环 $F_2+uF_2+vF_2+uvF_2$ 上 $(1+uv)$-循环码

余海峰*[①] 朱士信[②] 张 霞[①]
[①](合肥学院数学与物理系 合肥 230601)
[②](合肥工业大学数学学院 合肥 230009)

摘 要：该文定义了有限非链环 $R=F_2+uF_2+vF_2+uvF_2$ 上 $(1+uv)$-循环码的相关概念，讨论了其与该环上循环码的关系，证明了此环上 $(1+uv)$-循环码在关于齐次重量的等距Gray映射 $\phi_{\rm hom}$ 下的二元象是一个长为 $8n$ 的4-准循环码, 并由此映射得到了一些好的二元线性准循环码。

关键词：循环码；$(1+uv)$-循环码；Gray映射；准循环码
中图分类号： TN911.22 **文献标识码**：A **文章编号**：1009-5896(2014)06-1419-04
DOI: 10.3724/SP.J.1146.2013.01339

$(1+uv)$-Cyclic Codes Over $F_2+uF_2+vF_2+uvF_2$

Yu Hai-feng[①] Zhu Shi-xin[②] Zhang Xia[①]
[①](*Department of Mathematics and Physics*, *Hefei University*, *Hefei* 230601, *China*)
[②](*School of Mathematics*, *Hefei University of Technology*, *Hefei* 230009, *China*)

Abstract: $(1+uv)$-cyclic codes over $F_2+uF_2+vF_2+uvF_2$ is defined, and the relations between $(1+uv)$-cyclic codes and cyclic codes is discussed. It is proved that the binary image on isometric Gray map $\phi_{\rm hom}$ of a $(1+uv)$-cyclic code of length n over R is a linear quasi-cyclic code of index 4 and of length $8n$. Furthermore, some optimal binary linear quasi-cyclic codes are obtained.

Key words: Cyclic codes; $(1+uv)$-cyclic code; Gray map; Quasi-cyclic code

1 引言

自1994年Hammons等人在文献[1]中证明了二元Kerdock码及其它一些高效的二元非线性码可视为环 Z_4 上线性码在Gray映射下的二元象后，环上码的研究成为纠错码理论研究的一个热点。近年来对环上线性码的研究主要集中在有限链环如环 $Z_{p^n}, F_p+uF_p+\cdots+u^kF_p$ 上，有限链环上循环码和常循环码是重点研究内容[2–9]。2010年，文献[10]首次引入环 $R=F_2+uF_2+vF_2+uvF_2$ 作为有限非链环的代表载体，研究了该环上的线性码，将该环上线性码与二元域上的Reed-Muller码联系起来，使得该环上码的研究也成为了一个热门内容。之后，该环上的自对偶码、循环码和常循环码也不断被人们加以研究，并得到了一些非常好的结果[11–15]。

由于该环既不是有限链环，也不是主理想环，因而以往在有限链环上的很多研究方法难以利用，一个较好的方法就是通过不同的Gray映射将该环上线性码和有限链环 F_2+uF_2 上线性码以及二元码联系起来，一方面可通过有限链环上的码来研究该环上的码，另一方面也可通过此映射构造具有更好参数的二元码。这样就构造出了许多不同形式的Gray映射，文献[12]中定义了两种不同的Gray映射：一种关于Lee重量的Gray映射 ϕ_L，并证明了循环码在该映射之下是一个 $4n$ 的4-拟循环码，另一种关于齐次重量的Gray映射 $\phi_{\rm hom}$，并证明了循环码在该映射之下是一个 $8n$ 的8-拟循环码。文献[15]通过定义该环到有限链环 F_2+uF_2 上的Gray映射进一步研究了该环上的 $(1+u)$-循环码，并证明了这类常循环码关于Lee重量的Gray映射 ϕ_L 的二元象是一个 $4n$ 的4-准循环码，将有限链环上常循环码的性质很好地推广到了非有限链环上，因为在环 R 上 u,v 地位等同，故显然环 R 上 $(1+u)$-循环码也具有此性质，但这些常循环码在另一种Gray映射 $\phi_{\rm hom}$ 下的二元象则无此性质。本文旨在寻找具有此类性质的常循环码。

