环 F_2+uF_2 上线性码的结构特性

耿 普[①]　　李 超[①②]
[①](国防科技大学数学与系统科学系　长沙　410073)
[②](东南大学移动通信国家重点实验室　南京　210096)

摘　要：该文研究了环 F_2+uF_2 上线性码的结构特性，讨论了环 F_2+uF_2 上线性码及其剩余码、挠码和商码之间的关系，通过这些关系。给出了线性码(特别是循环码)的深度分布与深度谱。

关键词：剩余码；挠码；商码；深度谱；深度分布
中图分类号：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2007)12-2912-03

Structure Character of Linear Codes on Ring F_2+uF_2

Geng Pu[①]　　Li Chao[①②]
[①](*Department of Mathematics and System Science, National University of Defense Technology, Changsha* 410073, *China*)
[②](*State Key Laboratory of Mobile of Southeast University, Nangjing* 210096, *China*)

Abstract: In this paper, the structure character of linear codes on ring F_2+uF_2 and the relation between the linear code and its residue code, torsion code, quotient code are studied. The depth distribution and depth spectrum of linear codes (especially the cyclic codes) are presented.

Key words: Residue codes; Torsion codes; Quotient code; Depth spectrum; Depth distribution

1　引言

随着有限域上纠错编码理论的完善，纠错码的研究热点已经从有限域上转到了有限环上。最近大多数的研究都是集中在四元环 F_2+uF_2 上的纠错码问题。文献[1]提出了环 F_2+uF_2 上线性码及其剩余码、挠码的概念，并分别给出了它们的生成矩阵，讨论了环 F_2+uF_2 上奇数长循环码得生成元形式。文献[2]给出了文献[1]中线性码的译码算法。文献[3]研究了环 F_2+uF_2 上一类特殊的线性码及其对偶码的问题。文献[4]讨论了环 F_2+uF_2 上线性码的重量问题。文献[5]讨论了一种用整值多项式求深度的方法，同时讨论了二元域上的循环码的深度谱。本文研究了环 F_2+uF_2 上的线性码的结构问题，给出了环 F_2+uF_2 上的线性码的商码的概念及其生成矩阵，讨论了环 F_2+uF_2 上线性码及其剩余码，挠码，商码之间的关系，通过这些关系，我们得到了线性码(特别是循环码)的深度分布与深度谱。

2　预备知识

F_2+uF_2 作为一个介于模 4 剩余类环 Z_4 和四元域 F_4 之间的一个环结构，它兼有环 Z_4 和域 F_4 的一些性质，其元素为 $\{0,1,u,1+u\}$ 。环 F_2+uF_2 上的加法(图 1)与 $F_4=\{0,1,\alpha,\alpha^2=1+\alpha\}$ 上的加法运算相同(此时把 u 当作 α)，但乘法(图 2)却与 Z_4 上的乘法运算相同(此时把 u 当作 2)，所以 F_2 是环 F_2+uF_2 的一个子环。

+	0	1	u	1+u
0	0	1	0	1+u
1	1	0	1+u	u
u	u	1+u	0	1
1+u	1+u	u	1	0

图 1　环 F_2+uF_2 上的加法运算

*	0	1	u	1+u
0	0	0	0	0
1	0	1	u	1+u
u	0	u	0	u
1+u	0	1+u	u	1

图 2　环 F_2+uF_2 上的乘法运算

为方便起见，下面用 R 表示四元环 F_2+uF_2，环 R 上的线性码 C 是 R 模 R^n 的一个子模，循环码就是 R 模 $R_n=R[x]/(x^n-1)$ 的一个理想。根据文献[1]，环 R 上的非零线性码 C 的生成矩阵都可以写成如下形式：

2006-05-19 收到，2006-10-16 改回
国家自然科学基金(60573028)和东南大学移动通信国家重点实验室开放基金(A200503)资助课题

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}\\ 0 & u\boldsymbol{I}_{k_2} & u\boldsymbol{D}\end{bmatrix} \tag{1}$$

