Vol. 36 (2016)
No. 1

数 学 杂 志
J. of Math. (PRC)

$F_2 + vF_2$ 上的循环码

张光辉, 李良辰
(洛阳师范学院数学科学学院, 河南 洛阳 471022)

摘 要: 本文研究了环 $F_2 + vF_2$ 上的循环码. 利用标准形生成元集刻画了环 $F_2 + vF_2$ 上的循环码的代数结构, 证明了环 $F_2 + vF_2$ 上的每一个非零的循环码均有唯一的标准形生成元集, 进而得到了每一个循环码均是由一个多项式生成的.

关 键 词: 环 $F_2 + vF_2$; 循环码; 标准形生成元集
MR(2010) **主题分类号**: 94B05; 94B15 **中 图 分 类 号**: O157.4
文 献 标 识 码: A **文 章 编 号**: 0255-7797(2016)01-0117-07

1 引言

有限环上的线性码的研究始于二十世纪七十年代 [2,3]. 在文献 [7] 中, Hammons 等证明了某些高效的二元非线性码, 如 Kerdock 码、Delsarte-Goethals 码都可以看做是 Z_4 - 线性码的 Gray 像, 这使得有限交换环上的码受到广泛关注, 从而环上的码的研究成为编码理论研究的一个新的方向. 我们知道, 除了四元域 F_4 和模 4 的剩余类环 Z_4 之外, 还有两个四元素环: $F_2 + uF_2 = \{0, 1, u, 1 + u\}$, 这里 $u^2 = 0$; $F_2 + vF_2 = \{0, 1, v, 1 + v\}$, 这里 $v^2 = v$. 研究这四个四元素环上的线性码的结构是一个有趣的课题. 对 F_4 上的线性码结构的研究, 已有很多相关文献, 并得出了很多结果; 对 Z_4 上的线性码 (即四元码) 也有很多相关研究工作 (如文献 [10] 等); 环 $F_2 + uF_2$ 上线性码的研究见文献 [1, 4, 8]. 与前三个不一样的是, 环 $F_2 + vF_2$ 不是链环. 但是, 文献 [9] 中的结果表明有限 Frobenius 环也适合于编码, 这使得非链环上的线性码也开始受到关注.

近年来, 一些学者开始研究非链环 $F_p + vF_p$ 上的线性码, 这里 $v^2 = v$, p 是一个素数. 在文献 [11] 里, 朱士信等研究了 $F_2 + vF_2$ 上的线性码和循环码; 在文献 [5], Cengellenmis 等研究了环 $A_k = F_2[v_1, v_2, \cdots, v_k]/\langle v_i^2 = v_i, v_i v_j = v_j v_i\rangle, 1 \le i, j \le k$ 上的线性码, 而这一类环是环 $F_2 + vF_2$ 的推广; 在文献 [12] 里, 朱士信等研究了 $F_p + vF_p$ 上的 $(1 - 2v)$ - 常循环码, 这里 p 是一个奇素数, 确定了 $F_p + vF_p$ 上的 $(1 - 2v)$ - 常循环码的 Gray 像和它们的代数结构.

本文主要利用标准形生成元集来刻画 $F_2 + vF_2$ 上的循环码及其对偶码的代数结构. 我们先根据环 $F_2 + vF_2$ 上的线性码的生成矩阵来探讨其对偶码的生成矩阵; 再根据标准形生成元集来刻画 $F_2 + vF_2$ 上的循环码及其对偶码的代数结构.

2 预备知识

*收稿日期: 2013-06-26 接收日期: 2013-09-23
基金项目: 国家自然科学基金资助 (11171370; 11301254); 河南省基础与前沿技术研究计划项目 (132300410313); 河南省教育厅科学技术研究重点项目 (13A110800).
作者简介: 张光辉 (1973–), 男, 河南叶县, 副教授, 主要研究方向: 代数编码理论.

设 R 是一个有单位元的有限交换环. 环 R 上长为 n 的线性码 C 就是 R^n 的一个 R - 子模, 这里 $R^n = \{(x_1, x_2, \cdots, x_n) | x_i \in R\}$. 对任意的 $x = (x_1, x_2, \cdots, x_n), y = (y_1, y_2, \cdots, y_n) \in R^n$, 我们定义 x, y 的内积: $\langle x, y\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n$. 如果 C 是环 R 上长为 n 的线性码, 那么定义 $C^\perp = \{x \in R^n | \langle x, c\rangle = 0, \forall c \in C\}$, 则 $C^\perp$ 是环 R 上长为 n 的线性码, 称之为 C 的对偶码. 如果 $C \subseteq C^\perp$, 称线性码 C 是自正交的; 如果 $C = C^\perp$, 称线性码 C 是自对偶的. 文献 [9] 证明了对有限 Frobenius 环 R 上的任一线性码 C, 均有 $|C||C^\perp| = |R|^n$.

