环 $F_2[u]/(u^4)$ 上的一类常循环码及其 Gray 象

王立启* 朱士信
(合肥工业大学数学学院 合肥 230009)

摘 要：该文定义了环 $R=F_2+uF_2+u^2F_2+u^3F_2$ 到 F_2^4 的一个新的 Gray 映射，其中 $u^4=0$。证明了 R 上长为 n 的 $(1+u+u^2+u^3)$-循环码的 Gray 象是 F_2 上长为 $4n$ 的距离不变的线性循环码。进一步确定了 R 上奇长度的该常循环码的 Gray 象的生成多项式，并得到了一些最优的二元线性循环码。

关键词：循环码；常循环码；生成多项式
中图分类号：TN911.22 **文献标识码**： A **文章编号**：1009-5896(2013)02-0499-05
DOI: 10.3724/SP.J.1146.2012.00869

A Class of Constacyclic Codes Over $F_2[u]/(u^4)$ and Its Gray Image

Wang Li-qi Zhu Shi-xin
(*School of Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: A new Gray map is defined from $R=F_2+uF_2+u^2F_2+u^3F_2$ to F_2^4 with $u^4=0$. It is proved that the Gray image of a linear $(1+u+u^2+u^3)$-cyclic code of length n over R is a distance-invariant linear cyclic code of length $4n$ over F_2. Further more, the generator polynomials of the Gray image of this constacyclic code for odd length over R is determined, some optimal binary linear cyclic codes are also obtained.

Key words: Cyclic codes; Constacyclic codes; Generator polynomial

1 引言

1994年，文献[1]证明了某些高效的二元非线性码可以看作 Z_4-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。自此，开辟了有限环上纠错码理论研究的新天地，使其成为纠错码理论研究的一个新热点。Gray 映射作为连接环上码和域上码的桥梁，被众多学者加以研究[2−10]。Wolfmann 在文献[2]中研究了 Z_4 上负循环码 Gray 映射性质。文献[3]通过引入 $Z_{2^{k+1}}$ 到 Z_4 的保距映射，证明了 $(1+2^k)$-循环码的 Gray 象是二元距离不变的准循环码。随后，文献[4]将其推广到环 $Z_{p^{k+1}}$。多项式剩余类环的结构介于有限域和环之间，因其具有良好的性质，其上的纠错码理论研究也倍受关注。文献[5]中首次研究了 F_2+uF_2 上常循环码的 Gray 象性质。文献[6]将其推广到环 $F_{p^k}+uF_{p^k}$。文献[7]研究了 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上 $(u\lambda-1)$-循环码的 Gray 象性质。随后，文献[8]研究了 $F_q+uF_q+\cdots+u^tF_q$ 上 $(1-u^t)$-循环码的 Gray 象。最近文献[11]研究了 $F_2[u]/(u^4-1)$ 上的循环码并由此构造了 DNA 码，文献[12]研究了 $F_{2^m}+uF_{2^m}+\cdots+u^{a-1}F_{2^m}$ 上形如 $(\alpha_0+u\alpha_1+\cdots+u^{a-1}\alpha_{a-1})$-循环码的结构。本文研究了 $F_2+uF_2+u^2F_2+u^3F_2$ 上 $(1+u+u^2+u^3)$-循环码的 Gray 象，并给出了奇长度该常循环码的 Gray 象生成多项式。在下文中记 $\xi=1+u+u^2+u^3$。