经过研究，我们发现了环 R 上关于Gray映射 $\phi_{\rm hom}$ 下的二元象具有此性质的一类常循环码：$(1+u)$-循环码。本文首先定义了该环上的等距Gray映射 $\phi_{\rm hom}$，其次讨论了循环码和 $(1+u)$-循环码的关系，得到了 $(1+u)$-循环码的结构，最后证明了该环上 $(1+u)$-循环码在Gray映射 $\phi_{\rm hom}$ 下的二元象是一个长为 $8n$ 的4-准循环码，并在此基础上利用Gray映射 $\phi_{\rm hom}$ 得到了一些好的二元准循环码。

2013-09-04 收到，2013-11-08 改回
国家自然科学基金(60973125)，安徽高校省级自然科学基金(KJ2013Z276)和合肥学院科研发展重点基金(10KY01ZD)资助课题
*通信作者：余海峰 yuhfslx@hfuu.edu.cn

2 环 $F_2+uF_2+vF_2+uvF_2$ 上的线性码及Gray映射

令 $R=F_2+uF_2+vF_2+uvF_2$，其中 u,v 满足 $u^2=v^2=0, uv=vu$，则 R 是一个特征为2的局部环，Frobenius环，但 R 既不是有限链环也不是主理想环。

环 R 上共有16个元素，每个元素均可记为 $x=a+ub+vc+uvd$，其中 $a,b,c,d\in F_2$。

首先给出环 R 上线性码的定义：

定义 1 环 R 上长为 n 的线性码指的是 R 模 R^n 的一个加法子模。

在文献[12]中，环 R 上任一元素 x 的齐次重量 $w_{\rm hom}(x)$ 可定义为

$$w_{\rm hom}(x)=\begin{cases}0, & x=0\\ 8, & x=uv\\ 4, & x\text{为}R\text{中其余元素}\end{cases}$$

进一步可扩展至 R^n 中向量 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$ 的齐次重量：$w_{\rm hom}(\boldsymbol{X})=\sum_{i=0}^{n-1}w_{\rm hom}(x_i)$,则可定义 R^n 中向量 $\boldsymbol{X},\boldsymbol{Y}$ 的齐次距离为 $d_{\rm hom}(\boldsymbol{X},\boldsymbol{Y})=w_{\rm hom}(\boldsymbol{X}-\boldsymbol{Y})$。

定义2 若记环 R 上任一元素 $x_i=a_i+ub_i+vc_i+uvd_i$，其中 $a_i,b_i,c_i,d_i\in F_2$，则可定义 x_i 的关于齐次重量的Gray映射 $\phi_{\rm hom}$ 为

$$\begin{aligned}\phi_{\rm hom}(x_i)=(&a_i+b_i+c_i+d_i,b_i+c_i+d_i,\\&a_i+b_i+d_i,b_i+d_i,a_i+c_i+d_i,\\&c_i+d_i,a_i+d_i,d_i)\end{aligned}$$

可延伸至 R^n 中向量 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$ 的关于齐次重量的Gray映射 $\phi_{\rm hom}$ 为

$$\begin{aligned}\phi_{\rm hom}(\boldsymbol{X})=(&a_0+b_0+c_0+d_0,\cdots,a_{n-1}+b_{n-1}+c_{n-1}+d_{n-1},\\&b_0+c_0+d_0,\cdots,b_{n-1}+c_{n-1}+d_{n-1},\\&a_0+b_0+d_0,\cdots,a_{n-1}+b_{n-1}+d_{n-1},\\&b_0+d_0,\cdots,b_{n-1}+d_{n-1},a_0+c_0+d_0,\cdots,\\&a_{n-1}+c_{n-1}+d_{n-1},c_0+d_0,\cdots,c_{n-1}+d_{n-1},\\&a_0+d_0,\cdots,a_{n-1}+d_{n-1},d_0,\cdots,d_{n-1})\end{aligned}$$