环 $F_2 + vF_2 = \{0, 1, v, 1 + v\}$, 这里 $v^2 = v$. 易知环 $F_2 + vF_2$ 等同于商环 $F_2[v]/\langle v^2 + v\rangle$; 其中的每一个元素均可以表示成 $c = a + vb$ 的形式, 这里 $a, b \in F_2$. 以后总假设 $R = F_2 + vF_2$, 则环 R 是一个半局部环, 仅有的两个极大理想是 $\langle v\rangle$ 和 $\langle 1 + v\rangle$, 相应的剩余类域为 $R/\langle v\rangle = R/\langle 1 + v\rangle = F_2$. 这样环 R 到 $R/\langle 1 + v\rangle = F_2$ 有一个自然同态, 记做 “α”: $R \longrightarrow R/\langle 1 + v\rangle = F_2 : x + vy \longmapsto x + y$; 同样地, 环 R 到 $R/\langle v\rangle = F_2$ 也有一个自然同态, 记做 “β”: $R \longrightarrow R/\langle v\rangle = F_2 : x + vy \longmapsto x$. 自然地, 可以将这两个同态分别扩充为 $R^n \longrightarrow F_2^n$ 的环同态, 仍分别记做 “α” 和 “β”. 为方便起见, 我们以后用 r^α 和 r^β 分别表示 R^n 中的元素 r 在 α 和 β 之下的像. 设 $A \subseteq R^n$, 用 A^α 和 A^β 分别表示集合 A 中的所有元素在 α 和 β 之下的像构成的集合.

环 R 到环 $F_2 \oplus F_2$ 有一个 Gray 映射 ϕ 如下: $\phi(c) = (a, a + b)$, 这里 $c = a + vb, a, b \in F_2$, 这样 ϕ 是一个环同构. 此环同构表明环 R 是一个有限交换的主理想环, 见文献 [6, 命题 2.7], 也表明环 R 是一个有限 Frobenius 环.

设 C 是环 R 上长为 n 的线性码. 类似于文献 [10] 中命题 1.1 的证明, 线性码 C 有一个如下的生成矩阵 G:

$$\begin{pmatrix} I_{k_0} & A & B & D_1 + vD_2 \\ 0 & vI_{k_1} & 0 & vC_1 \\ 0 & 0 & (1+v)I_{k_2} & (1+v)E \end{pmatrix},$$

其中 k_0, k_1, k_2 为非负整数; $I_{k_0}, I_{k_1}, I_{k_2}$ 分别是阶为 k_0, k_1, k_2 的单位矩阵; A, B, C_1, D_1, D_2 和 E 均是 $(0, 1)$ 矩阵. 这样线性码 C 的码字个数 $|C| = 4^{k_0}2^{k_1}2^{k_2}$.

设 C 是环 R 上长为 n 的线性码. 定义集合 C_1, C_2 如下:

$$\begin{aligned} C_1 &= \{x \in F_2^n | x + vy \in C, \text{存在某个 } y \in F_2^n\}; \\ C_2 &= \{x + y \in F_2^n | x + vy \in C\}, \end{aligned}$$

则 C_1, C_2 是二元线性码, 并且 C_1, C_2 的生成矩阵分别为

$$G_1 = \begin{pmatrix} I_{k_0} & A & B & D_1 \\ 0 & 0 & I_{k_2} & E \end{pmatrix}; \quad G_2 = \begin{pmatrix} I_{k_0} & A & B & D_1 + D_2 \\ 0 & I_{k_1} & 0 & C_1 \end{pmatrix}.$$

由此可知 $k_0 + k_2 = \dim C_1, k_0 + k_1 = \dim C_2$. 因此 $k_0 + k_2, k_0 + k_1$ 与环 R 上的线性码 C 的生成矩阵的选取无关. 由于线性码 C 的码字个数 $|C| = 4^{k_0}2^{k_1}2^{k_2} = 2^{(k_0+k_1)+(k_0+k_2)}$, 所以码字个数 $|C|$ 也与线性码 C 的生成矩阵的选取无关.

