Vol. 34 (2014)
No. 1

数 学 杂 志
J. of Math. (PRC)

环 $F_2+uF_2+vF_2$ 上自对偶码的两种构造方法

胡 鹏, 李 慧
(湖北理工学院数理学院, 湖北 黄石 435003)

摘 要: 本文研究环 $R=F_2+uF_2+vF_2$ 上的自对偶码问题. 利用 R^n 到 F_2^{3n} 的 Gray 映射及 R 上的自对偶码 C 的 Gray 像为 F_2 上自对偶码, 获得了 R 上任何偶长度的自对偶码存在性的结论. 最后, 给出了 R 上两种构造自对偶码的方法.

关键词: 自对偶码; Gray 映射; 双循环矩阵
MR(2010) **主题分类号**: 94B05 **中图分类号**: O157.4
文献标识码: A **文章编号**: 0255-7797(2014)01-0168-05

1 引言

自对偶码是一类重要的码. 人们通过研究发现, 自对偶码与组合、群论和格论有密切关系. 对有限环上的自对偶码的研究可以促进幺模格及非线性码的发展 (见文献 [1–3]), 从而导致了许多作者对各种类型的环中自对偶码的研究. Dougherty 等人在文献 [4] 研究了 R_k 与 F_2 上的自对偶码, Kim 和 Lee 研究了 Galois 环上自对偶码的构造方法并用这种方法研究了 Galois 环上的 MDS 自对偶码 (见文献 [5]), 接着 Dougherty 等人将这种自对偶码的构造方法扩展到了有限链环上 (见文献 [6]). 最近, Yildiz 和 Karadeniz 研究了有限非链环 $F_2+uF_2+vF_2+uvF_2$ 上的自对偶码, 通过对这种环自对偶码的研究, 可以获得许多新的二元好码 (见文献 [7]).

本文的目的是研究环 $R=F_2+uF_2+vF_2=\{a+ub+vd \mid a,b,d\in F_2, u^2=v^2=uv=vu=0\}$ 上的自对偶码. 首先定义了一个从 R^n 到 F_2^{3n} 的 Gray 映射 φ. 这个映射将 R 上长为 n 的自对偶码映射到 F_2 上长为 $3n$ 的自对偶码. 通过给出 R 上长为 2 的自对偶码证明了 R 上存在任何偶长度的自对偶码. 最后, 给出了 R 上两种构造自对偶码的方法.

2 R 上自对偶

环 $R=F_2+uF_2+vF_2$ 是一个特征为 2 且理想为

$$I_0=\{0\}\subseteq I_u, I_v\subseteq I_{u+v}, I_{1+v}\subseteq I_1=R$$

的主理想环, 其中 $I_u=\{0,u\}, I_v=\{0,v\}, I_{u+v}=\{0,u,v,u+v\}, I_{1+v}=\{0,u,1+v,1+u+v\}$. 且对于任意 $a\in F_2+uF_2+vF_2$, 有

$$a^2=\begin{cases}1, & \text{当}a\text{是一个单位},\\ 0, & \text{否则}.\end{cases} \tag{2.1}$$

*收稿日期: 2013-01-07 接收日期: 2013-05-09
基金项目: 湖北理工学院青年项目 (13xjz07Q).
作者简介: 胡鹏 (1981–), 男, 湖北黄石, 讲师, 主要研究方向: 代数编码, 仿真计算.

如果 C 为 R - 模 R^n 的一个加法子模, 则称 C 为 R 上长为 n 的线性码. 对于任意 $x=(x_1,\cdots,x_n)$, $y=(y_1,\cdots,y_n)\in R^n$, 称 $x_1y_1+\cdots+x_ny_n$ 为 x 与 y 的内积, 记为 $[x,y]$, 即 $[x,y]=x_1y_1+\cdots+x_ny_n$. 定义 $C^\perp=\{x\in R^n\mid [x,y]=0,\forall y\in C\}$, 称 $C^\perp$ 为 C 的对偶码. 若 $C\subseteq C^\perp$, 则称 C 为自正交码; 若 $C=C^\perp$, 则称 C 为自对偶码.

接下来, 给出 $R^n\longrightarrow F_2^{3n}$ 的 Gray 映射.

