环F_2+uF_2上线性码及其对偶码的二元象

余海峰[①②]　　朱士信[②]
[①](合肥学院数理系　合肥　230022)
[②](合肥工业大学应用数学系　合肥　230009)

摘　要　利用环 F_2+uF_2 上线性码 C 的生成矩阵给出了码 C 的对偶码 $C^{\perp}$ 及其 Gray 象 $\Phi(C)$ 的生成矩阵，证明了环 F_2+uF_2 上线性码及其对偶码的 Gray 象仍是对偶码，并由此给出了一个环 F_2+uF_2 上线性码为自对偶码的充要条件。

关键词　线性码，对偶码，生成矩阵，Gray 映射
中图分类号：TN911.2　　**文献标识码**：A　　**文章编号**：1009-5896(2006)11-2121-03

The Binary Images of the Linear Codes and Their Dual Codes Over F_2+uF_2

Yu Hai-feng[①②]　　Zhu Shi-xin[②]
[①](*Dept.of Mathematics, Hefei University, Hefei* 230022, *China*)
[②](*Dept.of Applied Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract　Based on the generator matrix of linear codes C over F_2+uF_2, the generator matrixes of the dual codes $C^{\perp}$ and the Gray images $\Phi(C)$ of the linear codes C are given, and the proposition that linear codes $\Phi(C^{\perp})$ are the dual codes of $\Phi(C)$ are showed. By using this proposition, the necessary and sufficient condition of a linear code over F_2+uF_2 which is self-dual is obtained.

Key words　Linear code, Dual code, Generator matrix, Gray map

1　引言

近年来，很多从事编码理论研究的学者将研究兴趣从有限域上编码理论转移到有限环上编码理论的研究上来[1-7]，特别是 Z_4 环上码的研究也日趋完善[1,7]。研究 Z_4 线性码的一个重点内容就是通过Gray映射将 Z_4 环上线性码与域 F_2 上的一些好码联系起来[1]，但 Z_4 环上Gray映射的一个遗憾之处是 Z_4 环上线性码在Gray映射下对应的象(本文中均简称为Gray象)不一定是二元线性码，而在含 4 个元素的环中，域 F_4 上虽然有类似于 Z_4 环上的Gray映射，且其上线性码的Gray象仍是二元线性码，但由其并不能得到二元好码，此时一种介于 Z_4 环与域 F_4 之间的四元环 $R=F_2+uF_2$ (其特征描述如第 2 节)被人们作为感兴趣的字母表加以引入，在文献[4−6]中，人们发现其上线性码的Gray象仍是二元线性码，而且作者们通过对该环上循环码及其自对偶码以及其Gray象的研究而得到一些好的二元线性码，并进一步发现其上循环码的解码也容易实现，因而对该环上线性码作进一步的研究是一件十分有意义的工作。

在文献[7]中，我们知道 Z_4 环上线性码及其对偶码的Gray象不一定是对偶码，而在环R上情形就不一样了，本文通过对环 R 上线性码与对偶码以及它们的Gray象的生成矩阵的研究，证明了环 R 上线性码及其对偶码的Gray象仍是域 F_2上的对偶码。

2005-03-08 收到, 2005-08-30 改回
安徽省自然科学基金(03042201)和安徽省教育厅自然科学基金项目资助课题

2　环 R 上线性码及其对偶码的生成矩阵

关于环 R 本身的结构在文献[4−6]中均有详细描述，它是指剩余类环 $F_2[u]/(u^2)$，其元素分别记为 $\{0,1,u,1+u\}$，若将 u 视为 Z_4 环上元素 2，$1+u$ 视为元素 3，则其乘法与 Z_4 环上乘法一致；若将 u 视为域 $F_4=\{0,1,\beta,\beta^2=1+\beta\}$ 中元素 β，$1+u$ 视为 β^2，则其加法与域 F_4 的加法一致，因而它分享了 Z_4 环与域 F_4 的一些良好性质，是介于 Z_4 环与域 F_4 之间的一类四元素环。

