第45卷第1期 中国科学技术大学学报 Vol. 45, No. 1
2015年1月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jan. 2015

文章编号:0253-2778(2015)01-0040-08

环 $F_2+uF_2+u^2F_2$ 上的 $(1+u)$ 常循环码

丁 健,李红菊

(安徽新华学院公课部,安徽合肥 230088)

摘要:基于 (x^n-1) 在 $F_2[x]$ 上的分解,研究了环 $R=F_2+uF_2+u^2F_2$ 上任意长度的 $(1+u)$ 常循环码的秩和极小生成元集,定义了环 R 到 F_2^4 的一个新的 Gray 映射,确定了环 R 上任意长度的 $(1+u)$ 常循环码的 Gray 象的结构及 Gray 象的生成多项式,得到了一些最优的二元线性循环码.

关键词:常循环码;秩;极小生成元集;Gray 映射

中图分类号:TN911.22 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2015.01.007

引用格式:Ding Jian, Li Hongju. $(1+u)$-constacyclic codes over the ring $F_2+uF_2+u^2F_2$ [J]. Journal of University of Science and Technology of China, 2015,45(1):40-47.

丁健,李红菊. 环 $F_2+uF_2+u^2F_2$ 上的 $(1+u)$ 常循环码[J]. 中国科学技术大学学报,2015,45(1):40-47.

$(1+u)$-constacyclic codes over the ring $F_2+uF_2+u^2F_2$

DING Jian, LI Hongju

(*Department of Common Course, Anhui Xinhua University, Hefei* 230088, *China*)

Abstract: In view of the factorization of (x^n-1) in $F_2[x]$, the minimal generating set and rank of $(1+u)$-constacyclic codes with an arbitrary length over the ring $R=F_2+uF_2+u^2F_2$ were studied. A new Gray map from R to F_2^4 was defined, the structures and generator polynomials of the Gray image of a linear $(1+u)$-constacyclic code with an arbitrary length were determined, and some optimal binary linear cyclic codes were obtained.

Key words: constacyclic codes; rank; the minimal generating set; Gray map

0 引言

1994年,Roger等[1]发现了二元 Kerdock 码和 Preparata 码等一些高效的二元非线性码可以看作是环 Z_4 上线性码在 Gray 映射下的二元象,由此从根本上解决了二元非线性 Preparata 码和 Kerdock 码关于重量计数器具有形式对偶性这一困扰人们近30年的问题;2001年,Dougherty 等[2]为了计算环 Z_4 上码的距离定义了秩. 因环 F_2+uF_2 是介于环 Z_4 和域 F_4 之间的一种四元环,Gray 映射是连接环上码和域上码的桥梁,码秩的确定对该码的距离分布、译码均有重要意义,所以环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上的 Gray 映射的构造、码秩的确定成为研究的热点. 文献[3]得到了环 F_2+uF_2 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;文献[4]得到了环 R 上单根 $(1+u^2)$ 常循环码的 Gray 象是距离不变的二元准循环码;文献[5]讨论了有限链环上的单根循环码和负循环码的秩;文献[6]确

收稿日期:2014-03-12;**修回日期**:2014-05-16

基金项目:安徽省高等学校自然科学项目(KJ2013B107),新华学院自然科学项目(2014ZR009)资助.

作者简介:丁健(通讯作者),男,1982年生,硕士/讲师. 研究方向:密码学. E-mail: dingjian_happy@163.com

定了 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上的单根常循环码的秩和极小生成元集；文献[7]研究了环 F_2+uF_2 上任意长度的常循环码的秩、极小生成元集，得到的 Gray 象是二元线性码；文献[8]得到了环 R 上单根 $(1+u+u^2)$ 常循环码的 Gray 象是距离不变的二元线性循环码；文献[9]得到了环 F_p+uF_p 上任意长度的 $(1+\lambda u)$ 常循环码的 Gray 象是距离不变的二元线性循环码；近来，文献[10]得到了环 $F_{p^m}+uF_{p^m}$ 上一批常循环码的 Gray 象的结构；文献[11]给出了环 $F_2[u]/\langle u^4\rangle$ 上的单根 $(1+u+u^2+u^3)$ 常循环码的 Gray 象的结构和生成多项式；此外，文献[12-16]得到的是单根常循环码的 Gray 象，且为二元准循环码. 大量的文章研究了环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上的单根 $(1+\lambda u)$ 常循环码的秩、极小生成元集和 Gray 象的结构，但是单根 α 常循环码的秩、极小生成元集皆是基于 $(x^N-\alpha)$ 的分解，不利于确定常循环码的距离和译码且所得 Gray 象的结构多为准循环码，该环上重根常循环码的秩、极小生成元集和 Gray 象的结构研究的很少. 本文将文献[7]推广至环 R 上的情形，基于 (x^n-1) 在 $F_2[x]$ 上的分解，探讨了环 R 上任意长度的 $(1+u)$ 常循环码的秩和极小生成元集，定义了环 R 到 F_2^4 的一个新的 Gray 映射，证明了环 R 上该常循环码在 Gray 映射下的象是 F_2 上的长为 $4N$ 的循环码且确定了 Gray 象的生成多项式，得到了一些最优的二元线性循环码，这对进一步确定该环上常循环码的距离分布、译码及构造好码有一定的意义.