定义 2.1 显然映射

$$\varphi: R\to F_2^3$$

$$a+ub+vc\mapsto (c,b+c,a+b+c)$$

是 R 到 F_2^3 的双射. 将其扩充 R^n 到 F_2^{3n} 仍记为

$$\varphi: R\to F_2^{3n}$$

$$(x_1,\cdots,x_n)\mapsto(\varphi(x_1),\cdots,\varphi(x_n)),$$

则 φ 也是 R^n 到 F_2^{3n} 的双射. 称这个映射 φ 为 R^n 到 F_2^{3n} 的 Gray 映射.

定义 2.2 设 $(x_1,\cdots,x_n)\in R^n$, 称 $W_H(\varphi(x_1),\cdots,\varphi(x_n))$ 为 R^n 中元素 $(x_1,\cdots,x_n)$ 的 Lee 重量, 记为 $W_L(x_1,\cdots,x_n)$. 即 $W_L(x_1,\cdots,x_n)=W_H(\varphi(x_1),\cdots,\varphi(x_n))$, 其中 W_H 表示 F_2^{3n} 中元素的 Hamming 重量.

显然, 我们有下面引理.

引理 2.1 如果 C 是 $F_2+uF_2+vF_2$ 上长为 n, $|C|=2^k$, 且最小 Lee 重量为 d 的线性码, 则 $\varphi(C)$ 是 F_2 上长为 $3n$, 维数为 k 且最小 Hamming 重量为 d 的线性码.

有了以上准备, 我们可以证明如下重要定理.

定理 2.2 设 C 为 R 上长为 n 的线性码, $C^\perp$ 为它的对偶码, 则 $\varphi(C^\perp)=\varphi(C)^\perp$. 进而, 如果 C 为自对偶码, 则 $\varphi(C)$ 也为自对偶码.

证 显然 C 中的任意码字 C 可以表示为 $C=a+ub+vd$, 其中 $a,b,d\in F_2^n$.

对于任意 $c_1=a_1+ub_1+vd_1, c_2=a_2+ub_2+vd_2\in C$, 这里 $a_1,a_2,b_1,b_2,d_1,d_2\in F_2^n$, 若 $[c_1,c_2]=0$, 则

$$[a_1,a_2]+[d_1,d_2]=0,[a_2,b_2]+[a_2,b_1]=0,[d_1,a_2]+[a_1,d_2]=0,$$

因此

$$[\varphi(c_1),\varphi(c_2)]=[a_1,a_2]+[d_1,d_2]+[a_1,b_2]+[a_2,b_1]+[d_1,a_2]+[a_1,d_2]=0,$$

从而

$$\varphi(C^\perp)\subseteq\varphi(C)^\perp. \tag{2.2}$$

由引理 2.1 知, $\varphi(C)$ 是长为 $3n$ 的二元线性码且 $|\varphi(C)|=|C|$, 因此根据二元自对偶码的性质, 得 $|\varphi(C)^\perp|=\frac{2^{3n}}{|\varphi(C)|}=\frac{2^{3n}}{|C|}$. 又 R 为 Frobenius 环, 故由文献 [8] 知 $|C|\cdot|C^\perp|=2^{3n}$. 从而

$$|\varphi(C^\perp)|=|\varphi(C)^\perp|. \tag{2.3}$$

综合 (2.2) 式与 (2.3) 式, 得 $\varphi(C^\perp)=\varphi(C)^\perp$.

注 R 中不存在长为 1 的自对偶. 若不然, 设 C 是 R 上长为 1 的自对偶码, 则 $|C| = |C^{\perp}|$ 且 $|C| \cdot |C^{\perp}| = 8$, 这是不可能的.

取

$$\begin{aligned} & C = \langle (1,1) \rangle \\ = \ & \{(0,0),(1,1),(u,u),(v,v),(1+u,1+u),(1+v,1+v),(1+u+v,1+u+v),(u+v,u+v)\}, \end{aligned}$$

则 C 是自正交码. 又 $|C| = 8$, 因此 $|C^{\perp}| = 8$. 故 C 是 R 上的自对偶码.

由文献 [6] 的引理 3.2, 我们有如下定理.

