x^{s-1}\}$.

②当 $r=s$ 即 $f=g$ 时,码 $C=<g^2(\xi_1x)>$,其极小生成元集为 $\beta=\{g^2(\xi_1x),xg^2(\xi_1x),\cdots,x^{N-r-1}g^2(\xi_1x),u^2,u^2x,\cdots,u^2x^{r-1}\}$.

(2)若 $\min\{k_1,k_2,\cdots,k_j\}=1$,则必存在 $F_2[x]$上的首一多项式 $g=f_1^{k_1-1}f_2^{k_2-1}\cdots f_j^{k_j-1}$ 使得码 $C=<ug(\xi_1x)>$ 且 $g|(x^N-1)$.令 $\deg(g)=r\geq1$,该码的极小生成元集 $\beta=\{ug(\xi_1x),uxg(\xi_1x),\cdots,ux^{N-r-1}g(\xi_1x),u^2,u^2x,\cdots,u^2x^{r-1}\}$.

(3)若 $\min\{k_1,k_2,\cdots,k_j\}=2$ 即 $k_1=k_2=\cdots=k_j=2$,则码 $C=<u^2>$,其极小生成元集为 $\beta=\{u^2,xu^2,\cdots x^{N-1}u^2\}$.

定理 9 对于环 R 上码长 $N\equiv1(\mathrm{mod}\ 4)$的$(1+u^2)$常循环码 $C=<f_1^{k_1}(\xi_1x)f_2^{k_2}(\xi_1x)\cdots f_j^{k_j}(\xi_1x)>$,当 $\max\{k_1,k_2,\cdots,k_j\}=3$ 时,

(1)若 $\min\{k_1,k_2,\cdots,k_j\}=0$,则必存在 $F_2[x]$上的首一多项式 f,g,h 使得 $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=fgh$, $h\mid f\mid g\mid(x^N-1)$, g 是满足条件的次数最高的多项式,在 g 确定后,f 是满足条件的次数最高的多项式.令 $\deg(g)=r$, $\deg(f)=s$, $\deg(h)=t\geq 1$.

①当 $r>s>t$ 时码 $C=<f(\xi_1x)g(\xi_1x)h(\xi_1x)>$, $rank(C)=N-t$,其极小生成元集为 $\beta=\{h(\xi_1x)f(\xi_1x)g(\xi_1x),xh(\xi_1x)f(\xi_1x)g(\xi_1x),\cdots,x^{N-r-1}h(\xi_1x)f(\xi_1x)g(\xi_1x),uh(\xi_1x)f(\xi_1x),ux\,h(\xi_1x)f(\xi_1x),\cdots,ux^{r-s-1}\,h(\xi_1x)f(\xi_1x),u^2h(\xi_1x),u^2xh(\xi_1x),\cdots,u^2x^{s-t-1}h(\xi_1x)\}$.

②当 $r=s>t$ 即 $f=g$ 时码 $C=<h(\xi_1x)g^2(\xi_1x)>$, $rank(C)=N-t$,其极小生成元集为 $\beta=\{h(\xi_1x)g^2(\xi_1x),xh(\xi_1x)g^2(\xi_1x),\cdots,x^{N-r-1}h(\xi_1x)g^2(\xi_1x),u^2h(\xi_1x),u^2xh(\xi_1x),\cdots,u^2x^{r-t-1}h(\xi_1x)\}$.

③当 $r>s=t$ 即 $f=h$ 时码 $C=<f^2(\xi_1x)g(\xi_1x)>$, $rank(C)=N-s$,其极小生成元集为 $\beta=\{f^2(\xi_1x)g(\xi_1x),xf^2(\xi_1x)g(\xi_1x),\cdots,x^{N-r-1}f^2(\xi_1x)g(\xi_1x),uf^2(\xi_1x),uxf^2(\xi_1x),\cdots,ux^{r-s-1}f^2(\xi_1x)\}$.

④当 $r=s=t$ 即 $g=f=h$ 时码 $C=<g^3(\xi_1x)>$, $rank(C)=N$,其极小生成元集为 $\beta=\{g^3(\xi_1x),xg^3(\xi_1x),\cdots,x^{N-r-1}g^3(\xi_1x)\}$.

(2)若 $\min\{k_1,k_2,\cdots,k_j\}=1$,则必存在 $F_2[x]$上的首一多项式 f、g 使得 $fg=f_1^{k_1-1}f_2^{k_2-1}\cdots f_j^{k_j-1}$, $f\mid g\mid(x^N-1)$, g 是满足条件的次数最高的多项式,令 $\deg(g)=r$, $\deg(f)=s\geq 1$.

①当 $r>s$ 时码 $C=<uf(\xi_1x)g(\xi_1x)>$, $rank(C)=N-s$,其极小生成元集为 $\beta=\{uf(\xi_1x)g(\xi_1x),xuf(\xi_1x)g(\xi_1x),\cdots,x^{N-r-1}uf(\xi_1x)g(\xi_1x),u^2f(\xi_1x),u^2xf(\xi_1x),\cdots,u^2x^{r-s-1}f(\xi_1x)\}$.