2012-07-09 收到，2012-10-16 改回
国家自然科学基金(60973125)资助课题
*通信作者：王立启 liqiwangg@163.com

2 基础知识

设 R 是有限交换环 $F_2+uF_2+u^2F_2+u^3F_2=F_2[u]/(u^4)$，其中 $u^4=0$。该环为有限链环，它的所有理想可表示为 $\{0\}=u^4R\subset u^3R\subset u^2R\subset uR\subset R$。有限环 R 上长为 n 的码是 R^n 的一个非空子集，若它是 R^n 的 R-子模，则称其为线性码。若对任意码字 $\underline{c}=(c_0,c_1,\cdots,c_{n-1})\in C$，仍然有其 λ-循环移位 $v(\underline{c})=(\lambda c_{n-1},c_0,\cdots,c_{n-2})\in C$，其中 λ 为 R 中的单位，则称 C 为 λ-循环码。若 $\lambda=1$，则称其为循环码，并将该循环移位记为 σ。每个码字 $\underline{c}=(c_0,c_1,\cdots,c_{n-1})\in C$ 对应 $R[x]/(x^n+\lambda)$ 中的多项式 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，此多项式称为 $\underline{c}$ 的码字多项式。这样可以将 R 上长为 n 的 λ-循环码看作多项式剩余类环 $R[x]/(x^n+\lambda)$ 的理想。码字 $\underline{c}$ 的 Hamming 重量 $W_H(\underline{c})$ 定义为其非零码元的个数，两个码字 $\underline{c},\underline{c}'$ 的 Hamming 距离为 $\underline{c}-\underline{c}'$ 的 Hamming 重量。

下面的命题证明与有限域上循环码的相应结论类似，证明省略。

命题 1 (1) R^n 的子集 S 是长度为 n 的线性循环码当且仅当其多项式表示是 $R[x]/(x^n+1)$ 的一个理想。(2) R^n 的子集 S 是长度为 n 的线性 ξ-循环码

当且仅当其多项式表示是 $R[x]/(x^n+\xi)$ 的一个理想。

3 R 上的 Gray 映射及其性质

对于每一个元素 $c\in R$ 可以唯一地表示为 $c=\beta_0(c)+u\beta_1(c)+u^2\beta_2(c)+u^3\beta_3(c)$，其中 $\beta_i(c)\in F_2$。定义 Gray 映射 $\Phi: R\to F_2^4$ 为 $\Phi(c)=(\beta_3(c),\beta_3(c)+\beta_2(c),\beta_3(c)+\beta_1(c),\beta_3(c)+\beta_2(c)+\beta_1(c)+\beta_0(c))$。显然该映射为线性的。

该 Gray 映射 Φ 可以自然地扩展到 R^n 上。对任意的 $\underline{c}=(c_0,c_1,\cdots,c_{n-1})\in R^n$，定义 $\beta_i(\underline{c})=(\beta_i(c_0),\beta_i(c_1),\cdots,\beta_i(c_{n-1}))$，$0\le i\le 3$。则 Φ 扩展到 R^n 如下：

$$\Phi: R^n\to F_2^{4n},$$

$$\begin{aligned}\Phi(\underline{c})=(&\beta_3(\underline{c}),\beta_3(\underline{c})+\beta_2(\underline{c}),\beta_3(\underline{c})\\&+\beta_1(\underline{c}),\beta_3(\underline{c})+\beta_2(\underline{c})+\beta_1(\underline{c})+\beta_0(\underline{c}))\end{aligned}$$

显然扩展映射 Φ 是 R^n 到 F_2^{4n} 的双射。其中 R 中元素的 Lee 重量分别定义为 u^3 为 4; $1+u+u^2$, $1+u^3$,$1+u+u^3$,$1+u^2+u^3$ 为 3; $u,u^2,u+u^2$, $u+u^3$, u^2+u^3,$u+u^2+u^3$ 为 2;1,$1+u$,$1+u^2$,$1+u+u^2+u^3$ 为 1。R^n 中码字的 Lee 重量为其码元的 Lee 重量之和，两个码字 $\underline{c},\underline{c}'$ 的 Lee 距离为 $\underline{c}-\underline{c}'$ 的 Lee 重量。由 Gray 映射的定义我们可以得到其下面的性质。

命题 2 Gray 映射 Φ 是(R^n, Lee 距离)到(F_2^{4n}, Hamming 距离)的保距映射。

下面我们研究奇数长度的 ξ-循环码的一些性质。

假设 n 为奇数，k 是一个正整数。若 $n=4k-1$，我们设 $\alpha=\xi$。若 $n=4k+1$，则设 $\alpha=1+u$。注意到 $\alpha^n=1+u$ 且 $(1+u)\cdot\xi=1$。

设 μ 是如下映射

$$\mu: R[x]/(x^n+1)\to R[x]/(x^n+\xi),\ \ \mu(c(x))=c(\alpha x)$$

命题 3 设 α 如上，则 μ 是 $R[x]/(x^n+1)$ 到 $R[x]/(x^n+\xi)$ 的环同构映射。

由此我们可以立即得到下面的推论。

推论 1 设 I 是 $R[x]/(x^n+1)$ 的子集，J 是 $R[x]/(x^n+\xi)$ 的子集，n 为奇数，并满足 $J=\mu(I)$，则 I 是 $R[x]/(x^n+1)$ 的理想当且仅当 J 是 $R[x]/(x^n+\xi)$ 的理想。