环 R 上的线性码 C 是指 R -模 R^n 的一加法子模。

若 $\forall X=(x_1,x_2,\cdots,x_n),Y=(y_1,y_2,\cdots,y_n)\in R^n$，定义 X 与 Y 的内积为

$$X\bullet Y=x_1y_1+x_2y_2+\cdots+x_ny_n \tag{1}$$

如果 $X\bullet Y=0$，则称 X 与 Y 正交。

设 C 是环 R 上长为 n 的线性码，令

$$C^{\perp}=\{X\in R^n \mid X\bullet Y=0,\forall Y\in C\} \tag{2}$$

则容易证明 $C^{\perp}$ 也是环 R 上长为 n 的线性码，称之为线性码 C 的对偶码。若环 R 上线性码 C 满足 $C\subseteq C^{\perp}$，则称 C 为环 R 上的自正交码；进一步若 $C=C^{\perp}$，则称 C 为环 R 上的自对偶码。

设 C_1,C_2 均是环 R 上长为 n 的线性码，若 C_1 通过坐标置换，必要时将码元 1 与 $1+u$ 互换，能得到码 C_2，则称 C_1 与 C_2 为环 R 上等价的线性码。

引理 1[6] R 上非零线性码 C 都等价于一个由

$$\begin{pmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B} \\ 0 & u\boldsymbol{I}_{k_2} & u\boldsymbol{D} \end{pmatrix} \tag{3}$$

所生成的线性码，其中 $\boldsymbol{A}$，$\boldsymbol{D}$ 为域 F_2 上矩阵，$\boldsymbol{B}$ 为环 R 上矩阵。此时也称码 C 的生成矩阵为式(3)，显然，码 C 中共包含 $4^{k_1}2^{k_2}$ 个码字。

证明 对码长 n 用数学归纳法。分两种不同情形:

(1) C 中有一个含码元 1 或码元 $1+u$ 的码字 c，则经过坐标变换(必要时将 1 或 $1+u$ 互换)可设该码字为 $c=(1,c_2,\cdots,c_n)$，令 $C'=\{(0,x_2,\cdots,x_n)\in C\}$，显然 C' 也是一线性码，且通过删除第 1 个坐标可将之看成一长为 $n-1$ 的线性码，由归纳假设知 C' 的生成矩阵为

$$\begin{pmatrix} 0 & \boldsymbol{I}_{k_1-1} & \boldsymbol{A}_1 & \boldsymbol{B}_1 \\ 0 & 0 & u\boldsymbol{I}_{k_2} & u\boldsymbol{D} \end{pmatrix}$$

其中 $\boldsymbol{A}_1$，$\boldsymbol{D}$ 为域 F_2 上矩阵，$\boldsymbol{B}_1$ 为环 R 上矩阵。则 C 有生成矩阵为

$$\begin{pmatrix} 1 & c_2\cdots c_{k_1} & c_{k_1+1}\cdots c_{k_1+k_2} & c_{k_1+k_2+1}\cdots c_n \\ 0 & \boldsymbol{I}_{k_1-1} & \boldsymbol{A}_1 & \boldsymbol{B}_1 \\ 0 & 0 & u\boldsymbol{I}_{k_2} & u\boldsymbol{D} \end{pmatrix}$$

将该矩阵的后 k_1+k_2-1 行的一个适当线性组合加到第 1 行可得:

$$\begin{pmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B} \\ 0 & u\boldsymbol{I}_{k_2} & u\boldsymbol{D} \end{pmatrix}$$

其中 $\boldsymbol{A}$，$\boldsymbol{D}$ 为域 F_2 上矩阵，$\boldsymbol{B}$ 为环 R 上矩阵，即此时 C 有形如式(3)的生矩阵。

(2) C 中所有码字均不含码元 1 与码元 $1+u$，则因 $C\neq\{0^n\}$，故 C 中一定有一个含码元 u 的码字 c，则经过坐标变换可设该码字为 $c=(u,uc_2,\cdots,uc_n)$。

类似地定义 $C'=\{(0,ux_2,\cdots,ux_n)\in C\}$，则通过删除第一个坐标也可将之看成一长为 $n-1$ 的线性码，由归纳假设知 C' 的生成矩阵为 $\begin{pmatrix} 0 & u\boldsymbol{I}_{k_2-1} & u\boldsymbol{D}_1 \end{pmatrix}$，其中 $\boldsymbol{D}_1$ 为域 F_2 上矩阵。

则 C 有生成矩阵为

$$\begin{pmatrix} u & uc_2\cdots uc_{k_2} & uc_{k_2+1}\cdots uc_n \\ 0 & u\boldsymbol{I}_{k_2-1} & u\boldsymbol{D}_1 \end{pmatrix}$$