②当 $r=s$ 即 $f=g$ 时码 $C=<ug^2(\xi_1x)>$, $rank(C)=N-r$,其极小生成元集为 $\beta=\{ug^2(\xi_1x),ux\,g^2(\xi_1x),\cdots,ux^{N-r-1}g^2(\xi_1x)\}$.

(3)若 $\min\{k_1,k_2,\cdots,k_j\}=2$,则必存在 $F_2[x]$上的首一多项式 $g=f_1^{k_1-2}f_2^{k_2-2}\cdots f_j^{k_j-2}$ 使得码 $C=<u^2g(\xi_1x)>$且 $g\mid(x^N-1)$.令 $\deg(g)=r\geq 1$,该码的秩 $rank(C)=N-r$,极小生成元集为 $\beta=\{u^2g(\xi_1x),u^2x\,g(\xi_1x),\cdots,u^2x^{N-r-1}g(\xi_1x)\}$.

(4)若 $\min\{k_1,k_2,\cdots,k_j\}=3$ 即 $k_1=k_2=\cdots=k_j=3$,则码 $C=<u^3>=<0>$.

4.2 环 R 上码长 $N\equiv 3\pmod 4$ 时的 $(1+u^2)$ 常循环码

当码长 $N\equiv 3\pmod 4$ 时,必存在非负整数 k 使得 $N=4k+3$.令 $\xi_2=1+u$,构造映射

$\varphi_2: R[x]/<x^N-(1+u)>\to R[x]/<x^N-(1+u^2)>$, $c(x)\to c(\xi_2x)$.

类似引理 2 的证明易得如下引理.

引理 3　如上构造的映射 φ_2 为同构映射.

由于环 R 上码长 $N\equiv 3\pmod 4$ 和码长 $N\equiv 1\pmod 4$ 时的 $(1+u)$ 常循环码的生成多项式的表达形式相同,故只须将定理 5 至定理 9 中所有的 ξ_1x 替换成 ξ_2x,就得到了码长 $N\equiv 3\pmod 4$ 时的 $(1+u^2)$ 常循环码的生成多项式、秩和生成元集.

4.3 环 R 上码长 $N\equiv 2\pmod 4$ 时的 $(1+u^2)$ 常循环码

当码长 $N\equiv 2\pmod 4$ 时,必存在非负整数 k 使得 $N=4k+2$,构造映射 φ_3:

$R[x]/<x^N-1>\to R[x]/<x^N-(1+u^2)>$, $c(x)\to c(\xi_2x)$.

类似引理 2 的证明易得如下引理.

引理 4　如上构造的映射 φ_3 为同构映射.

设 $g(x)$、$p_1(x)$、$p_2(x)$、$a_1(x)$、$a_2(x)$、$q_1(x)$ 皆为 $F_2(x)$上的多项式,以下简记为 g、p_1、p_2、a_1、a_2、q_1,由引理 4 及文献[6]的定理 2 和定理 5 立得如下定理.

定理 10　环 R 上码长 $N\equiv 2\pmod 4$ 的 $(1+u^2)$ 常循环码 C 必是下列三种情形之一:

(1) $C=<g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x)>$,其中在环 R 上 $(g+up_1+u^2p_2)\mid(x^N-1)$且 $\deg(p_2)<\deg(p_1)$.若令 $\deg(g+up_1+u^2p_2)=r$,则 $(1+u^2)$常循环码 C 的秩 $rank(C)=N-r$,其极小生成元集为 $\beta=\{g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x),x[g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x)],\cdots,x^{N-r-1}[g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x)]\}$.

(2) $C=<g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x),u^2a_2(\xi_2x)>$,其中在 F_2 上有 $a_2\mid g\mid(x^N-1)$, $g\mid p_1(\frac{x^N-1}{g})$, $a_2\mid p_1(\frac{x^N-1}{g})$, $a_2\mid p_2(\frac{x^N-1}{g})(\frac{x^N-1}{g})$, $\deg(p_2)<\deg(p_1)$,在 F_2+uF_2 上 $(g+up_1)\mid(x^N-1)$.若令 $\deg(g+up_1+u^2p_2)=r$、$\deg(a_2)=t$,则 $(1+u^2)$常循环码 C 的秩 $rank(C)=N-t$,其极小生成元集为 $\beta=\{g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x),x[g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x)],\cdots,x^{N-r-1}[g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x)],u^2a_2(\xi_2x),xu^2a_2(\xi_2x),\cdots,x^{r-t-1}u^2a_2(\xi_2x)\}$.