推论 2 设 n 为奇数，$\tilde{\mu}$ 是 R^n 上的一个置换，即 $\tilde{\mu}(c_0,c_1,\cdots,c_{n-1})=(c_0,\alpha c_1,\cdots,\alpha^i c_i,\cdots,\alpha^{n-1}c_{n-1})$。设 D 是 R^n 的一个子集，则 D 是线性循环码当且仅当 $\tilde{\mu}(D)$ 为线性 ξ-循环码。

命题 4 设 v 是 R^n 上的 ξ-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 $\Phi v=\sigma\Phi$。

证明 设 $\underline{c}=(c_0,c_1,\cdots,c_{n-1})\in R^n$, $c_i=\beta_0(c_i)+u\beta_1(c_i)+u^2\beta_2(c_i)+u^3\beta_3(c_i)$，其中 $\beta_j(c_i)\in F_2$，$0\le i\le n-1, 0\le j\le 3$。由 Gray 映射的定义有

$$\begin{aligned}\Phi(\underline{c})=(&\beta_3(c_0),\beta_3(c_1),\cdots,\beta_3(c_{n-1}),\beta_3(c_0)+\beta_2(c_0),\cdots,\\&\beta_3(c_{n-1})+\beta_2(c_{n-1}),\beta_3(c_0)+\beta_1(c_0),\cdots,\\&\beta_3(c_{n-1})+\beta_1(c_{n-1}),\beta_3(c_0)+\beta_2(c_0)+\beta_1(c_0)\\&+\beta_0(c_0),\cdots,\beta_3(c_{n-1})+\beta_2(c_{n-1})+\beta_1(c_{n-1})\\&+\beta_0(c_{n-1}))\end{aligned}$$

从而

$$\begin{aligned}\sigma\Phi(\underline{c})=(&\beta_3(c_{n-1})+\beta_2(c_{n-1})+\beta_1(c_{n-1})+\beta_0(c_{n-1}),\\&\beta_3(c_0),\beta_3(c_1),\cdots,\beta_3(c_{n-1}),\beta_3(c_0)+\beta_2(c_0),\cdots,\\&\beta_3(c_{n-1})+\beta_2(c_{n-1}),\beta_3(c_0)+\beta_1(c_0),\cdots,\\&\beta_3(c_{n-1})+\beta_1(c_{n-1}),\beta_3(c_0)+\beta_2(c_0)+\beta_1(c_0)\\&+\beta_0(c_0),\cdots,\beta_3(c_{n-2})+\beta_2(c_{n-2})+\beta_1(c_{n-2})\\&+\beta_0(c_{n-2}))\end{aligned}$$

另一方面，$v(\underline{c})=(\xi c_{n-1},c_0,\cdots,c_{n-2})$，从而根据 Gray 映射的定义有

$$\begin{aligned}\Phi(v(\underline{c}))=(&\beta_3(c_{n-1})+\beta_2(c_{n-1})+\beta_1(c_{n-1})+\beta_0(c_{n-1}),\\&\beta_3(c_0),\beta_3(c_1),\cdots,\beta_3(c_{n-1}),\beta_3(c_0)+\beta_2(c_0),\\&\cdots,\beta_3(c_{n-1})+\beta_2(c_{n-1}),\beta_3(c_0)+\beta_1(c_0),\cdots,\\&\beta_3(c_{n-1})+\beta_1(c_{n-1}),\beta_3(c_0)+\beta_2(c_0)+\beta_1(c_0)\\&+\beta_0(c_0),\cdots,\beta_3(c_{n-2})+\beta_2(c_{n-2})+\beta_1(c_{n-2})\\&+\beta_0(c_{n-2}))\end{aligned}$$