1　基本概念

令 R 代表环 $F_2+uF_2+u^2F_2$，其中 $u^3=0$，F_2 是以 2 为特征的域. 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 $f_1(x)$、$f_2(x)$、…、$f_j(x)$ 为 $F_2[x]$ 上两两互素的首一不可约多项式，以下简记为

$$f_1、f_2、\cdots、f_j.$$

令 C 是环 R 上长为 $N=2^en$ 的码（e 为非负整数）、$P(C)$ 是码 C 的多项式表示，则

$$P(C)=\{\sum_{i=0}^{N-1}c_ix^i \mid (c_0,c_1,\cdots,c_{N-1})\in C\}.$$

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$\Leftrightarrow V(C)=C$. 易得如下命题：

命题 1.1　环 R 上长为 N 的码 C 是 α 常循环码$\Leftrightarrow P(C)$ 是 $R[x]/\langle x^N-\alpha\rangle$ 的理想.

环 R 上常循环码 C 的基所含元素的个数记为 $\mathrm{rank}(C)$，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.

2　环 R 上任意长度的 $(1+u)$ 常循环码

由文献[9]的定理 3.4 及推论 4.10 可得如下引理：

引理 2.1[9]　设 C 是环 R 上长为 $N=2^en$ 的 $(1+u)$ 常循环码，则

$$C=\langle f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}\rangle.$$

其中，$0\leqslant k_i\leqslant 2^e\cdot 3$，$i=1,2,\cdots,j$，此时 $|C|=2^{3N-\omega}$，$\omega=\sum_{i=1}^{j}k_i\mathrm{dge}(f_i)$.

由引理 2.1 得到如下定理：

定理 2.1　对于环 R 上长为 $N=2^en$ 的 $(1+u)$ 常循环码

$$C=\langle f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}\rangle,$$

当 $\max\{k_1,k_2,\cdots,k_j\}=0$ 时码 $C=\langle 1\rangle$，$\mathrm{rank}(C)=N$，其极小生成元集为：

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

定理 2.2　对于环 R 上长为 $N=2^en$ 的 $(1+u)$ 常循环码

$$C=\langle f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}\rangle,$$

当 $0<\max\{k_1,k_2,\cdots,k_j\}\leqslant 2^e$ 时，$\mathrm{rank}(C)=N$. 令

$$f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=g,$$

则 $\deg(g)=r\geqslant 1$，$g\mid(x^N-1)$，此时：

（Ⅰ）若 $\min\{k_1,k_2,\cdots,k_j\}<2^e$，则码 $C=\langle g\rangle$，其极小生成元集为：

$$\beta=\{g,xg,\cdots,x^{N-r-1}g,u,ux,\cdots,ux^{r-1}\}.$$

（Ⅱ）若 $\min\{k_1,k_2,\cdots,k_j\}=2^e$，即

$$k_1=k_2=\cdots=k_j=2^e,$$

则码 $C=\langle u\rangle$，其极小生成元集为 $\beta=\{u,ux,\cdots,ux^{N-1}\}$.

证明　因为在 $F_2[x]$ 中，

$$x^n-1=f_1f_2\cdots f_j,$$

故在 $R[x]/<x^N-(1+u)>$ 中仍有

$$x^n-1=f_1f_2\cdots f_j,$$

且

$$u=x^N-1=(x^n-1)^{2^e}=f_1^{2^e}f_2^{2^e}\cdots f_j^{2^e},$$

所以 $g\mid(x^N-1)$ 即 $g\mid u$. 又由 $0<\max\{k_1,k_2,\cdots,k_j\}\leqslant 2^e$ 可知，

$$\deg(g) = r \geqslant 1.$$

(Ⅰ) 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

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

则

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

故

$$u \mid (g\sum_{i=0}^{N-r-1} a_i x^i)$$

即

$$\frac{x^N-1}{g} \mid \sum_{i=0}^{N-r-1} a_i x^i.$$

因为

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

所以

$$a_0 = a_1 = \cdots = a_{N-r-1} = 0 \quad (2)$$

故式(1)可化为：

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

又因为 $g \mid u$，所以

$$ug \mid (u\sum_{l=0}^{r-1} D_l x^l),$$

即

$$g \mid \sum_{l=0}^{r-1} D_l x^l.$$

由于 $r-1<\deg(g)=r<N$，于是

$$D_0 = D_1 = \cdots = D_{r-1} = 0 \quad (3)$$

所以式(1)可化为：

$$ug\sum_{i=0}^{N-r-1} b_i x^i + u^2\sum_{l=0}^{r-1} E_l x^l + u^2 g\sum_{i=0}^{N-r-1} c_i x^i = 0.$$

所以

$$u^2 \mid ug\sum_{i=0}^{N-r-1} b_i x^i,$$

即

$$\frac{x^N-1}{g} \mid \sum_{i=0}^{N-r-1} b_i x^i.$$

由于

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

于是

$$b_0 = b_1 = \cdots = b_{N-r-1} = 0 \quad (4)$$

所以式(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

$$g \mid \sum_{l=0}^{r-1} E_l x^l.$$

由于 $r-1<r=\deg(g)<N$，故

$$E_0 = E_1 = \cdots = E_{r-1} = 0 \quad (5)$$

所以式(1)可化为：

$$u^2 g\sum_{i=0}^{N-r-1} c_i x^i = 0 = u^3,$$

因此 $\frac{x^N-1}{g} \mid \sum_{i=0}^{N-r-1} c_i x^i$.