关于该映射，有

命题 1[12]：如果 C 是环 R 上一个 $(n,2^k,d_{\min({\rm hom})})$ 线性码，则 $\phi_{\rm hom}(C)$ 是域 F_2 上的 $[8n,k,d_{\min(H)}]$ 线性码。

3 环 $F_2+uF_2+vF_2+uvF_2$ 上的循环码与 $(1+uv)$-循环码

定义 3 对于 R^n 中向量 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$，定义 $\boldsymbol{\nu}_\lambda(\boldsymbol{X})=(\lambda x_0,x_1,\cdots,x_{n-1})$ 为向量 $\boldsymbol{X}$ 的 λ-循环移位向量，对于 R 上一线性码 C，若 $\forall\mathcal{C}=(c_0,c_1,\cdots,c_{n-1})\in C$ 均有 $\nu_\lambda(\mathcal{C})\in C$，则称 C 为 R 上的 λ-循环码；若 $\lambda=1+uv$，则称 C 为 R 上的 $(1+uv)$-循环码；若 $\lambda=1$，则称 C 为 R 上的循环码。

类似文献[15]中的证明方法，有

命题 2 定义 R^n 上码字 $\mathcal{C}=(c_0,c_1,\cdots,c_{n-1})$ 的多项式表示是指从 R^n 到 $R[x]$ 的一同构映射：$P(\mathcal{C})=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$。那么有：若码 C 为 R 上一长为 n 的循环码，则 $P(C)$ 为 $A_n=R[x]/(x^n-1)$ 的一理想；若码 C 为 R 上一长为 n 的 $(1+uv)$-循环码，则 $P(C)$ 为 $B_n=R[x]/(x^n-1-uv)$ 的一理想。

关于循环码和 $(1+uv)$-循环码，可证明如下结论：

命题 3 设 n 为奇数，若 μ 是 A_n 到 B_n 的满足：$\mu(c(x))=c((1+uv)x)$ 的映射，则 μ 为一环同构。

证明 因 $a(x)\equiv b(x)\bmod(x^n-1)\Leftrightarrow a((1+uv)x)\equiv b((1+uv)x)\bmod(x^n-1-uv)$。至于 μ 对多项式的加法和乘法保持性是自然的，故 μ 是环同构。 证毕

推论 1 设 I 为 A_n 的子集，J 为 B_n 的子集且满足 $J=\mu(I)$，则 I 是 A_n 的理想当且仅当 J 是 B_n 的理想。

推论 2 对 R^n(n 为奇数)上任一码字 $\mathcal{C}=(c_0,c_1,\cdots,c_{n-1})$ 记 $\overline{\mu}\mathcal{C}=(c_0,(1+uv)c_1,\cdots,(1+uv)^ic_i,\cdots,(1+uv)^{n-1}c_{n-1})$，若 D 为 R^n 的一子模，则 D 是循环码当且仅当 $\overline{\mu}D$ 是 $(1+uv)$-循环码。

在文献[12]中，当码长 n 为奇数时，有：

引理 1 若码 C 为 R 上一长为 n 的循环码，则 $P(C)$ 为 $A_n=R[x]/(x^n-1)$ 的一理想，且有 $P(C)=<g_1(x)+up_1(x)+uvb_2(x),vg_2(x)+uvp_2(x)>$，其中 $g_i,p_i,\ b_2\in F_2[x]/(x^n-1)$，且有 $p_1|g_1|x^n-1,p_2|g_2|x^n-1,\ \ g_2|g_1|x^n-1$。