因此，$\Phi v=\sigma\Phi$。

定理 1 R 上长为 n 的线性码 C 是 ξ-循环码当且仅当 $\Phi(C)$ 是 F_2 上长为 $4n$ 的循环码。

证明 若 C 是 R 上长为 n 的 ξ-循环码，由命题 4，我们有 $\sigma(\Phi(C))=\Phi(v(C))=\Phi(C)$。因此，$\Phi(C)$ 是 F_2 上长为 $4n$ 的循环码。反之，若 $\Phi(C)$ 是 F_2 上长为 $4n$ 的循环码，由命题 4，可得 $\Phi(v(C))=\sigma(\Phi(C))=\Phi(C)$。注意到 Φ 是单射，故有 $v(C)=C$。

我们立即可以得到下面的推论：

推论 3 R 上长为 n 的 ξ-循环码在 Gray 映射 Φ 下的象是 F_2 上长为 $4n$ 的距离不变的线性循环码。

下面我们介绍 F_2^{4n} 上一个特殊的置换。

对于奇数 $n=4k-1,4k+1$，设 S 是集合

$$\begin{matrix}\{0 & n & 2n & 3n\\ 1 & n+1 & 2n+1 & 3n+1\\ 2 & n+2 & 2n+2 & 3n+2\\ \vdots & \vdots & \vdots & \vdots\\ n-1 & 2n-1 & 3n-1 & 4n-1\}\end{matrix}$$

注意到这是一个 n 行 4 列的数组。我们定义置换 φ 如下：

若 $n=4k+1$，置换 φ 在行 $4j+2,4j+3,4j$

$+4(j=0,1,\cdots,k-1)$ 上分别为 1,2,3-循环移位。

若 $n=4k-1$，置换 φ 在行 $4j+2,4j+3,4j+4(j=0,1,\cdots,k-1)$ 上分别为 3,2,1-循环移位。其中 i-循环移位是对行 $(s,n+s,2n+s,3n+s)$ 作 i-循环移位。

由该置换可以得到 F_2^{4n} 上向量的一个置换 π，即若 $\underline{c}=(c_0,c_1,\cdots,c_{4n-1})$，我们有 $\pi(\underline{c})=(c_{\varphi(0)},c_{\varphi(1)},\cdots,c_{\varphi(4n-1)})$。

命题 5　假设 n 为奇数，$\alpha,\mu,\tilde{\mu}$ 的定义如上，则有 $\Phi\tilde{\mu}=\pi\Phi$。

证明　设 $\underline{c}=(c_0,c_1,\cdots,c_{n-1})\in R^n$，且 $\Phi(\underline{c})=(s_0,s_1,\cdots,s_{n-1},s_n,\cdots,s_{4n-1})$。由 $\tilde{\mu}(c_0,c_1,\cdots,c_{n-1})=(c_0,\alpha c_1,\cdots,\alpha^i c_i,\cdots,\alpha^{n-1}c_{n-1})$，我们记 $\Phi(\tilde{\mu}(\underline{c}))=(t_0,t_1,\cdots,t_{n-1},t_n,\cdots,t_{4n-1})$。

若 $n=4k+1$，易知对于 $0\le j\le k-1$，我们有

$$\begin{aligned}t_{4j+1}&=s_{3n+4j+1},t_{n+4j+1}=s_{4j+1},t_{2n+4j+1}\\&=s_{n+4j+1},t_{3n+4j+1}=s_{2n+4j+1}\\t_{4j+2}&=s_{2n+4j+2},t_{n+4j+2}=s_{3n+4j+2},t_{2n+4j+2}\\&=s_{4j+2},t_{3n+4j+2}=s_{n+4j+2}\\t_{4j+3}&=s_{n+4j+3},t_{n+4j+3}=s_{2n+4j+3},t_{2n+4j+3}\\&=s_{3n+4j+3},t_{3n+4j+3}=s_{4j+3}\end{aligned}$$

若 $n=4k-1$，易知对于 $0\le j\le k-1$，我们有

$$\begin{aligned}t_{4j+1}&=s_{n+4j+1},t_{n+4j+1}=s_{2n+4j+1},t_{2n+4j+1}\\&=s_{3n+4j+1},t_{3n+4j+1}=s_{4j+1};\\t_{4j+2}&=s_{2n+4j+2},t_{n+4j+2}=s_{3n+4j+2},t_{2n+4j+2}\\&=s_{4j+2},t_{3n+4j+2}=s_{n+4j+2};\\t_{4j+3}&=s_{3n+4j+3},t_{n+4j+3}=s_{4j+3},t_{2n+4j+3}\\&=s_{n+4j+3},t_{3n+4j+3}=s_{2n+4j+3}.\end{aligned}$$