由于

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

故

$$c_0 = c_1 = \cdots = c_{N-r-1} = 0 \quad (6)$$

由式(1)至式(6)可知，$\beta=\{g, xg, \cdots, x^{N-r-1}g, u, ux, \cdots, ux^{r-1}\}$ 可线性组合成 $(2^{N-r})^3\cdot(2^r)^2 = 2^{3N-r}$ 个不同的码字，且组合成的码字皆在码 $C=\langle g\rangle$ 中，又由引理 2.1 可得

$$|C| = 2^{3N-r},$$

故 $\beta=\{g, xg, \cdots, x^{N-r-1}g, u, ux, \cdots, ux^{r-1}\}$ 为码 $C=\langle g\rangle$ 的极小生成元集.

(Ⅱ) 由定理 2.1 可得：

定理 2.3 对于环 R 上长为 $N=2^e n$ 的 $(1+u)$ 常循环码

$$C = \langle f_1^{k_1} f_2^{k_2}\cdots f_j^{k_j}\rangle,$$

当 $2^e < \max\{k_1, k_2, \cdots, k_j\} \leqslant 2^{e+1}$ 时，$\mathrm{rank}(C) = N$，此时：

(Ⅰ) 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 $\deg(g)=r, \deg(f)=s\geqslant 1$.

① 当 $r>s$ 时，码 $C=\langle fg\rangle$，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 $C=\langle g^2\rangle$，其极小生成元集为：

$$\beta=\{g^2,xg^2,\cdots,x^{N-r-1}g^2,u^2,u^2x,\cdots,u^2x^{r-1}\}.$$

（Ⅱ）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 $C=\langle ug\rangle$ 且 $g|(x^N-1)$. 令 $\deg(g)=r\geqslant1$，则该码的极小生成元集为：

$$\beta=\{ug,uxg,\cdots,ux^{N-r-1}g,u^2,u^2x,\cdots,u^2x^{r-1}\}.$$

（Ⅲ）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 $C=\langle u^2\rangle$，其极小生成元集为：

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

证明　（Ⅰ）对于环 R 上长为 $N=2^en$ 的 $(1+u)$ 常循环码

$$C=\langle f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}\rangle,$$

当 $2^e<\max\{k_1,k_2,\cdots,k_j\}\leqslant2^{e+1}$ 且 $\min\{k_1,k_2,\cdots,k_j\}<2^e$ 时，若 $k_1\leqslant2^e$，则将 $f_1^{k_1}$ 作为函数 g 的因子；若 $2^e<k_1\leqslant2^{e+1}$，则将 $f_1^{2^e}$ 作为函数 g 的因子，$f_1^{k_1-2^e}$ 作为函数 f 的因子. 依次分析 $f_1^{k_1}$、$f_2^{k_2}$、…、$f_j^{k_j}$，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. 由 f、g 的取法可知：

$$\frac{x^N-1}{g}=\frac{f_1^{2^e}f_2^{2^e}\cdots f_j^{2^e}}{g}$$

与 f 互素即

$$\left(\frac{x^N-1}{g},f\right)=1.$$

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

$$\sum_{i=0}^{N-r-1}(a_i+ub_i+u^2c_i)x^ifg+\sum_{l=0}^{r-s-1}(a_l'+ub_l')ux^lf+\sum_{m=0}^{s-1}D_mu^2x^m=0,$$

则类似定理 2.2（Ⅰ）可证得

$$a_i=b_i=c_i=a_l'=b_l'=D_m=0;$$
$$i=0,1,\cdots,N-r-1;$$
$$l=0,1\cdots,r-s-1;$$
$$m=0,1,\cdots,s-1,$$

即说明：

$$\beta=\{fg,xfg,\cdots,x^{N-r-1}fg,uf,uxf,\cdots,ux^{r-s-1}f,u^2,u^2x,\cdots,u^2x^{s-1}\}$$

可线性组合成 $(2^{N-r})^3\cdot(2^{r-s})^2\cdot2^s=2^{3N-(r+s)}$ 个不同码字，组合成的码字皆在码 C 中，由引理 2.1 知

$$|C|=2^{3N-(r+s)},$$

故

$$\beta=\{fg,xfg,\cdots,x^{N-r-1}fg,uf,uxf,\cdots,ux^{r-s-1}f,u^2,u^2x,\cdots,u^2x^{s-1}\}$$

为码 $C=\langle fg\rangle$ 的极小生成元集.