设 C 是环 R 上长为 n 的线性码, $a \in R$. 记 $(C : a) = \{x \in R^n | ax \in C\}$, 则 $(C : a)$ 也是环 R 上长为 n 的线性码. 注意到环 R^n 中的每一个元素 c 均可以表示成 $c = a + vb$ 的形式, 这里 $a, b \in F_2^n$. 这样有

引理 2.1 符号如上, 则 (1) $(C:v)^\alpha=C_2$; (2) $(C:(1+v))^\beta=C_1$.

证 (1) 首先证明 $(C:v)^\alpha\subseteq C_2$. 任取 $y\in(C:v)^\alpha$, 则存在 $x\in(C:v)$, 使得 $y=x^\alpha$. 设 $x=r+vq$, 这里 $r,q\in F_2^n$, 则 $x^\alpha=r+q$. 由 $vx\in C$, 得 $v(r+q)\in C$, 故 $r+q\in C_2$. 因此 $y=x^\alpha=r+q\in C_2$. 由此可得 $(C:v)^\alpha\subseteq C_2$.

再证明 $(C:v)^\alpha\supseteq C_2$. 任取 $z\in C_2$, 则存在 $x+vy\in C$, 使得 $z=x+y$. 既然 $x+vy\in C$, 则 $v(x+y)=v(x+vy)\in C$, 即得 $x+y\in(C:v)$. 故有 $z=x+y=(x+y)^\alpha\in(C:v)^\alpha$, 即得 $(C:v)^\alpha\supseteq C_2$. 因此 $(C:v)^\alpha=C_2$.

(2) 先证明 $(C:(1+v))^\beta\subseteq C_1$. 任取 $y\in(C:(1+v))^\beta$, 则存在 $z\in(C:(1+v))$, 使得 $y=z^\beta$. 设 $z=r+vq$, 这里 $r,q\in F_2^n$, 则 $z^\beta=r$. 由 $(1+v)z\in C$, 得

$$r+vr=(1+v)r=(1+v)(r+vq)=(1+v)z\in C,$$

故 $r\in C_1$. 因此 $y=z^\beta=r\in C_1$. 由此可得 $(C:(1+v))^\beta\subseteq C_1$.

再证明 $(C:(1+v))^\beta\supseteq C_1$. 任取 $r\in C_1$, 则存在 $q\in F_2^n$, 使得 $r+vq\in C$. 因为 $(1+v)r=(1+v)(r+vq)\in C$, 所以 $r\in(C:(1+v))$. 因此 $r=r^\beta\in(C:(1+v))^\beta$.

综上所述, $(C:(1+v))^\beta=C_1$.

3 环 F_2+vF_2 上的循环码

环 R 上的线性码 C 称为一个循环码, 如果对任意的 $(c_0,c_1,\cdots,c_{n-1})\in C$, 均有 $(c_{n-1},c_0,\cdots,c_{n-2})\in C$. 记 $R_n=R[x]/\langle x^n-1\rangle$. 这样把线性码 C 中的元素 $c=(c_0,c_1,\cdots,c_{n-1})\in C$ 与 R_n 中的元素 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 等同. 因此线性码 C 是一个长为 n 的循环码当且仅当 C 是环 R_n 的一个理想. 我们再回顾一下二元域 F_2 上的循环码. 每一个二元域上长为 n 的循环码 C 就是 $F_2[x]/\langle x^n-1\rangle$ 的一个主理想. 每一个循环码 C 中均有一个首一的次数最低的多项式 $g(x)$, 使得 $C=\langle g(x)\rangle$, 并且 $g(x)|(x^n-1)$, 称 $g(x)$ 为循环码 C 的生成多项式. 设 $g(x)$ 是环 R_n 中的一个首一多项式, $g(x)$ 生成循环码 C, 则 $g(x)$ 是循环码 C 的生成多项式当且仅当 $g(x)|(x^n-1)$.

设 $f_1(x),f_2(x),\cdots,f_n(x)\in R_n$, 记由 $f_1(x),f_2(x),\cdots,f_n(x)$ 所生成的理想为

$$\langle f_1(x),f_2(x),\cdots,f_n(x)\rangle.$$

设 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1},a_i\in R,i=0,1,\cdots,n-1$, 记

$$f(x)^\alpha=a_0^\alpha+a_1^\alpha x+\cdots+a_{n-1}^\alpha x^{n-1};\ \ f(x)^\beta=a_0^\beta+a_1^\beta x+\cdots+a_{n-1}^\beta x^{n-1}.$$

我们用 M^T 表示矩阵 M 的转置矩阵.