因此 $\Phi\tilde{\mu}=\pi\Phi$。

推论 4　设 π 为定义的如上置换，若 n 为奇数，Γ 是 R 上线性循环码的 Gray 象，则 $\pi(\Gamma)$ 为循环码。

证明　设 $\Gamma=\Phi(D)$，其中 D 为 R 上的线性循环码，由命题 5 知 $(\Phi\tilde{\mu})(D)=(\pi\Phi)(D)=\pi(\Gamma)$。由推论 2 知 $\tilde{\mu}(D)$ 是线性 ξ-循环码 C，从而 $(\Phi\tilde{\mu})(D)=\Phi(C)$，又由定理 2 知 $\Phi(C)$ 为二元线性循环码，从而得证。

下面回顾一下码等价的定义：设 Γ 和 Δ 分别为 F_2 上长为 n 的码，ω 是关于 $\{0,1,\cdots,n-1\}$ 的置换，若 $\Delta=\varpi(\Gamma)$，则称 Γ 和 Δ 等价，其中 $\varpi(c_0,c_1,\cdots,c_{n-1})=(c_{\omega(0)},c_{\omega(1)},\cdots,c_{\omega(n-1)})$。

由前面的结果立即可以得到下面的推论：

推论 5　R 上奇数长度的线性循环码的 Gray 象等价于一个线性循环码。

4　R 上 ξ-循环码 Gray 象的结构

文献[13]给出了环 $F_p+uF_p+\cdots+u^{k-1}F_p$ 上循环码的结构，类似地我们有如下定理。

定理 2　设 C 是 R 上长为 n 的循环码，则存在唯一的两两互素的首一多项式 f,g,h,k,l，使得 $C=(fhkl,\ ufgkl,u^2fghl,u^3fghk)$，其中 $x^n+1=fghkl$ 且 $|C|=2^{4\deg(g)+3\deg(h)+2\deg(k)+\deg(l)}$。

由上面的同构映射 μ，可得：

定理 3　若 C 是 R 上长为 n 的 ξ-循环码，则存在唯一的两两互素的首一多项式 $f_i,0\le i\le 4$，使得 $C=(\hat{f}_1,u\hat{f}_2,u^2\hat{f}_3,u^3\hat{f}_4)$，其中 $x^n+\xi=\prod_{i=0}^4 f_i,\hat{f}_i=(x^n+\xi)/f_i$ 且 $|C|=2^{4\deg(f_1)+3\deg(f_2)+2\deg(f_3)+\deg(f_4)}$。

由上面的 Gray 映射的定义，对任意的 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in R[x]$，记 $g_i(x)=\sum_{j=0}^{n-1}\beta_i(c_j)x^j$，$0\le i\le 3$。则

$$\begin{aligned}\Phi_P(c(x))&=g_3(x)+x^n(g_3(x)+g_2(x))+x^{2n}(g_3(x)\\&\quad+g_1(x))+x^{3n}(g_3(x)+g_2(x)+g_1(x)+g_0(x))\end{aligned}$$

是 $R[x]$ 到 $F_2[x]$ 的多项式 Gray 映射，我们仍将其记为 Φ。

对于任意的 $\underline{c}=(c_0,c_1,\cdots,c_{n-1})\in R^n$，记 $\beta_i(\underline{c})=(\beta_i(c_0),\beta_i(c_1),\cdots,\beta_i(c_{n-1})),0\le i\le 3$，称 $\overline{c}=\beta_0(\underline{c})$ 为 $\underline{c}$ 的模 u 约化。类似地，若 $c(x)=\sum_{i=0}^m c_ix^i\in R[x]$，则称 $\overline{c}(x)=\sum_{i=0}^m\overline{c}_ix^i\in F_2[x]$ 为 $c(x)$ 的模 u 约化。显然有 $\overline{c}(x)=\overline{c}(\xi x)$。