② 当 $r=s$ 即 $f=g$ 时，码 $C=\langle g^2\rangle$，类似①可证得其极小生成元集为

$$\beta=\{g^2,xg^2,\cdots,x^{N-r-1}g^2,u^2,u^2x,\cdots,u^2x^{r-1}\}.$$

（Ⅱ）类似定理 2.2（Ⅰ）可证.

（Ⅲ）由定理 2.1 直接可得.

定理 2.4　对于环 R 上长为 $N=2^en$ 的 $(1+u)$ 常循环码

$$C=\langle f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}\rangle,$$

当 $2^{e+1}<\max\{k_1,k_2,\cdots,k_j\}\leqslant2^e\cdot3$ 时：

（Ⅰ）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

$$f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=fgh,$$

$h|f|g|(x^N-1)$，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 $\deg(g)=r,\deg(f)=s,\deg(h)=t\geqslant1$.

① 当 $r>s>t$ 时，码 $C=\langle fgh\rangle$，$\mathrm{rank}(C)=N-t$，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 $C=\langle hg^2\rangle$，$\mathrm{rank}(C)=N-t$，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 $C=\langle f^2g\rangle$，$\mathrm{rank}(C)=N-s$，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 $C=\langle g^3\rangle$，$\mathrm{rank}(C)=N$，其极小生成元集为：

$$\beta=\{g^3,xg^3,\cdots,x^{N-r-1}g^3\}.$$

（Ⅱ）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

$$fg=f_1^{k_1-2^e}f_2^{k_2-2^e}\cdots f_j^{k_j-2^e},$$

$f|g|(x^N-1)$，g 是满足条件的次数最高的多项式，令 $\deg(g)=r,\deg(f)=s\geqslant 1$.

① 当 $r>s$ 时，码 $C=\langle ufg\rangle$，$\mathrm{rank}(C)=N-s$，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 $C=\langle ug^2\rangle$，$\mathrm{rank}(C)=N-r$，其极小生成元集为：

$$\beta=\{ug^2,uxg^2,\cdots,ux^{N-r-1}g^2\}.$$

(Ⅲ) 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 $C=\langle u^2g\rangle$ 且 $g|(x^N-1)$. 令

$$\deg(g)=r\geqslant 1,$$

码 $C=\langle u^2g\rangle$ 的秩 $\mathrm{rank}(C)=N-r$，极小生成元集为：

$$\beta=\{u^2g,u^2xg,\cdots,u^2x^{N-r-1}g\}.$$

(Ⅳ) 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 $C=\langle u^3\rangle=\langle 0\rangle$.

证明 (Ⅰ) 对于环 R 上长为 $N=2^en$ 的 $(1+u)$ 常循环码

$$C=\langle f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}\rangle,$$

当

$$2^{e+1}<\max\{k_1,k_2,\cdots,k_j\}\leqslant 2^e\cdot 3$$

且 $\min\{k_1,k_2,\cdots,k_j\}<2^e$ 时，若 $k_1\leqslant 2^e$，则将 $f_1^{k_1}$ 作为函数 g 的因子；若 $2^e<k_1\leqslant 2^{e+1}$，则将 $f_1^{2^e}$ 作为函数 g 的因子，$f_1^{k_1-2^e}$ 作为函数 f 的因子；若

$$2^{e+1}<k_1\leqslant 2^e\cdot 3,$$

则将 $f_1^{2^e}$ 作为函数 g 和 f 的因子，$f_1^{k_1-2^{e+1}}$ 作为函数 h 的因子. 依次分析 $f_1^{k_1}$、$f_2^{k_2}$、…、$f_j^{k_j}$，则存在 $F_2[x]$ 上的首一多项式 f、g、h 使得

$$f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=fgh,$$

$h|f|g|(x^N-1)$，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 $\deg(g)=r,\deg(f)=s,\deg(h)=t\geqslant 1$. 由 f、g、h 的取法可知

$$\frac{x^N-1}{g}=\frac{f_1^{2^e}f_2^{2^e}\cdots f_j^{2^e}}{g}$$

与 f、h 互素，即，

$$\left(\frac{x^N-1}{g},f\right)=1,\left(\frac{x^N-1}{g},h\right)=1.$$

① 当 $r>s>t$ 时，码 $C=\langle fgh\rangle$，假设存在：

$$a_i,b_i,c_i,a'_l,b'_l,D_m\in F_2;$$
$$i=0,1,\cdots,N-r-1;$$
$$l=0,1,\cdots,r-s-1;$$
$$m=0,1,\cdots,s-t-1;$$

使得

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

则类似定理 2.2(Ⅰ)可证得

$$a_i=b_i=c_i=a'_l=b'_l=D_m=0;$$
$$i=0,1,\cdots,N-r-1;$$
$$l=0,1,\cdots,r-s-1;$$
$$m=0,1,\cdots,s-t-1,$$

即说明

$$\beta=\{hfg,xhfg,\cdots,x^{N-r-1}hfg,uhf,uxhf,\cdots,$$
$$ux^{r-s-1}hf,u^2h,u^2xh,\cdots,u^2x^{s-t-1}h\}$$

可线性组合成 $(2^{N-r})^3(2^{r-s})^2(2^{s-t})$ 个不同码字，且显然组合成的码字皆在码 $C=\langle fgh\rangle$ 中，又由引理 2.1 知 $|C|=2^{3N-(r+s+t)}$，故

$$\beta=\{hfg,xhfg,\cdots,x^{N-r-1}hfg,uhf,uxhf,\cdots,$$
$$ux^{r-s-1}hf,u^2h,u^2xh,\cdots,u^2x^{s-t-1}h\}$$

为码 $C=\langle fgh\rangle$ 的极小生成元集.