由此可得：

定理 1 若码 C 为 R 上一长为奇数 n 的 $(1+uv)$-循环码，则 $P(C)$ 为 $B_n=R[x]/(x^n-1-uv)$ 的一理想，且有：$P(C)=<g_1(\tilde{x})+up_1(\tilde{x})+uvb_2(\tilde{x}),vg_2(\tilde{x})+uvp_2(\tilde{x})>$。其中 $\tilde{x}=(1+uv)x,\ g_i,\ p_i,\ b_2\in F_2[x]/(x^n-1)$，且 $p_1|g_1|x^n-1,\ p_2|g_2|x^n-1,g_2|g_1|x^n-1$。

4 环 $F_2+uF_2+vF_2+uvF_2$ 上 $(1+uv)$-循环码与循环码的Gray象

4.1 码长 n 为任意整数情形

对任意整数 m,s 若定义：

$$\sigma_s:F_2^{sm}\rightarrow F_2^{sm}$$

$$\left(a^{(1)}\middle|a^{(2)}\middle|\cdots\middle|a^{(s)}\right)\rightarrow\left(\sigma a^{(1)}\middle|\sigma a^{(2)}\middle|\cdots\middle|\sigma a^{(s)}\right)$$

其中 $a^{(1)},a^{(2)},\cdots,a^{(s)}\in F_2^m,\sigma:F_2^m\to F_2^m$ 为循环移位。则对于域 F_2 的码 C，若 $\sigma_s(C)=C$，称码 C 为域 F_2 上长为 sm 的 s - 准循环码。

下面给出本文的一个主要定理：

定理 2　环 R 上的一长为 n 码 C 为 $(1+uv)$ - 循环码 $\Leftrightarrow$ $\phi_{\text{hom}}(C)$ 为域 F_2 上长为 $8n$ 的 4 - 准循环码。

证明　对于环R上任一码字 $\mathcal{C}=(c_0,c_1,\cdots,c_{n-1})$，由前述定义

$$\begin{aligned}\phi_{\text{hom}}\nu_{1+uv}(\mathcal{C})&=\phi_{\text{hom}}\left((1+uv)c_{n-1},c_0,\cdots,c_{n-2}\right)\\&=(b_{n-1}+c_{n-1}+d_{n-1},a_0+b_0+c_0+d_0,\cdots,\\&\quad a_{n-1}+b_{n-1}+c_{n-1}+d_{n-1},\\&\quad b_0+c_0+d_0,\cdots,b_{n-2}+c_{n-2}+d_{n-2},|\\&\quad b_{n-1}+d_{n-1},a_0+b_0+d_0,\cdots,\\&\quad a_{n-1}+b_{n-1}+d_{n-1},\\&\quad b_0+d_0,\cdots,b_{n-2}+d_{n-2},|c_{n-1}+d_{n-1},\\&\quad a_0+c_0+d_0,\cdots,a_{n-1}+c_{n-1}+d_{n-1},\\&\quad c_0+d_0,\cdots,c_{n-2}+d_{n-2},|d_{n-1},\\&\quad a_0+d_0,\cdots,a_{n-1}+d_{n-1},d_0,\cdots,d_{n-2})\\&=\sigma_4\phi_{\text{hom}}(\mathcal{C})\end{aligned}$$

即 $\phi_{\text{hom}}\nu_{1+uv}(C)=\sigma_4\phi_{\text{hom}}(C)$。因 ϕ_{hom} 为双射，故码 C 为 $(1+uv)$ -循环码

$$\begin{aligned}&\Leftrightarrow\nu_{1+uv}(C)=C\Leftrightarrow\phi_{\text{hom}}\nu_{1+uv}(C)\\&\qquad=\phi_{\text{hom}}(C)\Leftrightarrow\sigma_4\phi_{\text{hom}}(C)\\&\qquad=\phi_{\text{hom}}(C)\Leftrightarrow\phi_{\text{hom}}(C)\end{aligned}$$

