环Z_4上线性循环码的深度谱

朱士信 杨善林* 童宏玺
(合肥工业大学应用数学系 合肥 230009)
*(合肥工业大学网络研究所 合肥 230009)

摘 要：Etzion 定义并研究了域 F_q 上线性码的深度谱，该文研究了环 Z_4 上线性码与线性循环码的深度谱，证明了 $4^{k_1}2^{k_2}$ 型线性码的深度谱至少含有 k_1+k_2 个非零值，并给出了一类 4^k 型线性循环码的深度谱为 $\{n,n-1,\cdots,n-k+1\}$。

关键词：线性码，线性循环码，深度，深度谱
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2005)10-1597-03

On the Depth Spectrums of Linear Cyclic Codes on Ring Z_4

Zhu Shi-xin Yang Shan-lin* Tong Hong-xi
(*Department of Applied Mathematics, Hefei University of Technology, Hefei* 230009，*China*)
*(*Institute of Network, Hefei University of Technology, Hefei* 230009, *China*)

Abstract Etzion defined and studied the depth spectrums of linear codes on field F_q. In this correspondence, the depth spectrums of linear codes and linear cyclic codes on ring Z_4 are studied, and it is proved that the depth spectrum of linear code of type $4^{k_1}2^{k_2}$ has at least k_1+k_2 nonzero values, and the depth spectrum of linear cyclic code of type 4^k is $\{n,n-1,\cdots,n-k+1\}$.

Key words Linear code, Linear cyclic code, Depth, Depth spectrum

1 引言

Etzion在文献[1]中首先定义了线性码的深度及深度谱，给出了计算二元线性码的码字深度的算法，证明了q元[n, k]线性码的深度谱恰好由k个非零值组成；Mitchell在文献[2]中研究了二元线性循环码深度谱；Luo等在文献[3]中给出了计算q元线性码的码字深度的算法，并研究了一些计算问题。这些研究结果可广泛应用于域上的编码理论研究，如文献[4]给出了利用码的深度分布求码的周期分布的方法，并确定了码长为二幂次的扩展码和扩展循环码的周期分布；又如文献[1]利用深度分布给出了构造新码的方法和码的一种新的等价分类方法，因此研究线性码、循环码的深度分布是有价值的，但上述研究都是域上码的深度研究。 众所周知，近十几年来，Z_4环或Z_k环上的编码问题的研究[5,6]是编码理论研究的一个热点研究领域。 文献[7]给出了计算Z_4环上码的深度的两种递归算法，本文研究了Z_4环上的线性码与线性循环码的深度谱，证明了 $4^{k_1}2^{k_2}$ 型线性码的深度谱至少含有 k_1+k_2 个非零值，并给出了一类 4^k 型线性循环码和一类 2^k 型线性循环码的深度谱。 这些结论对进一步研究 Z_4 环上的编码问题应有一定的参考价值。

2 Z_4环上线性码的深度分布

为了方便，本文中用 $[a^k]$ 表示连续 k 个分量为 a。

定义 1 对 $\forall \boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in Z_4^n$，定义微分算子 D：

$$D\boldsymbol{x}=(x_2-x_1,x_3-x_2,\cdots,x_n-x_{n-1})$$

称使 $D^i\boldsymbol{x}=[0^{n-i}]$ 成立的最小非负整数为 $\boldsymbol{x}$ 的深度，记为 $\mathrm{depth}(\boldsymbol{x})$；若没有这样的 i 存在，则令 $\boldsymbol{x}$ 的深度为 n。