②、③、④可类似证明.

(Ⅱ) 类似定理 2.3(Ⅰ)可证得.

(Ⅲ) 类似定理 3.3(Ⅱ)可证得.

(Ⅳ) 显然成立.

3 环上任意长度的 $(1+u)$ 常循环码的 Gray 象

为不引起混淆，下面均将 $R,R^N,R[x]$ 上加法记为“$+$”，将 $F_2,F_2^{4N},F_2[x]$ 上加法记为“$\oplus$”.

对于任意 $a,b\in R$，存在唯一的 $r_i(a),r_i(b)\in F_2(i=0,1,2)$，使得

$$a=r_0(a)+ur_1(a)+u^2r_2(a),$$
$$b=r_0(b)+ur_1(b)+u^2r_2(b)$$

且

$$r_i(a+b)=r_i(a)+r_i(b),i=0,1,2.$$

定义 Gray 映射 $\Phi:R\to F_2^4$ 为：

$$\Phi(a)=(r_2(a),r_2(a)\oplus r_1(a)\oplus r_0(a),$$
$$r_2(a)\oplus r_0(a),r_2(a)\oplus r_1(a)).$$

此时，

$$\Phi(a+b)=$$

$(r_2(a+b), r_2(a+b)\oplus r_1(a+b)\oplus r_0(a+b),$
$r_2(a+b)\oplus r_0(a+b), r_2(a+b)\oplus r_1(a+b)) =$
$\Phi(a)\oplus\Phi(b)$,

故该映射是线性的.

该 Gray 映射 Φ 可以自然地扩展到 R^N 上. 对于任意的 $c=(c_0,c_1,\cdots,c_{N-1})\in R^N$,定义

$r_i(c)=(r_i(c_0),r_i(c_1),\cdots,r_i(c_{N-1})), i=0,1,2,$

称 $\bar{c}=r_0(c)$为 c 的模 u 约化,则 Φ扩展到 R^N 为:

$$\Phi: R^N\to F_2^{4N}$$
$$\Phi(c)=(r_2(c), r_2(c)\oplus r_1(c)\oplus r_0(c),$$
$$r_2(c)\oplus r_0(c), r_2(c)\oplus r_1(c)).$$

由扩展映射 Φ的定义可知,该映射是 R^N 到 F_2^{4N} 的双射. 对于任意 $c(x)=c_0+c_1x+c_2x^2+\cdots+c_{N-1}x^{N-1}\in R[x]$,记

$$p_i(x)=\sum_{m=0}^{N-1} r_i(c_m)x^m, i=0,1,2,$$

称$\overline{c(x)}=p_0(x)$为 $c(x)$的模 u 约化,则

$\Phi(c(x))=$
$p_2(x)\oplus x^N[p_2(x)\oplus p_1(x)\oplus p_0(x)]\oplus$
$x^{2N}[p_2(x)\oplus p_0(x)]\oplus x^{3N}[p_2(x)\oplus p_1(x)]$

为 $R[x]$到 $F_2[x]$的多项式 Gray 映射.

R 中元素的 Lee 重量分别定义为 u^2 为 4;1, u, $1+u$, $1+u^2$, $u+u^2$, $1+u+u^2$ 为 2;0 为 0. R^N 中码字的 Lee 重量为其码元的 Lee 重量之和,两个码字 c,c'的 Lee 距离为$(c-c')$的 Lee 重量. 由上述 Gray 映射的定义及 R 中元素的 Lee 重量的定义得如下引理:

引理 3.1　Gray 映射 Φ是保线性和保距离(从 R^N 上的 Lee 距离到 F_2^{4N} 上的 Hamming 距离)的双射.

引理 3.2　设 ν是 R^N 上的$(1+u)$循环移位且 σ是 F_2^{4N} 上的循环移位. 设 Φ是 R^N 到 F_2^{4N} 的 Gray 映射,则 $\Phi\nu=\sigma\Phi$.