将该矩阵的后 k_2-1 行的一个适当线性组合加到第一行可得：$\begin{pmatrix} u\boldsymbol{I}_{k_2} & u\boldsymbol{D} \end{pmatrix}$，其中 $\boldsymbol{D}$ 为域 F_2 上矩阵。此即为式(3)中当 $k_1=0$ 时的情形。综上所述，无论何种情形，C 的生成矩阵均为式(3)。 证毕

定理 1 若 C 为引理 1 所设的线性码，则其对偶码 $C^{\perp}$ 的生成矩阵为

$$\begin{pmatrix} \boldsymbol{B}^{\mathrm{T}}+\boldsymbol{D}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}} & \boldsymbol{D}^{\mathrm{T}} & \boldsymbol{I}_{n-k_1-k2} \\ u\boldsymbol{A}^{\mathrm{T}} & u\boldsymbol{I}_{k_2} & 0 \end{pmatrix} \tag{4}$$

且 $C^{\perp}$ 共包含 $4^{n-k_1-k_2}2^{k_2}$ 个码字。

证明 设 C_1 为 R 上的由式(4)所生成的线性码，则有 $C_1\subseteq C^{\perp}$；$\forall c=(c_1,c_2,\cdots,c_n)\in C^{\perp}$，将式(4)中前 $n-k_1-k_2$ 行的一个适当线性组合加到 c 上，则可得到 $C^{\perp}$ 中的一个码字 $c'=(c_1,\cdots,c_{k_1},c_{k_1+1},\cdots,c_{k_1+k_2},0,\cdots,0)$，且又因 c' 与式(3)中后 k_2 行正交，故 $c_{k_1+1},\cdots,c_{k_1+k_2}$ 只能取 0 或 u，将式(4)中后 k_2 行的一个适当线性组合加到 c' 上，则可得 $C^{\perp}$ 中的码字 $c''=(c_1,\cdots,c_{k_1},0,\cdots,0)$，因 c'' 与式(3)中前 k_1 行正交，故 $c_1=\cdots=c_{k_1}=0$，因此 $c\in C_1$，即 $C^{\perp}\subseteq C_1$，综上所述，即有 $C^{\perp}=C_1$。 证毕

由引理 1 与定理 1，我们即可得到:

推论 1 任一长度为 n 的环 R 上的自对偶码恰好包含 2^n 个码字。

3 环 R 上线性码及其对偶码的 Gray 象

对于环 R 上任一元素 λ，均可表示为 $\lambda=r(\lambda)+uq(\lambda)$，其中 $r(\lambda),q(\lambda)\in F_2$，则可定义从 R 到 F_2^2 的 Gray 映射：$\Phi(\lambda)=(q(\lambda),q(\lambda)+r(\lambda))$，若令 $s(\lambda)=q(\lambda)+r(\lambda)$，则有 $\Phi(\lambda)=(q(\lambda),s(\lambda))$。

可自然延伸至 R^n 上向量 $\boldsymbol{X}$ 及 R 上的矩阵 $\boldsymbol{M}$ 的 Gray 映射，即若设 $X=(x_1,x_2,\cdots,x_n)\in R$，其中 $x_i=r_i+uq_i$，$i=1,2,\cdots,n$，定义 $r(X)=(r_1,r_2,\cdots,r_n)$，$q(X)=(q_1,q_2,\cdots,q_n)$，则有 $\Phi(X)=(q(X),q(X)+r(X))$。

若设 R 上的矩阵 $\boldsymbol{M}=(a_{ij})_{m\times n}$，其中 $a_{ij}=r_{ij}+uq_{ij}$，定义 $r(\boldsymbol{M})=(r_{ij})$，$q(\boldsymbol{M})=(q_{ij})$，则有 R 上的矩阵 $\boldsymbol{M}$ 的 Gray 映射：$\Phi(\boldsymbol{M})=(q(\boldsymbol{M}),q(\boldsymbol{M})+r(M))$，若设 $s(\boldsymbol{M})=r(\boldsymbol{M})+q(\boldsymbol{M})$，则 $\Phi(\boldsymbol{M})=(q(\boldsymbol{M}),s(\boldsymbol{M}))$。