(3) $C=<g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x),ua_1(\xi_2x)+u^2q_1(\xi_2x),u^2a_2(\xi_2x)>$,其中在 F_2 上有 $a_2\mid a_1\mid g\mid(x^N-1)$, $a_1\mid p_1(\frac{x^N-1}{g})$, $a_2\mid q_1(\frac{x^N-1}{a_1})$, $a_2\mid p_2$

$(\frac{x^N-1}{g})(\frac{x^N-1}{a_1})$ 且 $\deg(p_2)<\deg(a_2)$, $\deg(q_1)<\deg(a_2)\deg(p_1)$, $\deg(a_1)$. 若令 $\deg(g+up_1+u^2p_2)=r$、$\deg(g+ua_1+u^2p_1)=s$、$\deg(a_2)=t$,则$(1+u^2)$常循环码 C 的秩 $rank(C)=N-t$,其极小生成元集为

$\beta=\{g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x), x[g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x)], \cdots, x^{N-r-1}[g(\xi_2x)+up_1(\xi_2x)+u^2p_2(\xi_2x)], u[a_1(\xi_2x)+uq_1(\xi_2x)], xu[a_1(\xi_2x)+uq_1(\xi_2x)], \cdots, x^{r-s-1}u[a_1(\xi_2x)+uq_1(\xi_2x)], u^2a_2(\xi_2x), xu^2a_2(\xi_2x), \cdots, x^{s-t-1}u^2a_2(\xi_2x)\}$.

5 结束语

本文基于(x^n-1)在 $F_2[x]$上的分解及循环码、常循环码间的置换等价性,给出了环 $F_2+uF_2+u^2F_2$ 上任意长度的$(1+\lambda u)$常循环码的秩和极小生成元集(λ为R 上的单位)、该环上码长为奇数及码长 $N\equiv 2(\mathrm{mod}\ 4)$时的$(1+u^2)$常循环码的生成多项式和极小生成元集,对于环 $F_q[u]/<u^k>$上的情形值得进一步研究.

参考文献

[1] Qian Jianfa, Zhang Lina, Zhu Shixin. $(1+u)$constacyclic and cyclic codes over F_2+uF_2[J]. Applied Mathematics Letters, 2006, 19(8): 820 – 823.

[2] Abular T, Siap I. Cyclic codes over the ring Z_2+uZ_2 and $Z_2+uZ_2+u^2Z_2$[J]. Designs Codes and Cryptography, 2007, 42(3): 273 – 287.

[3] Abular T, Siap I. Constacyclic codes over F_2+uF_2[J]. Journal of the Franklin Institute, 2009, 346(5): 520 – 529.

[4] 施敏加,朱士信,环 F_2+uF_2 上长为 2^e 的循环码和$(1+u)$常循环码的秩[J]. 计算机应用研究, 2008, 5(1): 37 – 38.
Shi Minjia, Zhu Shixin. Ranks of repeated-root cyclic codes and $(1+u)$-cycliccodes of length 2^e over ring F_2+uF_2[J]. Application Research of Computers, 2008, 25(1): 37 – 38. (in Chinese)

[5] Shi Minjia, Zhu Shixin. Constacyclic codes over ring $F_q+uF_q+\cdots+u^{k-1}F_q$[J]. Joural of University of Science and Technology of China, 2009, 39(6): 583 – 587.

[6] 丁健,李红菊,刘家保. $F_{p^k}+uF_{p^k}$上的一类常循环码[J]. 合肥工业大学学报(自然科学版), 2010, 34(4): 634 – 635.
DingJian, Li Hongju, Liu Jiabao. A class of constacyclic codes over the ring $F_{p^k}+uF_{p^k}$[J]. Journal of Hefei University of Technology, 2010, 3(4): 634 – 635. (in Chinese)

[7] Zhu Shixin, Shi Minjia, The ranks of cyclic and negacyclic codes over the finite ring R[J]. Journal of Electronics (China), 2008, 25(1): 96 – 101.

[8] Kai Xiaoshan, Zhu Shixin, Li Ping, $(1+\lambda u)$-Constacyclic codes over $F_p[u]/<u^k>$[J]. Journal of the Franklin Institute, 2010, 347: 751 – 762.

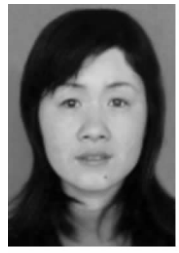
[9] 丁健,李红菊,李海霞,关于环 $F_{p^m}+uF_{p^m}$上循环码的等价性[J]. 中国科学技术大学学报, 2013, 3(2): 334 – 339.
Ding Jian, Li Hongju, Li Haixia. On the equivalence of constacyclic codes over the ring $F_{p^m}+uF_{p^m}$[J]. Joural of University of Science and Technology of China, 2013, 3(2): 334 – 339. (in Chinese)

[10] 胡庆,李平,环 $F_q+uF_q+u^2F_q$ 上任意长度的循环码[J]. 合肥工业大学学报(自然科学版), 2013, 36(2): 243 – 247.
Hu Qing, Li Ping. Cyclic codes of arbitrary lengths over the ring $F_q+uF_q+u^2F_q$[J]. Journal of Hefei University of Technology, 2013, 36(2): 243-247. (in Chinese)

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

作者简介

丁 健 男,1982 年生于安徽合肥. 安徽新华学院讲师. 研究方向为代数编码与密码.
E-mail: dingjian_happy@163.com



李红菊 女,1982 年生于安徽宿州. 安徽新华学院讲师. 研究方向为代数编码与密码.
E-mail: zhenxidj.happy@163.com