证明　设 $c=(c_0,c_1,\cdots,c_{N-1})\in R^N$,

$$c_i=r_0(c_i)+ur_1(c_i)+u^2r_2(c_i).$$

其中 $i=0,1,\cdots,N-1$, $r_0(c_i), r_1(c_i), r_2(c_i)\in F_2$,由 Gray 映射的定义有

$\Phi(c)=(r_2(c_0), r_2(c_1),\cdots, r_2(c_{N-1}),$
$r_2(c_0)\oplus r_1(c_0)\oplus r_0(c_0),$
$r_2(c_1)\oplus r_1(c_1)\oplus r_0(c_1),\cdots,$
$r_2(c_{N-1})\oplus r_1(c_{N-1})\oplus r_0(c_{N-1}),$
$r_2(c_0)\oplus r_0(c_0), r_2(c_1)\oplus r_1(c_1),\cdots,$
$r_2(c_{N-1})\oplus r_0(c_{N-1}), r_2(c_0)\oplus r_1(c_0),$
$r_2(c_1)\oplus r_2(c_1),\cdots, r_2(c_{N-1})\oplus r_1(c_{N-1})),$

故

$\sigma\Phi(c)=(r_2(c_{N-1})\oplus r_1(c_{N-1}), r_2(c_0), r_2(c_1),\cdots,$
$r_2(c_{N-1}), r_2(c_0)\oplus r_1(c_0)\oplus r_0(c_0),$
$r_2(c_1)\oplus r_1(c_1)\oplus r_0(c_1),\cdots,$
$r_2(c_{N-1})\oplus r_1(c_{N-1})\oplus r_0(c_{N-1}),$
$r_2(c_0)\oplus r_0(c_0), r_2(c_1)\oplus r_0(c_1),\cdots,$
$r_2(c_{N-1})\oplus r_0(c_{N-1}), r_2(c_0)\oplus r_1(c_0),$
$r_2(c_1)\oplus r_1(c_1),\cdots,$
$r_2(c_{N-2})\oplus r_1(c_{N-2})).$

另一方面,

$$\nu(c)=((1+u)c_{N-1}, c_0, c_1,\cdots, c_{N-2}),$$

所以

$\Phi\nu(c)=(r_2((1+u)c_{N-1}), r_2(c_0), r_2(c_1),\cdots, r_2(c_{N-2}),$
$r_2((1+u)c_{N-1})\oplus r_1((1+u)c_{N-1})\oplus r_0((1+u)c_{N-1}),$
$r_2(c_0)\oplus r_1(c_0)\oplus r_0(c_0),$
$r_2(c_1)\oplus r_1(c_1)\oplus r_0(c_1),\cdots,$
$r_2(c_{N-2})\oplus r_1(c_{N-2})\oplus r_0(c_{N-2}),$
$r_2((1+u)c_{N-1})\oplus r_0((1+u)c_{N-1}),$
$r_2(c_0)\oplus r_0(c_0), r_2(c_1)\oplus r_0(c_1),\cdots,$
$r_2(c_{N-2})\oplus r_0(c_{N-2}),$
$r_2((1+u)c_{N-1})\oplus r_1((1+u)c_{N-1}),$
$r_2(c_0)\oplus r_1(c_0), r_2(c_1)\oplus r_2(c_1),\cdots,$
$r_2(c_{N-2})\oplus r_1(c_{N-2})).$

又因为

$(1+u)c_{N-1}=$
$(1+u)[r_0(c_{N-1})+ur_1(c_{N-1})+u^2r_2(c_{N-1})]=$
$r_0(c_{N-1})+[r_1(c_{N-1})+r_0(c_{N-1})]u+$
$[r_2(c_{N-1})+r_1(c_{N-1})]u^2,$

即有

$$r_2((1+u)c_{N-1})=r_2(c_{N-1})\oplus r_1(c_{N-1}),$$
$$r_1((1+u)c_{N-1})=r_1(c_{N-1})\oplus r_0(c_{N-1}),$$
$$r_0((1+u)c_{N-1})=r_0(c_{N-1}),$$

所以 $\Phi\nu=\sigma\Phi$.

由引理 3.1、引理 3.2 易得如下定理:

定理 3.1　R 上长为 N 的线性码 C 是$(1+u)$常循环码当且仅当 $\Phi(C)$是 F_2 上长为 $4N$ 的循环码.

推论 3.2　R 上长为 N 的$(1+u)$常循环码在 Gray 映射下的象是 F_2 上长为 $4N$ 的距离不变的线性循环码.

定理 3.3 设 C 是环 R 上长为 $N=2^e n$ 的 $(1+u)$ 常循环码 $C=\langle f_1^{k_1} f_2^{k_2} \cdots f_j^{k_j} \rangle$. 其中，$0 \leqslant k_i \leqslant 2^e \cdot 3$；$i=1,2,\cdots,j$；$n$ 为奇数；$f_1(x)$、$f_2(x)$、$\cdots$、$f_j(x)$ 为 $F_2[x]$ 上两两互素的首一不可约多项式且 $x^n-1=f_1(x) f_2(x) \cdots f_j(x)$，则其 Gray 象 $\Phi(C)$ 是 F_2 上长为 $4N$ 的线性循环码，且有

$$\Phi(C)=\langle f_1^{k_1+2^e} f_2^{k_2+2^e} \cdots f_j^{k_j+2^e} \rangle.$$

证明 由推论 3.2 可知，$\Phi(C)$ 是 F_2 上长为 $4N$ 的线性循环码. 下面证明

$$\Phi(C)=\langle f_1^{k_1+2^e} f_2^{k_2+2^e} \cdots f_j^{k_j+2^e} \rangle.$$

事实上，在 $R[x]/\langle x^N-(1+u)\rangle$ 中 $u=1+x^N$，$u^2=1+x^{2N}$. 取该 $(1+u)$ 常循环码 $C=\langle f_1^{k_1} f_2^{k_2} \cdots f_j^{k_j} \rangle$ 中一码字 $\tilde{c}(x)=f_1^{k_1} f_2^{k_2} \cdots f_j^{k_j}$，因 $0 \leqslant k_i \leqslant 2^e \cdot 3$，$i=1,2,\cdots,j$，故必存在 $F_2(x)$ 上次数皆小于 N 的首一多项式 $p_0(x)$，$p_1(x)$，$p_2(x)$ 使得