定理 3.1 设 C 是环 R 上长为 n 的线性码, 其生成矩阵 G 如下:

$$G=\begin{pmatrix} I_{k_0} & A & B & D_1+vD_2\\ 0 & vI_{k_1} & 0 & vC_1\\ 0 & 0 & (1+v)I_{k_2} & (1+v)E\end{pmatrix},$$

其中 k_0,k_1,k_2 都为非负整数; I_{k_0},I_{k_1},I_{k_2} 分别是阶为 k_0,k_1,k_2 的单位矩阵; A,B,C_1,D_1,D_2 和 E 均是 $(0,1)$ 矩阵, 则

(1) 矩阵

$$H=\begin{pmatrix} E^TB^T+C_1^TA^T+(D_1+vD_2)^T & C_1^T & E^T & I_{n-k} \\ vB^T & 0 & vI_{k_2} & 0 \\ (1+v)A^T & (1+v)I_{k_1} & 0 & 0 \end{pmatrix}$$

是线性码 C 的对偶码 $C^\perp$ 的生成矩阵, 即为线性码 C 的校验矩阵, 这里 $k=k_0+k_1+k_2$.

(2) $(C^\perp:v)^\alpha=((C:v)^\alpha)^\perp$; $((C^\perp:(1+v))^\beta=((C:(1+v))^\beta)^\perp$.

证 (1) 设 D 是由矩阵 H 所生成的线性码. 可以直接验证 HG^T=0, 所以 $D\subseteq C^\perp$. 由于环 R 是一个有限 Frobenius 环, 那么 $|C||C^\perp|=|R|^n$, 即得

$$|C^\perp|=\frac{|R|^n}{|C|}=\frac{4^n}{4^{k_0}2^{k_1}2^{k_2}}=4^{n-k_0}2^{-k_1}2^{-k_2}.$$

再注意到 $|D|=4^{n-k}2^{k_1}2^{k_2}=4^{n-k_0}2^{-k_1}2^{-k_2}$, 所以 $|D|=|C^\perp|$, 因此 $D=C^\perp$.

(2) 首先证明 $(C^\perp:v)^\alpha\subseteq((C:v)^\alpha)^\perp$. 任取 $x\in(C^\perp:v), y\in(C:v)$, 则有 $vx\in C^\perp, vy\in C$, 故 $(vx)(vy)^T=0$, 即 $v(xy^T)=0$, 因此 $xy^T\in(1+v)R$, 即得 $x^\alpha(y^\alpha)^T=0$, 此式表明 $(C^\perp:v)^\alpha\subseteq((C:v)^\alpha)^\perp$. 又根据定理 3.1(1) 和引理 2.1, 有

$$\begin{aligned}&\dim(C^\perp:v)^\alpha=n-k+k_2=n-(k_0+k_1),\\ &\dim((C:v)^\alpha)^\perp=n-\dim((C:v)^\alpha)=n-(k_0+k_1),\end{aligned}$$

即得 $\dim(C^\perp:v)^\alpha=\dim((C:v)^\alpha)^\perp$. 因此 $(C^\perp:v)^\alpha=((C:v)^\alpha)^\perp$.

另一个等式同理可证.

推论 3.2 符号如上. 设 C 是环 R 上长为 n 的线性码, 其生成矩阵为矩阵 G, 则 C 是自对偶的当且仅当下面两个条件成立:

(i) C 是自正交的;

(ii) $n=2(k_0+k_1), k_1=k_2$.

证 ($\Longrightarrow$) 若 C 是自对偶的, 则 (i) 显然成立. 既然 $C=C^\perp$, 则

$$k_0+k_1=n-k+k_2, k_0+k_2=n-k+k_1.$$

因此 $n=2(k_0+k_1)=2(k_0+k_2)$, 即得 $k_1=k_2$, 故 (ii) 成立.

($\Longleftarrow$) 由于 $n=2(k_0+k_1), k_1=k_2$, 则

$$|C|=4^{k_0}2^{k_1}2^{k_2}=4^{k_0+k_1}, |C^\perp|=4^{n-k}2^{k_1}2^{k_2}=4^{k_0+k_1}.$$

又 $C\subseteq C^\perp$, 故 $C=C^\perp$, 即 C 是自对偶的.