显然，$0\le \mathrm{depth}(\boldsymbol{x})\le n$，且对 $\forall \boldsymbol{x},\boldsymbol{y}\in Z_4^n$，$\forall k\in Z_4$，有 $D(\boldsymbol{x}+\boldsymbol{y})=D(\boldsymbol{x})+D(\boldsymbol{y})$，$D(k\boldsymbol{x})=kD(\boldsymbol{x})$，故微分算子 D 是一个线性算子。 值得注意的是，在域上，$k\boldsymbol{x}(k\ne 0)$ 与 $\boldsymbol{x}$ 有相同的深度，而在环 Z_4 上，此结论显然不成立，如 $\mathrm{depth}[2^n]=1$，但 $\mathrm{depth}(2[2^n])=\mathrm{depth}[0^n]=0$；又如 $\mathrm{depth}(02002)=5$，但 $\mathrm{depth}(2(02002))=\mathrm{depth}[0^5]=0$。

2004-06-28 收到，2004-12-09 改回
国家自然科学基金(70471046)和安徽省自然科学基金(03042201)资助课题

定义 2 设 C 是环 Z_4 上长为 n 的码，用 D_i 表示 C 中具有深度为 i 的码字的个数，则称集合 $\{D_0,D_1,\cdots,D_n\}$ 为码 C 的深度分布，称集合 $\{i\,|\,D_i\neq 0,1\le i\le n\}$ 为码 C 的深度谱。

文献[1]证明了 F_q 上 $[n,k]$ 线性码 C 的深度谱恰好有 k 个非零值，但此结论在 Z_4 环上不成立。

文献[5]性质 1.1 证明了 Z_4 环上任何含非零码字的线性码一定等价于以如下形式矩阵:

$$\begin{bmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B} \\ 0 & 2\boldsymbol{I}_{k_2} & 2\boldsymbol{F} \end{bmatrix}$$

为生成矩阵的线性码 C，其中 $\boldsymbol{A},\boldsymbol{F}$ 是 Z_2 上矩阵，$\boldsymbol{B}$ 是 Z_4 上矩阵。 本文中称这种形式的线性码为 $4^{k_1}2^{k_2}$ 型线性码。 显然， $4^{k_1}2^{k_2}$ 型线性码 C 含有 $4^{k_1}2^{k_2}$ 个码字，这些码字可由生成矩阵的 $k=k_1+k_2$ 个行向量生成。

定理 1 设 C 是 $4^{k_1}2^{k_2}$ 型 Z_4 线性码，则 C 的深度谱中至少有 k_1+k_2 个非零值。

证明 设 C 的生成矩阵为

$$\begin{bmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B} \\ 0 & 2\boldsymbol{I}_{k_2} & 2\boldsymbol{F} \end{bmatrix}$$

令 C_1 是以矩阵:

$$\begin{bmatrix} 2\boldsymbol{I}_{k_1} & 2\boldsymbol{A} & 2\boldsymbol{B} \\ 0 & 2\boldsymbol{I}_{k_2} & 2\boldsymbol{F} \end{bmatrix}$$

为生成矩阵的线性码，则 C_1 是 C 的子码。

再令 C_2 是以矩阵

$$\begin{bmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_1 \\ 0 & \boldsymbol{I}_{k_2} & \boldsymbol{F} \end{bmatrix}$$

为生成矩阵的 Z_2 线性码，其中 $\boldsymbol{B}_1$ 中各元素是 $\boldsymbol{B}$ 中相应元素摸 2 的值，则

$$\forall\alpha\in C_2 \text{ 当且仅当 } 2\alpha\in C_1$$

又由于 C_2 是 Z_2 线性码， C_1 是 Z_4 线性码，且对 $\forall\alpha\in Z_2^n$，在 Z_2 中 $D\alpha=0$ 当且仅当在 Z_4 中 $D(2\alpha)=0$ ， 故 $\mathrm{depth}(2\alpha)=\mathrm{depth}(\alpha)$，因此 C_1 与 C_2 有相同的深度分布。 由文献[1]中定理 1 知， C_2 的深度谱恰好含有 k_1+k_2 个非零值，故 C_1 的深度谱恰好含有 k_1+k_2 个非零值。 又 C_1 是 C 的子码，故 C 的深度谱中至少含有 k_1+k_2 个非零值。 证毕