$$\tilde{c}(x)=$$
$$p_0(x)+p_1(x)+p_2(x)+x^N p_1(x)+x^{2N} p_2(x)=$$
$$p_0(x)+(1+x^N) p_1(x)+(1+x^{2N}) p_2(x)=$$
$$p_0(x)+u p_1(x)+u^2 p_2(x),$$

所以 $(1+u+u^2)\tilde{c}(x)=p_0(x)+u[p_1(x)+p_0(x)]+u^2[p_2(x)+p_1(x)+p_0(x)] \in C$，由多项式 Gray 映射可得在 $F_2[x]/\langle x^{4N}-1\rangle$ 中.

$$\begin{aligned}
&\Phi[(1+u+u^2)\tilde{c}(x)]=\\
&\quad p_2(x) \oplus p_1(x) \oplus p_0(x) \oplus\\
&\quad x^N[p_2(x) \oplus p_0(x)] \oplus\\
&\quad x^{2N}[p_2(x) \oplus p_1(x)] \oplus x^{3N} p_2(x)=\\
&\quad (1 \oplus x^N) p_0(x) \oplus (1 \oplus x^{2N}) p_1(x) \oplus\\
&\quad (1 \oplus x^N \oplus x^{2N} \oplus x^{3N}) p_2(x)=\\
&\quad (1 \oplus x^N)[p_0(x) \oplus (1 \oplus x^N) p_1(x) \oplus\\
&\quad (1 \oplus x^{2N}) p_2(x)]=\\
&\quad (1 \oplus x^N)\tilde{c}(x) \in \Phi(C)
\end{aligned}$$

故

$$\Phi(C) \subseteq \langle (1 \oplus x^N)\tilde{c}(x) \rangle = \langle f_1^{k_1+2^e} f_2^{k_2+2^e} \cdots f_j^{k_j+2^e} \rangle.$$

比较码字的个数可得

$$\Phi(C)=\langle f_1^{k_1+2^e} f_2^{k_2+2^e} \cdots f_j^{k_j+2^e} \rangle.$$

4 例题

例 1 在 $F_2[x]$ 中，$x^3-1=f_1 f_2$. 其中，$f_1=x+1$，$f_2=x^2+x+1$，由引理 2.1 可知，环 $F_2+uF_2+u^2 F_2$ 上长为 $N=2^e \cdot 3$ 的所有 $(1+u)$ 常循环码为 $C=\langle f_1^{k_1} f_2^{k_2} \rangle$. 其中，$0 \leqslant k_j \leqslant 2^e \cdot 3$，$j=1,2$，由定理 3.3 可得表 1 所示的二元最优码.

表 1 基于 (x^3-1) 在 $F_2[x]$ 上分解得到的二元最优码

Tab. 1 Binary optimal codes obtained from the fractorization of (x^3-1) in $F_2[x]$

码 C 的长	码 C 的生成多项式	Gray 象的生成多项式	Gray 象
3	1	$f_1 f_2$	[12,9,2]
3	f_1^2	$f_1^3 f_2$	[12,7,4]
3	f_1^3	$f_1^4 f_2$	[12,6,4]
3	f_2^2	$f_1 f_2^3$	[12,5,4]
3	f_2^3	$f_1 f_2^4$	[12,3,6]
3	$f_1^2 f_2$	$f_1^3 f_2^2$	[12,5,4]
3	$f_1^2 f_2^2$	$f_1^3 f_2^3$	[12,1,12]
3	$f_1^3 f_2^2$	$f_1^4 f_2^3$	[12,2,8]
6	f_1^3	$f_1^3 f_2^2$	[24,15,4]

例 2 在 $F_2[x]$ 中，$x^7-1=f_1 f_2 f_3$. 其中，$f_1=x+1$，$f_2=x^3+x+1$，$f_3=x^3+x^2+1$，由引理 2.1 可知，环 $F_2+uF_2+u^2 F_2$ 上长为 $N=2^e \cdot 7$ 的所有 $(1+u)$ 常循环码为 $C=\langle f_1^{k_1} f_2^{k_2} f_3^{k_3} \rangle$. 其中，$0 \leqslant k_j \leqslant 2^e \cdot 3$，$j=1,2$，由定理 3.3 可得表 2 所示的二元最优码.