引理 2[4] 若 C 为 R 上的线性码，则 $\Phi(C)$ 为域 F_2 上的线性码。

定理 2 若 C 为 R 上长为 n 的线性码，其生成矩阵如式(3)所示，则 $\Phi(C)$ 的生成矩阵为

$$\begin{pmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{r}(\boldsymbol{B}) & \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{r}(\boldsymbol{B}) \\ 0 & \boldsymbol{I}_{k_2} & \boldsymbol{D} & 0 & \boldsymbol{I}_{k_2} & \boldsymbol{D} \\ 0 & 0 & \boldsymbol{q}(\boldsymbol{B}) & \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{s}(\boldsymbol{B}) \end{pmatrix} \tag{5}$$

即 $\Phi(C)$ 为域 F_2 上的 $[2n,2k_1+k_2]$ 线性码。

证明 由引理 2 知，$\Phi(C)$ 为域 F_2 上长为 $2n$ 的线性码，而 $\Phi(C)$ 是 R 上矩阵

$$\begin{pmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B} \\ u\boldsymbol{I}_{k_1} & u\boldsymbol{A} & u\boldsymbol{B} \\ (1+u)\boldsymbol{I}_{k_1} & (1+u)\boldsymbol{A} & (1+u)\boldsymbol{B} \\ 0 & u\boldsymbol{I}_{k_2} & u\boldsymbol{D} \end{pmatrix}$$

的行向量的 Gray 象所生成的，因 $\boldsymbol{A}$，$\boldsymbol{D}$ 均是域 F_2 上矩阵，$\boldsymbol{B}$ 为 R 上矩阵，则由上面 R 上的矩阵的 Gray 映射定义，

类似于文献[7]中证明 Z_4 环上线性码 C 的 Gray 象 $\Phi(C)$ (当 $\Phi(C)$ 为线性码时)的生成矩阵的方法可证得 $\Phi(C)$ 的生成矩阵为式(5)。　　证毕

定理 3　设 C 为 R 上长为 n 的线性码，$C^{\perp}$ 为其对偶码，则 $\Phi(C)$ 与 $\Phi(C^{\perp})$ 也为域 F_2 上的对偶码。

证明　由引理 2 知 $\Phi(C)$ 与 $\Phi(C^{\perp})$ 均为域 F_2 上的线性码，若记 $\Phi(C)$ 的对偶码为 $(\Phi(C))^{\perp}$，下证 $\Phi(C^{\perp})=(\Phi(C))^{\perp}$：$\forall c_1=r_1+uq_1\in C$，$c_2=r_2+uq_2\in C^{\perp}$，则因 C 与 $C^{\perp}$ 互为对偶码，故 $c_1\bullet c_2=0$ 即有 $r_1\bullet r_2=0, r_1\bullet q_2+r_2\bullet q_1=0$，故 $\Phi(c_1)\bullet\Phi(c_2)=(q_1,q_1+r_1)\cdot(q_2,q_2+r_2)=0$，又因为 Gray 映射 Φ 为双射，故有 $\Phi(C^{\perp})\subseteq(\Phi(C))^{\perp}$。

另一方面，由定理 2 知，$\Phi(C)$ 为域 F_2 上的 $[2n,2k_1+k_2]$ 线性码，故 $(\Phi(C))^{\perp}$ 为域 F_2 上的 $[2n,2n-2k_1-k_2]$ 线性码，故 $\left|(\Phi(C))^{\perp}\right|=2^{2n-2k_1-k_2}$，由于 Φ 为双射，故 $\left|\Phi(C^{\perp})\right|=\left|C^{\perp}\right|=2^{2n-2k_1-k_2}$,即有 $\left|\Phi(C^{\perp})\right|=\left|(\Phi(C))^{\perp}\right|$。

综上即有 $\Phi(C^{\perp})=(\Phi(C))^{\perp}$。　　证毕

推论 2　码 C 为 R 上自对偶码当且仅当 $\Phi(C)$ 为域 F_2 上自对偶码。

证明　设 $C^{\perp}$ 为 R 上码 C 的对偶码，则由定理 3 知 $\Phi(C^{\perp})$ 为 $\Phi(C)$ 的对偶码，由于 Φ 为双射，故由自对偶码的定义知该命题成立。　　证毕