定理 4　设 C 是 R 上长为 n 的 ξ-循环码，且 $C=(\hat{f}_1,u\hat{f}_2,u^2\hat{f}_3,u^3\hat{f}_4)$，其中 $x^n+\xi=\prod_{i=0}^4 f_i,\hat{f}_i=(x^n+\xi)/f_i$，$f_i$ 为两两互素的首一多项式，则其 Gray 象 $\Phi(C)$ 是 F_2 上长为 $4n$ 的线性循环码，且有 $\Phi(C)=(\overline{f}_0^4\overline{f}_2\overline{f}_3^2\overline{f}_4^3)$。

证明　由定理 1 知 $\Phi(C)$ 是 F_2 上长为 $4n$ 的线性循环码。下面证明 $\Phi(C)=(\overline{f}_0^4\overline{f}_2\overline{f}_3^2\overline{f}_4^3)$。

由 $C=(\hat{f}_1,u\hat{f}_2,u^2\hat{f}_3,u^3\hat{f}_4)$ 知，对于任意码字 $A(x)\in C$ 存在 $a(x),b(x),c(x),d(x)\in R[x]/(x^n+\xi)$ 使得 $A(x)=a\hat{f}_1+ub\hat{f}_2+u^2c\hat{f}_3+u^3d\hat{f}_4=X_0+uX_1+u^2X_2+u^3X_3$，其中 $X_i\in F_2[x]$ 且 $X_0=\overline{a}\overline{\hat{f}}_1$。由多项式 Gray 映射，则有

$$\begin{aligned}\Phi(A(x))&=X_3+x^n(X_3+X_2)+x^{2n}(X_3+X_1)\\&\quad+x^{3n}(X_3+X_2+X_1+X_0)=X_3(1+x^n)^3\\&\quad+X_2x^n(1+x^n)^2+X_1x^{2n}(1+x^n)\\&\quad+X_0(1+x^n)(1+x^n+x^{2n})+X_0\\&=(1+x^n)(X_3(1+x^n)^2+X_2x^n(1+x^n)\\&\quad+X_1x^{2n}+X_0(1+x^n+x^{2n}))+X_0\\&=\overline{\hat{f}}_1e(x)\end{aligned}$$

其中 $e(x)\in F_2[x]$。故 $\Phi(C)\subseteq(\overline{\hat{f}}_1)$。若取 $\overline{s}(x)\in\Phi(C)$，存在 $\overline{t}(x)\in F_2[x]/(x^{4n}+1)$ 使得 $\overline{s}(x)=\overline{t}(x)\overline{\hat{f}}_1$。因此