定理 2.3 R 上存在任何偶数长度的自对偶码.

3 R 上一类自对偶码的构造

记 R 上 k 阶循环矩阵 $A = \begin{pmatrix} a_1 & a_2 & \dots & a_k \\ a_k & a_1 & \dots & a_{k-1} \\ \vdots & & \ddots & \vdots \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}$ 为 $A = [a_1, a_2, \cdots, a_k]$. 称分块矩阵 $G = (I_k|A)$ 为 R 上的双循环矩阵, 其中 I_k 为 R 上单位矩阵.

下面我们考虑 R 上由 G 生成的自对偶码. 分两种情形讨论.

情形 1 k 为奇数, 令 $k = 2s+1$.

定理 3.1 设 C 是 R 上由 $G = (I_{2s+1}|A)$ 生成长为 $4s+2$ 的线性码, 这里 $A = [a_1, a_2, \cdots, a_s, a_s, a_{s-1}, \cdots, a_1, h]$, 其中 a_i 是 R 的非单位元, h 为 R 上的单位元. 则 C 是一个自对偶码.

证 记 G 的第 i 行为 $G_i (i = 1, 2, \cdots, 2s+1)$, 则

$$C = \{x_1 G_1 + x_2 G_2 + \cdots + x_{2s+1} G_{2s+1} | x_1, x_2, \cdots, x_{2s+1} \in R\},$$

从而

$$|C| = 8^{2s+1} = \sqrt{8^{4s+2}} = |C^{\perp}|. \tag{3.1}$$

分别用 e_i 与 A_i 表示 I_{2s+1} 与 A 的第 i 行 $(i = 1, 2, \cdots, 2s+1)$, 则 $G_i = (e_i, A_i)$. 注意到 $[G_i, G_j] = [e_i, e_j] + [A_i, A_j]$, 而

$$[e_i, e_j] = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

为此来计算 $[A_i, A_j]$.

当 $i = j$ 时, $[A_i, A_i] = h^2 + 2\sum\limits_{i=1}^{s} a_i^2 = 1$.

当 $i \neq j$ 时, 不妨设 $i < j$. 设 τ 表示对 A 中行向量的循环位移, 则 $A_i = \tau^{i-1}(A_1)$, 且 $[A_i, A_j] = [\tau(A_i), \tau(A_j)]$, 于是

$$[A_i, A_j] = [\tau^{i-1}(A_1), \tau^{j-1}(A_1)] = [A_1, \tau^{j-i}(A_1)].$$

易验证, 在 $[A_1,\tau^{j-i}(A_1)]$ 中, 如果 a_l 与 a_t 配对, 那么 a_t 也与 a_l 配对; 如果 h 与 a_r 配对, 那么 a_r 也与 h 配对. 由于 A 的行中总元素个数为奇数, 所以总有一个元素 a_q 与它自身配对. 因此 $[A_i,A_j]=[A_1,\tau^{j-i}(A_1)]$ 的表达式是由形为 $2a_rh, 2a_la_t$ 和 a_q^2 的项组成, 故 $[A_i,A_j]=0$.

根据以上计算, 有

$$[G_i,G_j]=0. \tag{3.2}$$

综合 (3.1) 式与 (3.2) 式知, C 为自对偶码.

情形 2 k 为偶数. 令 $k=2s$.

定理 3.2 设 C 是 R 上由 $G=(I_{2s}|B)$ 生成的长为 $4s$ 的线性码, 这里

$$B=[b_1,b_2,\cdots,b_{s-1},b_s,b_{s-1},\cdots,b_1,y],$$

其中 b_i 是单位且 y 是非单位或 b_i 是非单位且 y 是单位, 则 C 是 R 上的自对偶码.

证 类似于定理 3.1 的证明, 易证 $|C|=|C^{\perp}|$. 因此, 要证明 C 是自对偶码, 只需证 C 是自正交码. 同样, 类似于定理 3.1 的证明, 只需证

$$[B_i,B_j]=\begin{cases}1, & i=j,\\ 0, & i\neq j,\end{cases}$$

其中 B_i,B_j 分别表示 B 的 i,j 行.