定理 4 生成矩阵为式(3)的线性码 C 为 R 上自对偶码的充要条件是如下条件同时满足：

(1) $2k_1+k_2=n$；

(2)矩阵 $\boldsymbol{A}$ 的各行重量与矩阵 $\boldsymbol{r}(\boldsymbol{B})$ 对应的行重量之和皆为奇数；

(3)矩阵 $(\boldsymbol{q}(\boldsymbol{B})\ \ \boldsymbol{I}_{k_1}\ \ \boldsymbol{A}\ \ \boldsymbol{s}(\boldsymbol{B}))$ 的各行向量彼此正交，且该矩阵的各行向量与矩阵

$$\begin{pmatrix} \boldsymbol{r}(\boldsymbol{B}) & \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{r}(\boldsymbol{B}) \\ \boldsymbol{D} & 0 & \boldsymbol{I}_{k_2} & \boldsymbol{D} \end{pmatrix}$$

的各行向量正交。

证明　由定理 2 知，$\Phi(C)$ 为域 F_2 上的 $[2n,2k_1+k_2]$ 线性码，由文献[8]知：$\Phi(C)$ 为域 F_2 上自对偶码的充要条件是：$2k_1+k_2=n$，且 $\Phi(C)$ 的生成矩阵式(5)的各行重量皆为偶数及各行向量彼此正交，而由式(5)的特点知当且仅当满足本定理中(1)、(2)、(3)时，$\Phi(C)$ 为域 F_2 上自对偶码，再由推论知本定理成立。　　证毕

类似该定理证明方法，我们也可得到如下定理：

定理 5 (1)生成矩阵为 $(u\boldsymbol{I}_{k_2}\ \ u\boldsymbol{D})$ (即当 $k_1=0$ 时)的线性码 C 一定是自正交码；

(2)生成矩阵为 $(u\boldsymbol{I}_{k_2}\ \ u\boldsymbol{D})$ 的线性码 C 是自对偶码的充要条件是 $n=k_2$，其中 n 是指码长。

证明　(1)若线性码 C 的生成矩阵为 $(u\boldsymbol{I}_{k_2}\ \ u\boldsymbol{D})$，则 $\Phi(C)$ 的生成矩阵 $(\boldsymbol{I}_{k_2}\ \ \boldsymbol{D}\ \ \boldsymbol{I}_{k_2}\ \ \boldsymbol{D})$。故 $\Phi(C)$ 为域 F_2 上自正交码，则由于 Φ 为双射，故码 C 是 R 上的自正交码。

(2)由(1)及定理 4 显然可得。　　证毕

4　结束语

有限环上的编码理论的研究是近年来人们很感兴趣的一个热点问题，对其的研究可以对域上编码有更清楚的认识。而环 F_2+uF_2 由于自身特殊的结构，对其上线性码的更多研究必将极大地丰富环上的编码理论的发展。

参 考 文 献

[1] Hammons R, Kumar P V, Calderbank A R, Sloane N J A, Sole P. The Z_4-linearity of Kerdock, Preparata, Goethals, related codes[J]. *IEEE Trans. Inform.Theory*,1994, 40(2): 301−319.

[2] Carlet C. z_{2^k} -Linear codes[J]. *IEEE Trans. Inform. Theory*, 1998, 44(4): 1543−1547.

[3] 朱士信. z_k 线性码的对称形式的 MacWillmas 恒等式. 电子与信息学报, 2003, 25(7): 901−906.

[4] Bonnecaze A, Udaya P. Cyclic codes and self-dual codes over F_2+uF_2 , *IEEE Trans. Inform. Theory*, 1999, 45(4): 1250−1255.

[5] Udaya P, Bonnecaze A. Decoding of cyclic codes over F_2+uF_2 [J]. *IEEE Trans. Inform.Theory*, 1999, 45(6): 2148−2157.

[6] Dougherty S T, Gaborit P, Harad M, *et al*.. Type II codes over F_2+uF_2 [J]. *IEEE Trans. Inform. Theory*, 1999, 45(1): 32−45.

[7] Zhe-xian Wan, Quaternay code[M]. Singapore: World Scientific, 1997, Chapter 1,3.

[8] 肖国镇. 卿斯汉 《编码理论》. 北京: 国防工业出版社, 1993: 63−70.

余海峰：　男，1975 年生，硕士，讲师，主要从事代数编码方向的研究.

朱士信：　男，1962 年生，博士，教授，一直从事移位寄存器序列、代数编码等方面的教学和研究工作.