定义 3.3 设 $g_i(x)\in F_2[x], i=1,2$. 称集合 $S=\{vg_1(x),(1+v)g_2(x)\}$ 是 C 的一个标准形生成元集, 如果 $C=\langle vg_1(x),(1+v)g_2(x)\rangle$, 并且 $g_1(x), g_2(x)$ 满足条件: 对任一个 $i\in\{1,2\}$, 若 $g_i(x)$ 不为零, 则 $g_i(x)$ 是 $F_2[x]$ 中的首一多项式, 并且 $g_i(x)|(x^n-1)$.

引理 3.4 如果集合 $S=\{vg_1(x),(1+v)g_2(x)\}$ 是循环码 $C=\langle vg_1(x),(1+v)g_2(x)\rangle$ 的一个标准形的生成元集, 则

$$(C:v)^\alpha=\langle g_1(x)\rangle;\quad (C:(1+v))^\beta=\langle g_2(x)\rangle,$$

即 $g_1(x), g_2(x)$ 分别是循环码 $(C:v)^\alpha$ 和 $(C:(1+v))^\beta$ 的生成多项式.

证 (1) 因为 $vg_1(x)\in C$, 所以 $g_1(x)\in(C:v)$, 故 $g_1(x)=g_1(x)^\alpha\in(C:v)^\alpha$, 即得 $\langle g_1(x)\rangle\subseteq(C:v)^\alpha$. 再任取 $f(x)\in(C:v)$. 注意到 $vf(x)\in C$, 可设

$$vf(x)=h_1(x)vg_1(x)+h_2(x)(1+v)g_2(x),$$

这里 $h_1(x),h_2(x)\in R_n$. 令

$$f(x)=f_1(x)+(1+v)f_2(x), h_1(x)=h_{11}(x)+(1+v)h_{12}(x), h_2(x)=h_{21}(x)+vh_{22}(x),$$

这里 $f_1(x),f_2(x),h_{11}(x),h_{12}(x),h_{21}(x),h_{22}(x)\in F_2[x]$. 因此

$$\begin{aligned} vf(x) &= vf_1(x)\\ &= [h_{11}(x)+(1+v)h_{12}(x)]vg_1(x)+[h_{21}(x)+vh_{22}(x)](1+v)g_2(x)\\ &= vh_{11}(x)g_1(x)+(1+v)h_{21}(x)g_2(x)\\ &= v(h_{11}(x)g_1(x)+h_{21}(x)g_2(x))+h_{21}(x)g_2(x). \end{aligned}$$

即得 $v[f_1(x)+h_{11}(x)g_1(x)+h_{21}(x)g_2(x)]=h_{21}(x)g_2(x)$, 故有 $h_{21}(x)g_2(x)=0$ 且 $f_1(x)=h_{11}(x)g_1(x)+h_{21}(x)g_2(x)=h_{11}(x)g_1(x)$. 因此 $f(x)^\alpha=f_1(x)=h_{11}(x)g_1(x)\in\langle g_1(x)\rangle$, 此式表明 $\langle g_1(x)\rangle\supseteq(C:v)^\alpha$. 由此得到 $(C:v)^\alpha=\langle g_1(x)\rangle$.

(2) 因为 $(1+v)g_2(x)\in C$, 所以 $g_2(x)\in(C:(1+v))$, 故 $g_2(x)=g_2(x)^\beta\in(C:(1+v))^\beta$, 即得 $\langle g_2(x)\rangle\subseteq(C:(1+v))^\beta$. 再任取 $f(x)\in(C:(1+v))$. 注意到 $(1+v)f(x)\in C$, 可设 $(1+v)f(x)=u_1(x)vg_1(x)+u_2(x)(1+v)g_2(x)$, 这里 $u_1(x),u_2(x)\in R_n$. 令

$$f(x)=f_1(x)+vf_2(x), u_1(x)=u_{11}(x)+(1+v)u_{12}(x), u_2(x)=u_{21}(x)+vu_{22}(x),$$