$x^{2n}\bar{s}(x)\bar{f}_1(x)=\bar{t}(x)x^{2n}(1+x^n)=\Phi(u\bar{t}(x))$，故有 $u\bar{t}(x)\in C$。从而存在 $M_1(x),N_1(x),L_1(x),\ K_1(x)\in R[x]/(x^n+\xi)$ 使得 $u\bar{t}(x)=M_1(x)\hat{f}_1+uN_1(x)\hat{f}_2+u^2L_1(x)\hat{f}_3+u^3K_1(x)\hat{f}_4$，即存在 $\overline{H}(x)\in F_2[x]$ 使得 $\bar{t}(x)=\overline{f}_0\overline{f}_3\overline{f}_4\overline{H}(x)$，则可得 $\bar{s}(x)=\overline{f}_0^2\overline{f}_2\overline{f}_3^2\overline{f}_4^2\overline{H}(x)$。故 $\Phi(C)\subseteq(\overline{f}_0^2\overline{f}_2\overline{f}_3^2\overline{f}_4^2)$。再取 $\overline{m}(x)\in\Phi(C)$，存在 $\overline{n}(x)\in F_2[x]/(x^{4n}+1)$ 使得 $\overline{m}(x)=\overline{n}(x)\overline{f}_0^2\overline{f}_2\overline{f}_3^2\overline{f}_4^2$。从而有 $x^n\overline{f}_1^{\,2}\overline{f}_2\overline{m}(x)=\overline{n}(x)x^n(1+x^n)^2=\Phi(u^2\overline{n}(x))$，即有 $u^2\overline{n}(x)\in C$。从而存在 $M_2(x),N_2(x),L_2(x),K_2(x)\in R[x]/(x^n+\xi)$ 使得 $u^2\overline{n}(x)=M_2(x)\hat{f}_1+uN_2(x)\hat{f}_2+u^2L_2(x)\hat{f}_3+u^3K_2(x)\hat{f}_4$，即存在 $\overline{I}(x)\in F_2[x]$ 使得 $\overline{n}(x)=\overline{f}_0\overline{f}_4\overline{I}(x)$，则可得 $\overline{m}(x)=\overline{f}_0^3\overline{f}_2\overline{f}_3^2\overline{f}_4^3\overline{I}(x)$。故 $\Phi(C)\subseteq(\overline{f}_0^3\overline{f}_2\overline{f}_3^2\overline{f}_4^3)$。同理，取 $\overline{r}(x)\in\Phi(C)$，存在 $\overline{q}(x)\in F_2[x]/(x^{4n}+1)$ 使得 $\overline{r}(x)=\overline{q}(x)\overline{f}_0^3\overline{f}_2\overline{f}_3^2\overline{f}_4^3$。故 $\overline{f}_1^3\overline{f}_2^2\overline{f}_3\overline{r}(x)=\overline{q}(x)(1+x^n)^3=\Phi(u^3\overline{q}(x))$，即有 $u^3\overline{q}(x)\in C$。从而存在 $M_3(x),N_3(x),L_3(x),K_3(x)\in R[x]/(x^n+\xi)$ 使得 $u^3\overline{q}(x)=M_3(x)\hat{f}_1+uN_3(x)\hat{f}_2+u^2L_3(x)\hat{f}_3+u^3K_3(x)\hat{f}_4$，即存在 $\overline{J}(x)\in F_2[x]$ 使得 $\overline{q}(x)=\overline{f}_0\overline{J}(x)$，则可得 $\overline{r}(x)=\overline{f}_0^4\overline{f}_2\overline{f}_3^2\overline{f}_4^3\overline{J}(x)$。故 $\Phi(C)\subseteq(\overline{f}_0^4\overline{f}_2\overline{f}_3^2\overline{f}_4^3)$。比较码字个数可得 $\Phi(C)=(\overline{f}_0^4\overline{f}_2\overline{f}_3^2\overline{f}_4^3)$。

下面我们举例来阐明上述结论。

例 1 设 $n=7$，在 $R[x]$ 中，$x^7+1=(x+1)\cdot(x^3+x+1)(x^3+x^2+1)$。应用上述同构有

$$x^7+\xi=(x+\xi^3)(x^3+\xi^2x+\xi)(x^3+\xi^3x^2+\xi)$$

设 C 是 R 上长为 n 的 ξ-循环码，由定理 4 可以得到表 1 所示的二元最优码。

例 2 设 $n=9$，在 $R[x]$ 中，$x^9+1=(x+1)\cdot(x^2+x+1)(x^6+x^3+1)$。应用上述同构有

$$x^9+\xi=(x+\xi)(x^2+\xi x+\xi^2)(x^6+\xi^3x^3+\xi^2)$$

设 C 是 R 上长为 n 的 ξ-循环码，则

(1) 取 $f_0=x+\xi, f_1=x^2+\xi x+\xi^2, f_2=x^6+\xi^3x^3+\xi^2$，则 $\Phi(C)=((x+1)^4(x^6+x^3+1))$，其为[36,26,4]线性循环码，亦为最优码。

(2) 取 $f_1=x^2+\xi x+\xi^2, f_2=x^6+\xi^3x^3+\xi^2, f_4=x+\xi$，则 $\Phi(C)=((x+1)^3(x^6+x^3+1))$，其为[36,27,4]线性循环码，亦为最优码。

5 结束语

本文研究了 $F_2+uF_2+u^2F_2+u^3F_2$ 上 $(1+u+u^2+u^3)$-循环码的 Gray 映射及其性质，并给出了奇长度该常循环码的 Gray 象生成多项式。对于更为一般的多项式剩余类环上的常循环码情况值得进一步研究。