其中 $\boldsymbol{A}$，$\boldsymbol{D}$ 为 F_2 上的矩阵，$\boldsymbol{B}$ 为环 R 上的矩阵，可以记为 $\boldsymbol{B}=\boldsymbol{B}_0+u\boldsymbol{B}_1$，其中 $\boldsymbol{B}_0,\boldsymbol{B}_1$ 均为 F_2 中矩阵。C 的所有码字可以写成 $[\boldsymbol{v}_0,\boldsymbol{v}_1]\boldsymbol{G}$ 的形式，其中 $\boldsymbol{v}_0$ 为环 R 上的 k_1 维向量，$\boldsymbol{v}_1$ 为 F_2 上的 k_2 维向量，所以码 C 中包含 $4^{k_1}2^{k_2}$ 个码字。

定义1　设 C 为环 R 上的一个 n 长线性码，令 $C_1=\{\boldsymbol{x}\in F_2^n \mid \exists \boldsymbol{y}\in F_2^n, \boldsymbol{x}+u\boldsymbol{y}\in C\}$，$C_2=\{\boldsymbol{x}\in F_2^n \mid u\boldsymbol{x}\in C\}$，$C_u=\{\boldsymbol{x}\in F_2^n \mid \exists \boldsymbol{y}\in F_2^n, st, u\boldsymbol{x}+\boldsymbol{y}\in C\}$，称 C_1 为 C 的剩余码(reside code)，C_2 为 C 的挠码(torsion code)，C_u 为 C 的商码(quotient code)。

定义2　令 $\boldsymbol{w}=(a_1,a_2,\cdots,a_n)$ 为线性空间 R^n 中的一个元素，定义3种映射如下：$D:D(\boldsymbol{w})=(a_2-a_1,\cdots,a_n-a_{n-1})$，$E:E(\boldsymbol{w})=(a_2,\cdots,a_n)$，$G:G(\boldsymbol{w})=(a_1,\cdots,a_{n-1})$ 称 D,E,G 分别为 $\boldsymbol{w}$ 的微分运算，前截运算，后截运算。

定义3　设 $\boldsymbol{c}=(a_1,\cdots,a_n)$ 为线性码 C 的一个码字，称满足 $D^i(\boldsymbol{c})=[0^{n-i}]$ 的最小正整数 i 为码字 $\boldsymbol{c}$ 的深度，这里 $D^i(\boldsymbol{c})$ 表示对码字 $\boldsymbol{c}$ 进行了 i 次 D 运算。如果没有这样的整数存在，就称码字 $\boldsymbol{c}$ 的深度为 n。码字 $\boldsymbol{c}$ 的深度记为 $d(\boldsymbol{c})$。

定义4　设 C 为一个线性码，记 D_i 为码 C 中深度为 i 的码字的数量，则 $\{D_0,D_1,\cdots,D_n\}$ 为码 C 的深度分布，$\{i \mid D_i\neq 0,\quad 0\le i\le n\}$ 为码 C 的深度谱。

3　主要结果

引理 1　环 R 上的线性码 C 的剩余码、挠码和商码都是线性码，其生成矩阵分别为

$$\begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\end{bmatrix},\ \begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\\ 0 & \boldsymbol{I}_{k_2} & \boldsymbol{D}\end{bmatrix},\ \begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\\ 0 & \boldsymbol{I}_{k_2} & \boldsymbol{D}\\ 0 & 0 & \boldsymbol{B}_1'\end{bmatrix} \tag{2}$$

其中 $\boldsymbol{B}=\boldsymbol{B}_0+u\boldsymbol{B}_1$，$\boldsymbol{B}_0,\boldsymbol{B}_1$ 均为 F_2 中的矩阵，$\boldsymbol{B}_1'$ 为 B_1 中线性无关的 r 行(r 是 B_1 的秩)。

证明　文献[1]中已经给出剩余码和挠码的生成矩阵分别为

$$\begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\end{bmatrix},\ \begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\\ 0 & \boldsymbol{I}_{k_2} & \boldsymbol{D}\end{bmatrix} \tag{3}$$