这里 $f_1(x),f_2(x),u_{11}(x),u_{12}(x),u_{21}(x),u_{22}(x)\in F_2[x]$. 因此

$$\begin{aligned} (1+v)f(x) &= (1+v)f_1(x)\\ &= [u_{11}(x)+(1+v)u_{12}(x)]vg_1(x)\\ &\quad +[u_{21}(x)+vu_{22}(x)](1+v)g_2(x)\\ &= vu_{11}(x)g_1(x)+(1+v)u_{21}(x)g_2(x)\\ &= v[u_{11}(x)g_1(x)+u_{21}(x)g_2(x)]+u_{21}(x)g_2(x), \end{aligned}$$

即得

$$v[f_1(x)+u_{11}(x)g_1(x)+u_{21}(x)g_2(x)]=f_1(x)+u_{21}(x)g_2(x),$$

故有 $f_1(x)+u_{21}(x)g_2(x)=0$, 即得 $f_1(x)=u_{21}(x)g_2(x)$. 因此

$$f(x)^\beta=f_1(x)=u_{21}(x)g_2(x)\in\langle g_2(x)\rangle,$$

此式表明 $\langle g_2(x)\rangle\supseteq(C:(1+v))^\beta$. 由此得到 $(C:(1+v))^\beta=\langle g_2(x)\rangle$.

定理 3.5 设 C 是环 R 上一个非零的循环码, 则 C 有唯一的标准形生成元集.

证 既然 C 是环 R 上的循环码, 则 $(C:v)^\alpha$ 和 $(C:(1+v))^\beta$ 都是二元循环码. 已知 $C\neq 0$, 由引理 2.1 可知 $(C:v)^\alpha$ 和 $(C:(1+v))^\beta$ 不全为零. 不妨假设 $(C:v)^\alpha$ 和 $(C:(1+v))^\beta$ 全不为零. 令 $(C:v)^\alpha=\langle g_1(x)\rangle;(C:(1+v))^\beta=\langle g_2(x)\rangle$, 这里 $g_1(x),g_2(x)$ 分别是 $(C:v)^\alpha$ 和 $(C:(1+v))^\beta$ 的生成多项式. 我们断言 $C=\langle vg_1(x),(1+v)g_2(x)\rangle$.

取 $f(x)\in(C:v)$, 使得 $f(x)^\alpha=g_1(x)$. 令 $f(x)=g_1(x)+(1+v)f_1(x),f_1(x)\in F_2[x]$. 由 $vf(x)\in C$ 得 $vg_1(x)\in C$; 同理可证 $(1+v)g_2(x)\in C$, 故 $C\supseteq\langle vg_1(x),(1+v)g_2(x)\rangle$. 再任取 $f(x)\in C$, 则 $vf(x)\in C,(1+v)f(x)\in C$. 设

$$f(x)=f_1(x)+(1+v)f_2(x)=(f_1(x)+f_2(x))+vf_2(x),$$

这里 $f_1(x),f_2(x)\in F_2[x]$. 既然 $vf(x)\in C$, 那么 $f(x)\in(C:v)$, 进而得

$$f(x)^\alpha\in(C:v)^\alpha=\langle g_1(x)\rangle,$$

即 $f_1(x)\in\langle g_1(x)\rangle$. 令 $f_1(x)=u_1(x)g_1(x),u_1(x)\in F_2[x]$. 同样地, 由于 $(1+v)f(x)\in C$, 则 $f(x)\in(C:(1+v))$, 进而得 $f(x)^\beta\in(C:(1+v))^\beta=\langle g_2(x)\rangle$, 即 $f_1(x)+f_2(x)\in\langle g_2(x)\rangle$. 令

$$f_1(x)+f_2(x)=u_2(x)g_2(x),\ \ u_2(x)\in F_2[x],$$

则 $f_2(x)=u_1(x)g_1(x)+u_2(x)g_2(x)$. 因此

$$\begin{aligned}f(x)&=f_1(x)+(1+v)f_2(x)\\&=(f_1(x)+f_2(x))+vf_2(x)\\&=u_2(x)g_2(x)+v[u_1(x)g_1(x)+u_2(x)g_2(x)]\\&=u_1(x)(vg_1(x))+u_2(x)((1+v)g_2(x)).\end{aligned}$$

此式表明 $C\subseteq\langle vg_1(x),(1+v)g_2(x)\rangle$. 因此 $C=\langle vg_1(x),(1+v)g_2(x)\rangle$.

如果 $(C:v)^\alpha=0$, 那么取 $g_1(x)=0$; 如果 $(C:(1+v))^\beta=0$, 那么取 $g_2(x)=0$.