当 $i=j$ 时, $[B_i,B_j]=2(b_1^2+\cdots+b_{s-1}^2)+b_s^2+y^2=1$.

当 $i\neq j$ 时, 不妨设 $i<j$, 同样有

$$[B_i,B_j]=[B_1,\tau^{j-i}(B_1)].$$

易验证, 在 $[B_1,\tau^{j-i}(B_1)]$ 中, 如果 b_l 与 b_t 配对, 那么 b_t 也与 b_l 配对. 也可能发生 b_r 与它自身配对, 由于 B_1 中的坐标个数为偶数, 因此与自身配对的 b_r 的个数为偶数. 故 $[B_i,B_j]=[B_1,\tau^{j-i}(B_1)]=0$.

例 1 取 $G_1=\begin{pmatrix}1&0&0&0&0&u&v&v&u&1+u\\0&1&0&0&0&1+u&u&v&v&u\\0&0&1&0&0&u&1+u&u&v&v\\0&0&0&1&0&v&u&1+u&u&v\\0&0&0&0&1&v&v&u&1+u&v\end{pmatrix}$, 则由定理 3.1 知, G_1 生成 R 上长为 10 且码字个数为 8^5 的自对偶码 C_1, 再由定理 2.2 知 $\varphi(C_1)$ 是 F_2 上长为 30 且维数为 15 的自对偶码.

例 2 取 $G_2=\begin{pmatrix}1&0&0&0&1+u+v&1+v&1+u+v&1+u\\0&1&0&0&1+u&1+u+v&1+v&1+u+v\\0&0&1&0&1+u+v&1+u&1+u+v&1+v\\0&0&0&1&1+v&1+u+v&1+u&1+u+v\end{pmatrix}$, 则由定理 3.2 知, G_2 生成 R 上长为 8 且码字个数为 8^4 的自对偶码 C_2, 再由定理 2.2 知 $\varphi(C_2)$ 是 F_2 上长为 24 且维数为 12 的自对偶码.

参 考 文 献

[1] Bonnecuze A, Udaya P. Cyclic codes and self-dual codes over $F_2 + uF_2$ [J]. IEEE Trans. Inform. Theory, 1999, 45(4): 1250–1255.

[2] Bannai E, Dougherty S T, Harada M, Ouar M. Type II codes, Even unimodular lattices, and invariant rings [J]. IEEE-IT, 1999, 45(4): 1194–1205.

[3] Dougherty S T, Gaborit P, Harada M, Sole P. Type II codes over $F_2 + vF_2$ [J]. IEEE Frans. Inform. Theory, 1999, 45(4): 32–45.

[4] Dougherty S T, Yildiz B, Kandeniz S. Self-dual codes over R_k and binary self-dual codes [J]. in submission.

[5] Kim J-L, Lee Y. Construction of MDS self-dual codes over Galois rings [J]. Designs, Codes, and Crypto, 2007, 45: 247–258.

[6] Dougherty S T, Kim J-L, Kulosman H, Liu H. Self-dual codes over commutative Frobenius rings [J]. Finite Fields and Their Applications, 2010, 16(1): 14–26.

[7] Yildiz B, Karadeniz S. Self-dual codes over $F_2 + uF_2 + vF_2 + uvF_2$ [J]. J. Franklin Iust., 2010, 347: 1888–1894.

[8] Wood J. Duality for modules over finite rings and appplications to coding theory [J]. Amer. J. Math., 1999, 121: 555–575.

TWO STRUCTURAL METHODS OF SELF-DUAL CODES OVER THE RING $F_2 + uF_2 + vF_2$

HU Peng , LI Hui

(*School of Math. and Physics, Hubei Polytechnic University, Huangshi 435003, China*)

Abstract: In this paper, we study the self-dual codes over the ring $R = F_2 + uF_2 + vF_2$. According to the Gray map from R^n to F_2^{3n} and the fact that the Gray image of self-dual code C over the ring R is the self-dual code over F_2, we obtain the conclusion that there exists self-dual codes with any even length over R. Finally, we propose two structural methods of self-dual codes over the ring R.

Keywords: self-dual codes; Gray maps; double-circulant matrices

2010 MR Subject Classification: 94B05