为域 F_2 上长为 $8n$ 的 4- 准循环码。　　证毕

4.2 码长 n 为奇数情形

在4.1节中我们讨论了对码长 n 为任意整数时，环 R 上 $(1+uv)$ - 循环码的 ϕ_{hom} 二元象均是长为 $8n$ 的 4 - 准循环码，当码长为奇数时还可证明环 R 上循环码的广义Gray映射(即定理3中的映射 $\pi_4\phi_{\text{hom}}$)的二元象也是长为 $8n$ 的 4 - 准循环码。为方便起见，本节讨论所有出现的 n 均为奇数，以下不再一一说明。

对任意整数 s 若定义：

$$\pi_s:F_2^{2ns}\to F_2^{2ns}$$

$$\left(a^{(1)}\left|a^{(2)}\right|\cdots\left|a^{(s)}\right.\right)\to\left(\pi a^{(1)}\left|\pi a^{(2)}\right|\cdots\left|\pi a^{(s)}\right.\right)$$

其中 $a^{(1)},a^{(2)},\cdots,a^{(s)}\in F_2^{2n},\pi$ 为文献[3]中所定义的Nechaev变换。则可以证明：

定理 3　环 R 上的一长为 n 码 C 为循环码 $\Leftrightarrow$ $\pi_4\phi_{\text{hom}}(C)$ 为域 F_2 上长为 $8n$ 的 4 - 准循环码。

证明　对于环R上任一码字 $\mathcal{C}=(c_0,c_1,\cdots,c_{n-1})$，考虑到

$$(1+uv)^i=\begin{cases}1+uv, & i\text{为奇数}\\1, & i\text{为偶数}\end{cases}$$

则由前述 $\phi_{\text{hom}},\overline{\mu},\pi_4$ 定义可得：

$$\begin{aligned}\overline{\mu}(\mathcal{C})&=\phi_{\text{hom}}\left(c_0,(1+uv)c_1,\cdots,(1+uv)^ic_i,\cdots,\right.\\&\qquad\left.(1+uv)^{n-2}c_{n-2},(1+uv)^{n-1}c_{n-1}\right)\\&=\phi_{\text{hom}}(c_0,(1+uv)c_1,c_2,(1+uv)c_3,\cdots,\\&\qquad c_{n-3},(1+uv)c_{n-2},c_{n-1})\\&=(a_0+b_0+c_0+d_0,b_1+c_1+d_1,a_2+b_2+c_2+d_2,\\&\qquad b_3+c_3+d_3,\cdots,a_{n-1}+b_{n-1}+c_{n-1}+d_{n-1},\\&\qquad b_0+c_0+d_0,a_1+b_1+c_1+d_1,b_2+c_2+d_2,\\&\qquad a_3+b_3+c_3+d_3,\cdots,b_{n-1}+c_{n-1}+d_{n-1},|\\&\qquad a_0+b_0+d_0,b_1+d_1,a_2+b_2+d_2,\\&\qquad b_3+d_3,\cdots,a_{n-1}+b_{n-1}+d_{n-1},\\&\qquad b_0+d_0,a_1+b_1+d_1,b_2+d_2,\\&\qquad a_3+b_3+d_3,\cdots,b_{n-1}+d_{n-1},|\\&\qquad a_0+c_0+d_0,c_1+d_1,a_2+c_2+d_2,\\&\qquad c_3+d_3,\cdots,a_{n-1}+c_{n-1}+d_{n-1},\\&\qquad c_0+d_0,a_1+c_1+d_1,c_2+d_2,a_3\\&\qquad +c_3+d_3,\cdots,c_{n-1}+d_{n-1},|\\&\qquad a_0+d_0,d_1,a_2+d_2,d_3,\cdots,a_{n-1}+d_{n-1},\\&\qquad d_0,a_1+d_1,d_2,a_3+d_3,\cdots,d_{n-1})\\&=\pi_4\phi_{\text{hom}}(\mathcal{C})\end{aligned}$$