根据二元域上的循环码的生成多项式的唯一性, 由引理 3.4 可得环 R 上的非零循环码 C 的标准形生成元集是唯一的.

推论 3.6 $R_n=R[x]/\langle x^n-1\rangle$ 是主理想环.

证 设 C 是 R_n 的任一个理想. 由定理 3.5 可令 $C=\langle vg_1(x),(1+v)g_2(x)\rangle$, 这里 $\{vg_1(x),(1+v)g_2(x)\}$ 是 C 的标准形生成元集. 再注意到

$$vg_1(x)=v[vg_1(x)+(1+v)g_2(x)];(1+v)g_2(x)=(1+v)[vg_1(x)+(1+v)g_2(x)].$$

即得 $C=\langle vg_1(x)+(1+v)g_2(x)\rangle$, 故 $R_n=R[x]/\langle x^n-1\rangle$ 是主理想环.

下面是一个大家熟知的结果:

命题 3.7 设 C 是环 R 上的一个循环码, 则 C 的对偶码 $C^\perp$ 也是循环码. 设

$$\begin{aligned}&g_1(x)h_1(x)=x^n-1,g_2(x)h_2(x)=x^n-1;\\&\bar{h}_1(x)=x^{\deg(h_1(x))}h_1(\frac{1}{x}),\bar{h}_2(x)=x^{\deg(h_2(x))}h_2(\frac{1}{x}).\end{aligned}$$

即 $\bar{h}_1(x)$ 和 $\bar{h}_2(x)$ 分别是 $h_1(x)$ 和 $h_2(x)$ 的互反多项式. 记

$$h_1^*(x) = \frac{1}{h_1(0)}\bar{h}_1(x), h_2^*(x) = \frac{1}{h_2(0)}\bar{h}_2(x).$$

定理 3.8 设环 R 上的循环码 C 的标准形生成元集为 $\{vg_1(x), (1+v)g_2(x)\}$, 则 C 的对偶码 $C^\perp$ 的标准形生成元集为 $\{vh_1^*(x), (1+v)h_2^*(x)\}$.

证 由定理 3.1 (2) 可得.

参 考 文 献

[1] Abualrub T, Siap I. Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$[J]. Des. Codes Cryptogr., 2007, 42: 273–287.

[2] Blake I F. Codes over certain rings[J]. Inform. Control, 1972, 20: 396–404.

[3] Blake I F. Codes over integer residue rings[J]. Inform. Control, 1975, 29: 295–300.

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

[5] Cengellenmis Y, Dertli A, Dougherty S T. Codes over an infinite family of rings with a Gray map[J]. Des. Codes Cryptogr., DOI. 10.1007/s10623-012-9787-y, published online: 01 January 2013.

[6] Dougherty S T. Kim J -L. Kulosman H. MDS codes over finite principal ideal rings[J]. Des. Codes Cryptogr., 2009, 50: 77–92.

[7] Hammons A R, Jr Kumar P V, Calderbank A R, Sloane N J A Solé P, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes[J]. IEEE Trans. Inform. Theory, 1994, 40(2): 301–319.

[8] Udaya P, Bonnecaze A. Decoding of cyclic codes over $F_2 + uF_2$[J]. IEEE Trans. Inform. Theory, 1999, 45: 2148–2157.

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

[10] Wan Z X. Quaternary codes[M]. Singapore: World Scientific, 1997.

[11] Zhu S, Wang Y. Shi M. Some results on cyclic codes over $F_2 + vF_2$[J]. IEEE Trans. Inform. Theory, 2010, 56: 1680–1684.

[12] Zhu S, Wang L. A class of constacyclic codes over $F_p + vF_p$ and its Gray image[J]. Discrete Math., 2011, 311: 2677–2682.

CYCLIC CODES OVER $F_2 + vF_2$

ZHANG Guang-hui, LI Liang-chen

(*School of Mathematical Sciences, Luoyang Normal University, Luoyang 471022, China*)

Abstract: In this paper, cyclic codes over $F_2 + vF_2$ are studied. By virtue of the generating set in standard form for the cyclic codes over $F_2 + vF_2$, we characterize the structure of cyclic codes over the ring. Then we prove that any nonzero cyclic code over the ring has a unique generating set in standard form and they are principally generated.

Keywords: $F_2 + vF_2$; cyclic codes; generating set in standard form

2010 MR Subject Classification: 94B05; 94B15