表 1 二元最优码

f_0	f_1	f_2	f_3	f_4	$\Phi(C)$ 的生成多项式	Gray 象
$x+\xi^3$	$x^3+\xi^2x+\xi$	$x^3+\xi^3x^2+\xi$	1	1	$(x+1)^4(x^3+x^2+1)$	[28,21,4]
$x+\xi^3$	$x^3+\xi^3x^2+\xi$	$x^3+\xi^2x+\xi$	1	1	$(x+1)^4(x^3+x+1)$	[28,21,4]
1	$x^3+\xi^2x+\xi$	$x^3+\xi^3x^2+\xi$	1	$x+\xi^3$	$(x^3+x^2+1)(x+1)^3$	[28,22,4]
1	$x^3+\xi^3x^2+\xi$	$x^3+\xi^2x+\xi$	1	$x+\xi^3$	$(x^3+x+1)(x+1)^3$	[28,22,4]
$x+\xi^3$	1	$x^3+\xi^2x+\xi$	1	$x^3+\xi^3x^2+\xi$	$(x+1)^4(x^3+x+1)(x^3+x^2+1)^3$	[28,12,8]
$x+\xi^3$	1	$x^3+\xi^3x^2+\xi$	1	$x^3+\xi^2x+\xi$	$(x+1)^4(x^3+x^2+1)(x^3+x+1)^3$	[28,12,8]
$x^3+\xi^2x+\xi$	1	$x+\xi^3$	1	$x^3+\xi^3x^2+\xi$	$(x^3+x+1)^4(x+1)(x^3+x^2+1)^3$	[28,6,12]
$x^3+\xi^3x^2+\xi$	1	$x+\xi^3$	1	$x^3+\xi^2x+\xi$	$(x^3+x^2+1)^4(x+1)(x^3+x+1)^3$	[28,6,12]

参 考 文 献

[1] Hammons A R, Kumar P V, Calderbank A R, *et al*.. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes[J]. *IEEE Transactions on Information Theory*, 1994, 40(2): 301–319.

[2] Wolfmann J. Negacyclic and cyclic codes over Z_4 [J]. *IEEE Transactions on Information Theory*, 1999, 45(7): 2527–2532.

[3] Tapia-Recillas H and Vega G. Some constacyclic codes over $Z_{2^{k+1}}$ and binary quasi-cyclic codes[J]. *Discrete Applied Mathematics*, 2003, 128(1): 305–316.

[4] Ling S and Blackford T. $Z_{p^{k+1}}$-Linear codes[J]. *IEEE Transactions on Information Theory*, 2002, 48(7): 2592–2605.

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

[6] Amarra M C V and Nemenzo F R. On $(1-u)$-cyclic codes over $F_{p^k}+uF_{p^k}$ [J]. *Applied Mathematics Letters*, 2008, 21(11): 1129–1133.

[7] 朱士信, 李平, 吴波. 环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上一类重根常循环码[J]. 电子与信息学报, 2008, 30(6): 1394–1396.

Zhu S X, Li P, and Wu B. A class of repeated-root constacyclic codes over the ring $F_q+uF_q+\cdots+u^{k-1}F_q$ [J]. *Journal of Electronics & Information Technology*, 2008, 30(6): 1394–1396.

[8] Sobhani R and Esmaeili M. Some constacyclic and cyclic codes over $F_q[u]/\langle u^{t+1}\rangle$ [J]. *IEICE Transactions on*

Foundamentals of Electronics, *Communications and Computer Sciences*, 2010, 93(4): 808–813.

[9] Zhu S X and Wang L Q. A class of constacyclic codes over $F_p + vF_p$ and its Gray image[J]. *Discrete Mathematics*, 2011, 311(23/24): 2677–2682.

[10] Karadenniz S and Yildiz B. $(1+v)$-constacyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$ [J]. *Journal of the Franklin Institute*, 2011, 348(9): 2625–2632.

[11] Yildiz B and Siap I. Cyclic codes over $F_2[u]/(u^4-1)$ and applications to DNA codes[J]. *Computers & Mathematics with Applications*, 2012, 63(7): 1169–1176.

[12] Dinh H Q and Nguyen H D T. On some classes of constacyclic codes over polynomial residue rings[J]. *Advances in Mathematics of Communications*, 2012, 6(2): 175–191.

[13] Qian J F, Zhang L N, and Zhu S X. Cyclic codes over $F_p + uF_p + \cdots + u^{k-1}F_p$ [J]. *IEICE Transactions on Foundamentals of Electronics*, *Communications and Computer Sciences*, 2005, E88-A(3): 795–797.

王立启：　男，1986 年生，博士生，研究方向为代数编码与密码.

朱士信：　男，1962 年生，教授，博士生导师，研究方向为代数编码、信息安全、非线性移位寄存器序列.