则该定理由推论2及定理2可得。　　证毕

4.3 由Gray映射 ϕ_{hom} 构造二元好码举例

下面我们通过一个例子来说明由 $(1+uv)$ - 循环码确实可构造一些二元好码。

例　设 $n=3$，由定理1，可知环 R 上的 $(1+uv)$ - 循环码可由 B_n 的多项式生成，表1给出了一些利用生成多项式为一个多项式的 $(1+uv)$ - 循环码与循环码的Gray象得到的二元好码。

5　结束语

本文研究了环 $R=F_2+uF_2+vF_2+uvF_2$ 上 $(1+uv)$ - 循环码和它在Gray映射 ϕ_{hom} 下的二元象的性质，给出了在码长为奇数时 $(1+uv)$ - 循环码的生成元，并由此映射得到了一些好的二元线性准循环码，为构造二元好码提供了好的思路。寻找能够构造好码的其它类型的常循环码以及更为一般的非有限链环上常循环码性质研究将是我们下一步研究的目标。

表1 二元好码参数表

$(1+uv)$ - 循环码	对应循环码	$\phi_{\text{hom}}(C)$
$< uv+(uv)x+(uv)x^2 >$	$< uv+(uv)x+(uv)x^2 >$	$[24,1,24]$
$< uv+(uv)x >$	$< uv+(uv)x >$	$[24,2,16]$
$< u+vx+(u+v)x^2 >$	$< u+vx+(u+v)x^2 >$	$[24,4,12]$
$< 1+u+(1+v)x+(1+uv)x^2 >$	$< 1+u+(1+v+uv)x+(1+uv)x^2 >$	$[24,8,8]$
$< 1+u+(1+v+uv)x+(1+uv)x^2 >$	$< 1+u+(1+u)x+(1+uv)x^2 >$	$[24,9,8]$

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] Wolfmann J. Binary images of cyclic codes over z_4 [J]. *IEEE Transactions on Information Theory*, 2001, 47(5): 1773–1779.

[4] Ling S and Blackford J. $z_{p^{k+1}}$ -linear codes[J]. *IEEE Transactions on Information Theory*, 2002, 48(9): 2592–2605.

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

[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] Shi Min-jia, Yang Shan-lin, and Zhu Shi-xin. Good p-ary quasic-cyclic codes from cyclic codes over F_p+vF_p [J] . *Journal of Systems Science and Complexity*, 2012, 25(2): 375–384.

[8] 王立启, 朱士信. 环 $F_2[u]/(u^4)$ 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.
Wang Li-qi and Zhu Shi-xin. A class of constacyclic codes over $F_2[u]/(u^4)$ and its Gray image[J]. *Journal of Electronics & Information Technology*, 2013, 35(2): 499–503.

[9] Cao Yong-lin. On constacyclic codes over finite chain rings[J]. *Finite Fields and Their Applications*, 2013, 24: 124–135.

[10] Yildiz B and Karadenniz S. Linear codes over $F_2+uF_2+vF_2+uvF_2$ [J]. *Designs, Codes and Cryptography*, 2010, 54(1): 61–81.

[11] Yildiz B and Karadeniz S. Self-dual codes over $F_2+uF_2+vF_2+uvF_2$ [J]. *Journal of the Franklin Institute*, 2010, 347(10): 1888–1894.

[12] Yildiz B and Karadenniz S. Cyclic codes over $F_2+uF_2+vF_2+uvF_2$ [J]. *Designs, Codes and Cryptography*, 2011, 58(3): 221–234.

[13] 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.

[14] Siap I, Abualrub T, and Yildiz B. One generator quasi-cycliccodes over F_2+uF_2 [J]. *Journal of the Franklin Institute*, 2012, 349(1): 284–292.

[15] Kai Xiao-shan, Zhu Shi-xin, and Wang Li-qi. A family of constacyclic codes over $F_2+uF_2+vF_2+uvF_2$ [J]. Journal *of Systems Science and Complexity*, 2012, 25(5): 1032–1040.

余海峰： 男，1975年生，副教授，研究方向为代数编码.

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、序列密码.

张 霞： 女，1972年生，教授，研究方向为代数编码.