下面我们考虑商码的生成矩阵。

因为 $C=(\boldsymbol{v}_0,\boldsymbol{v}_1)\boldsymbol{G}$ (其中 $\boldsymbol{v}_0=\boldsymbol{v}_{01}+u\boldsymbol{v}_{0u}$：$\boldsymbol{v}_{01}$，$\boldsymbol{v}_{0u}$，$\boldsymbol{v}_1$ 分别是二元域上的 k_1,k_1,k_2 元向量)中的码字都有下面的表示形式：

$$\begin{aligned}&(\boldsymbol{v}_{01},\boldsymbol{v}_{01}\boldsymbol{A},\boldsymbol{v}_{01}\boldsymbol{B}_0)+u(\boldsymbol{v}_{0u},\boldsymbol{v}_{0u}\boldsymbol{A}+\boldsymbol{v}_1,\boldsymbol{v}_{0u}\boldsymbol{B}_0+\boldsymbol{v}_1D)\\&\qquad+u(0,0,\boldsymbol{v}_{01}\boldsymbol{B}_1)\end{aligned} \tag{4}$$

所以当我们把 C 中的码字表示成 $\boldsymbol{x}+u\boldsymbol{y}$ 的形式时，商码就是所有 $\boldsymbol{y}$ 的集合，也就是所有具有形式 $(\boldsymbol{v}_{0u},\boldsymbol{v}_{0u}\boldsymbol{A}+\boldsymbol{v}_1,\boldsymbol{v}_{0u}\boldsymbol{B}_0+\boldsymbol{v}_1\boldsymbol{D})+(0,0,\boldsymbol{v}_{01}\boldsymbol{B}_1)$ 的码字的集合，表示成矩阵的形式就是 $(\boldsymbol{v}_{0u},\boldsymbol{v}_1,\boldsymbol{v}_{01})\begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\\ 0 & \boldsymbol{I}_{k_2} & \boldsymbol{D}\\ 0 & 0 & \boldsymbol{B}_1\end{bmatrix}$，显然也是一个线性码。

所以环 R 上的线性码 C 的剩余码，挠码和商码都是线性码，其生成矩阵分别为

$$\begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\end{bmatrix},\ \begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\\ \boldsymbol{0} & \boldsymbol{I}_{k_2} & \boldsymbol{D}\end{bmatrix},\ \begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\\ 0 & \boldsymbol{I}_{k_2} & \boldsymbol{D}\\ 0 & 0 & \boldsymbol{B}_1'\end{bmatrix}$$

推论 1　对于剩余码 C_1 中任意一个码字 $\boldsymbol{x}$，在商码 C_u 中有且仅有 $2^{k_1+k_2}$ 个与之对应的码字 $\boldsymbol{y_i}(i=1,2,\cdots,2^{k_1+k_2})$，使得 $\boldsymbol{x}+u\boldsymbol{y_i}\in C$。

证明　由引理 1 的证明可知，码 C 中的码字有如下形式的表示：

$$\begin{aligned}&(\boldsymbol{v}_{01},\boldsymbol{v}_{01}\boldsymbol{A},\boldsymbol{v}_{01}\boldsymbol{B}_0)+u(\boldsymbol{v}_{0u},\boldsymbol{v}_{0u}\boldsymbol{A}+\boldsymbol{v}_1,\boldsymbol{v}_{0u}\boldsymbol{B}_0+\boldsymbol{v}_1\boldsymbol{D})\\&\qquad+u(\boldsymbol{0},\boldsymbol{0},\boldsymbol{v}_{01}\boldsymbol{B}_1)\end{aligned} \tag{5}$$

所以对于 C_1 中任意一个给定的码字 $(\boldsymbol{v}_{01},\boldsymbol{v}_{01}\boldsymbol{A},\boldsymbol{v}_{01}\boldsymbol{B}_0)$，只有对任意 C_u 中的具有形式 $(\boldsymbol{v}_{0u},\boldsymbol{v}_{0u}\boldsymbol{A}+\boldsymbol{v}_1,\boldsymbol{v}_{0u}\boldsymbol{B}_0+\boldsymbol{v}_1\boldsymbol{D})+(\boldsymbol{0},\boldsymbol{0},\boldsymbol{v}_{01}\boldsymbol{B}_1)$ 的码字 $\boldsymbol{y}$，有 $\boldsymbol{x}+u\boldsymbol{y}\in C$ 成立，而且 $\boldsymbol{v}_{0u}$，$\boldsymbol{v}_1$ 分别是二元域上的 k_1,k_2 元向量，所以推论成立。

定理 1　设 C 是环 R 上的线性码，C_1，C_2 和 C_u 分别为 C 的剩余码、挠码和商码，则 $C_1\subseteq C_2\subseteq C_u$。