表 2 基于 (x^7-1) 在 $F_2[x]$ 上分解得到的二元最优码

Tab. 2 Binary optimal codes obtained from the fractorization of (x^7-1) in $F_2[x]$

码 C 的长	码 C 的生成多项式	Gray 象的生成多项式	Gray 象
7	$f_1^3 f_3^2$	$f_1^4 f_2 f_3^3$	[28,12,8]
7	$f_1^3 f_2^2$	$f_1^4 f_2^2 f_3$	[28,12,8]
7	$f_2^3 f_3^2$	$f_1 f_2^4 f_3^3$	[28,6,12]
7	$f_2^2 f_3^3$	$f_1 f_2^3 f_3^4$	[28,6,12]

5 结论

本文基于 (x^n-1) 在 $F_2[x]$ 上的分解，探讨了环 R 上任意长度的 $(1+u)$ 常循环码的秩和极小生成元集，定义了环 R 到 F_2^4 的一个新的 Gray 映射，证明了环 R 上该常循环码在 Gray 映射下的象是 F_2 上的长为 $4N$ 的循环码且确定了 Gray 象的生成多项式，得到了一些最优的二元线性循环码. 相对于文献[7]，本文可以通过更短的 $(1+u)$ 常循环码构造了一些二元最优码，对于更一般的多项式剩余类环上常循环码的情况值得进一步研究.

参考文献(References)

[1] Roger H A, Vijay K P, Calderbank A R, et al. The linearity of Kerdock, Preparata, Goethals, and related

codes[J]. IEEE Transactions on Information Theory, 1994, 40 (2): 301-319.

[2] Dougherty S T, Shiromoto K. Maximum distance codes over rings of order 4[J]. IEEE Transactions on Information Theory, 2001, 47(1): 400-404.

[3] Qian J F, Zhang L N, Zhu S X. $(1+u)$ -constacyclic and cyclic codes over F_2+uF_2 [J]. Applied Mathematics Letters, 2006, 19(8): 820-823.

[4] Qian J F, Zhang L N. Constacyclic and cyclic codes over $F_2+uF_2+u^2F_2$ [J]. IEICE Transactions on Fundamentals, Communications and Computer Science, 2006, E89-A(6): 1 863-1 865.

[5] Zhu S X, Shi M J. The ranks of cyclic and negacyclic codes over the finite ring R[J]. Journal of Electronics (China), 2008, 25(1): 97-101.

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

[7] Shi M J, Zhu S X. Constacyclic codes over ring $F_q+uF_q+\cdots+u^{k-1}F_q$[J]. Journal of University of Science and Technology of China, 2009, 39(6): 583-587.
施敏加, 朱士信. 环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上的常循环码[J]. 中国科学技术大学学报, 2009, 39(6): 583-587.

[8] Qian J F. Cyclic codes over finite rings [C]// Proceedings of 7th International Conference on Wireless Communications, Networking and Mobile Computing. Wuhan, China: IEEE Press, 2011:1-4.

[9] Kai X S, Zhu S X, Li P. $(1+\lambda u)$ -constacyclic codes over[J]. Journal of Franklin Institute, 2010, 347(5): 751-762.

[10] Ding J, Li H J, Li H X. 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, 43(2): 334-339.
丁健, 李红菊, 李海霞. 关于环 $F_{p^m}+uF_{p^m}$ 上常循环码的等价性[J]. 中国科学技术大学学报, 2013, 43(2): 334-339.

[11] Wang L Q, Zhu S X. A class of constacyclic codes over and its Gray image [J]. Journal of electronics and information technology, 2013, 35(2): 499-503.
王立启, 朱士信. 环上的一类常循环码及其 Gray 象[J]. 电子与信息学报, 2013, 35(2): 499-503.

[12] Hu Q, Li P. 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.
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.

[13] Liu J Q, Liu L, Kai X S. $(1+u^k)$-cyclic codes over the ring $F_2+uF_2+\cdots u^kF_2$[J]. Journal of Hefei university of technology, 2013, 36(1): 124-128.
刘金秋, 刘丽, 开晓山. 环 $F_2+uF_2+\cdots u^kF_2$ 上的 $(1+u^k)$常循环码[J]. 合肥工业大学学报(自然科学版), 2013, 36(1): 124-128.

[14] Zhang X Y. The Gray images of the liner codes and their dual codes over $F_{2^m}+uF_{2^m}+u^2F_{2^m}+u^3F_{2^m}$[J]. Journal of Mathematics, 2013, 33(4): 661-664.
张晓燕. 环 $F_{2^m}+uF_{2^m}+u^2F_{2^m}+u^3F_{2^m}$ 上的线性码及其对偶码的 Gray 象[J]. 数学杂志, 2013, 33(4): 661-664.

[15] Li S S, Li P. Cyclic codes over the ring Z_4+uZ_4[J]. Journal of Hefei university of technology, 2013, 36(8): 1 006-1 009.
李珊珊,李平. 环 Z_4+uZ_4 上的循环码[J]. 合肥工业大学学报, 2013, 36(8): 1 006-1 009.

[16] Liang H, Tang Y S. The gray images of cyclic codes over $\frac{Z_p[u]}{(u^{k+1})}$[J]. Mathematics in Practice and Theory, 2013, 43(5): 200-203.
梁华, 唐元生. 环 $\frac{Z_p[u]}{(u^{k+1})}$ 上循环码的 Gray 象[J]. 数学的实践与认识, 2013, 43(5): 200-203.