证明　从引理 1 中剩余码、挠码和商码的生成矩阵可以得到结论。

由线性码 C 可以唯一地决定其剩余码和挠码，但是知道剩余码和挠码并不一定能够重构出原来的线性码，也就是说在知道 C_1,C_2 的情况下，对应的线性码 C 不并一定是唯一的。

推论 2　环 R 上的线性码 C 的深度谱中含有 k_1+k_2+r (r 是矩阵 B_1 的秩)个非零值，且线性码 C 的深度谱跟商码 C_u 的深度谱是一致的。

证明　对于线性码 C 上的任意一个码字 $\boldsymbol{x}+u\boldsymbol{y}$，由文献[6]，它的深度等于 $\max(d(\boldsymbol{x}),d(\boldsymbol{y}))$，其中 $d(\boldsymbol{x}),d(\boldsymbol{y})$ 分别表示 F_2 上的码字 $\boldsymbol{x},\boldsymbol{y}$ 的深度。再根据定理 1 可知，$C_1\subseteq C_u$，所以线性码 C 的深度谱跟商码 C_u 的深度谱是一致的。又因为有限域上线性码的深度谱中非零值个数等于码的信息位数，所以码 C 的深度谱中含有 k_1+k_2+r 个非零深度值。

以下讨论的循环码除非特别声明，都是指奇数长的循环码。

引理 2[1]　环 R 上码长为 n (n 为奇数)的循环码都可以写成 $(f(x)h(x),uf(x)g(x))$ 的形式。其中 $f(x)g(x)h(x)=x^n-1$，$f(x),g(x),h(x)\in F_2[x]$ 且两两互素。

定理 2　设 C 为环 R 上码长为 n (n 为奇数)的循环码，则 $C_2=C_u$。此时 C 的生成矩阵中 $\boldsymbol{B}_1$ 为零矩阵，即循环码 C 的生成矩阵为 $\begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_0\\ \boldsymbol{0} & u\boldsymbol{I}_{k_2} & u\boldsymbol{D}\end{bmatrix}$。

证明 因为循环码 C 为 $(f(x)h(x),uf(x)g(x))$ (其中 $f(x)g(x)h(x)=x^n-1;\ \ f(x),g(x),h(x)\in F_2(x)$)，所以码 C 中的码字都可以表示为如下形式：

$$\begin{aligned}&f(x)h(x)(m_0(x)+um_1(x))+uf(x)g(x)(l_0(x)+ul_1(x))\\&=f(x)h(x)m_0(x)+uf(x)g(x)l_0(x)+uf(x)h(x)m_1(x)\end{aligned}\tag{6}$$

根据定义，$C_2=\{\boldsymbol{x}\in F_2^n\mid u\boldsymbol{x}\in C\}$，$C_u$ 为所有使得 $\boldsymbol{x}+u\boldsymbol{y}\in C$ 成立的 $\boldsymbol{y}$ 的集合，所以 uC_2 就是 $m_0(x)$ 为零时的码字集合，C_2 中的码字可以写成 $f(x)g(x)l_0(x)+f(x)h(x)\cdot m_1(x)$ 的形式，所以 $C_2=(f(x)h(x),f(x)g(x))=(f(x))$。再根据引理 1，由生成矩阵可知 $C_2=C_u$ 当且仅当 $\boldsymbol{B}_1$ 为零矩阵，所以循环码 C 的生成矩阵为 $\begin{bmatrix}\boldsymbol{I}_{k_1}&\boldsymbol{A}&\boldsymbol{B}_0\\\boldsymbol{0}&u\boldsymbol{I}_{k_2}&u\boldsymbol{D}\end{bmatrix}$。

当 C 是循环码的时候 $C_1,uC_2\subseteq C$，所以对任意 $\boldsymbol{x}\in C_1,\boldsymbol{y}\in C_2$，有 $\boldsymbol{x}+u\boldsymbol{y}\in C$，即 $C=C_1+uC_2$，所以可由 C_1,C_2 重构循环码 C，即对任意两个二元循环码 C_1,C_2 且有 $C_1\subseteq C_2$，就可以重构出唯一的一个环 R 上的循环码 C 使得 C_1,C_2 分别为其剩余码和挠码。也就是 C_1,C_2 和 C 是相互唯一决定的。

推论 3 设 C_1,C_2 的深度分布分别为 $\{d_0,\cdots,d_n\},\{D_0,\cdots,D_n\}$，则循环码 C 的深度谱中有 k_1+k_2 个非零值，并且深度分布为 $\{X_0,\cdots,X_n\}$，其中 $X_i=d_i\times\sum_{k=0}^{i}D_k+D_i\times\sum_{k=0}^{i-1}d_k$，$(i=0,1,\ \ 2,\cdots,n)$。

证明 因为码字 $\boldsymbol{x}+u\boldsymbol{y}\in C$ 的深度值等于 $\boldsymbol{x},\boldsymbol{y}$ 中深度值较大的一个，所以要求 $\boldsymbol{x}+u\boldsymbol{y}$ 的深度值为 i 的时候只需要 $\boldsymbol{x},\boldsymbol{y}$ 中有一个的深度值为 i，另一个的深度值可以是小于等于 i 的任何数。因为对任意 $\boldsymbol{x}\in C_1$，$\boldsymbol{y}\in C_2$，有 $\boldsymbol{x}+u\boldsymbol{y}\in C$，所以根据 $\boldsymbol{x}+u\boldsymbol{y}$ 的深度等于 $\boldsymbol{x},\boldsymbol{y}$ 中深度值较大的那个二元码的深度，所以有 $X_i=d_i\times\sum_{k=0}^{i}D_k+D_i\times\sum_{k=0}^{i-1}d_k$ $(i=0,1,2,\cdots,n)$。

定理 3 当 $(x-1)\mid f(x)$ 时，环 R 上的循环码 C 的深度谱为 $\{n,n-1,\cdots,n-k+1\}$，否则深度谱为 $\{1\}\cup\ \{n,n-1,\cdots,n-k+1+1\}$，其中 k 为循环码 C 的挠码 C_2 的信息位数。

证明 因为 $C_1=(f(x)h(x))\subseteq C_2=(f(x))$，$\boldsymbol{x}+u\boldsymbol{y}$ 的深度值等于 $\boldsymbol{x},\boldsymbol{y}$ 当中某一个二元码的深度值，所以循环码 C 的深度谱跟 C_2 的深度谱一致。又因为 n 为奇数，所以 x^n-1 的因子中没有重因子，即 $(x-1)$ 要么不整除 $(x^n-1)/f(x)$，此时 $(x-1)\mid f(x)$；否则 $(x-1)$ 就恰好整除 $(x^n-1)/f(x)$，根据文献[5]中的定理 23 可知，$(x-1)\mid f(x)$ 时，环 R 上的循环码 C 的深度谱为 $\{n,n-1,\cdots,n-k+1\}$，否则深度谱为 $\{1\}\cup\{n,n-1,\cdots,n-k+1+1\}$。

4 结束语

根据研究结果，当 C 为环 R 上的一般线性码时，$C_2\neq C_u$，不能由 C_1,C_2 重构得出线性码 C，此时线性码 C 的深度谱中非零值的个数等于 k_1+k_2+r。当 C 为奇数长循环码的时候 $C_2=C_u$，此时能由 C_1,C_2 重构得出循环码 C，我们可以明确地给出 C 的深度谱，还可根据 C_1,C_2 的深度分布求出 C 的深度分布。

参 考 文 献

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

[2] Udaya P and Bonnecaze A. Decoding of cyclic codes over F_2+uF_2 [J]. *IEEE Trans on Inform Theory*. 1999, 45(6): 2520–2522.

[3] Dougherty S T, Gaborit P, Harada M, and Sole P. Type II codes over F_2+uF_2 [J]. *IEEE Trans. on Inform Theory*. 1999, 45(6): 32–45.

[4] Gulliver T A and Harada M. Construction of optimal type IV self-dual codes over F_2+uF_2 [J]. *IEEE Trans on Inform Theory*. 1999, 45(6): 2148–2157.

[5] Chris J Mitchell. On the integer-valued rational polynomials and depth distribution of binary codes [J]. *IEEE Trans on Inform Theory*. 1998, 44(7): 3146–3150.

[6] 张振涛, 杨义先, 胡正名, 钮心忻. 关于线性码深度分布的研究 [J]. 北京邮电大学学报, 2000, 25(3): 68–72.

耿 普： 男，1982 年生，硕士生，感兴趣的方向是纠错编码.

李 超： 男，1966 年生，教授，博士生导师，研究方向为编码与密码.