文献[5]中例 1.1 给出的以矩阵 $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}$ 为生成矩阵的 Klemm 码 k_4 是 $4^1 2^2$ 型线性码，容易计算得 Klemm 码 k_4 的深度谱恰好含有 3 个非零值 1，2，3，其中 $k_1+k_2=3$；但以 $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \end{pmatrix}$ 为生成矩阵 $4^1 2^1$ 型 Z_4 线性码的深度谱含有 3 个非零值 1，2，3，但 $3>k_1+k_2=2$，即域上线性码的深度理论对 Z_4 环上线性码不一定成立。

3 Z_4 线性循环码的深度谱

文献[2]给出了 F_2 上线性循环码的深度谱的一些结果，本节我们讨论 Z_4 线性循环码的深度理论。

设 C 是 Z_4 线性循环码， 由于 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in C$ 当且仅当 $(c_{n-1},c_0,c_1\cdots,c_{n-2})\in C$ ，故 Z_4 环上任何一个线性循环码一定是 $4^{k_1}2^{k_2}$ 型线性码。 当 $k_2=0$ 时，称 C 为 4^k 型线性循环码。 由于环上编码问题的复杂性，本节仅讨论 4^k 型或 2^k 型线性循环码。

引理 1 设 C 是一个长为 n 的 Z_4 线性循环码，$[2^n]\notin C$，若 C 中所有非零码字中最长的 0 游程的长为 l ， 则 C 的所有非零码字的深度最小值大于 $n-l-1$。

证明 设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$ 是线性循环码 C 中一个非零码字。 记 $T\boldsymbol{x}=(x_2,\cdots,x_n,x_1)$ ， 则 $T\boldsymbol{x}\in C$ 。 由于 $[2^n]\notin C$ ，则 $[1^n]\notin C$ ， $[3^n]\notin C$ ，则 $\boldsymbol{y}=T\boldsymbol{x}-\boldsymbol{x}=[x_2-x_1,x_3-x_2,\cdots,x_n-x_{n-1},x_1-x_n]\in C$ 且 $y\neq 0$ ， 则 $D\boldsymbol{x}=[x_2-x_1,x_3-x_2,\cdots,x_n-x_{n-1}]$ 是 C 中非零码字 $\boldsymbol{y}$ 的连续的 $n-1$ 个分量。 同理 $D^2\boldsymbol{x}=D(D\boldsymbol{x})$ 是 C 中非零码字 $T\boldsymbol{y}-\boldsymbol{y}$ 的连续 $n-2$ 个分量，令 $s=n-l-1$，则 $D^s\boldsymbol{x}$ 是 C 中某非零码字的连续 $n-s$ 个分量，由于 $n-s=l+1>l$，又 C 中所有非零码字中最长的 0 游程的长为 l ， 则 $D^s\boldsymbol{x}\neq 0$，即 $\mathrm{depth}\boldsymbol{x}>s=n-l-1$，从而得证引理。 证毕

定理 2 设 $g(x)$ 是长为 n 的 4^k 型 Z_4 线性循环码 C 的生成多项式，且 $g(x)\nmid 2(x^{n-1}+\cdots+x+1)$ ， 则 C 的深度谱为 $\{n,n-1,\cdots,n-k+1\}$ 。

证明 由于 C 是 4^k 型 Z_4 线性循环码，则 C 的生成矩阵具有形式 $(\boldsymbol{I}_k\boldsymbol{A})$ 。 对 $\forall\alpha\in C$ ，若码字 α 中含有长为 k 的零游程。设 $\alpha=(c_1\cdots c_i0^k c_{i+k+1}\cdots c_n)$ ， 由于 C 是循环码，故 $\beta=(0^k c_{i+k+1}\cdots c_n c_1\cdots c_i)\in C$ 。 若 $(a_1\cdots a_k)(\boldsymbol{I}_k\boldsymbol{A})=\beta$ ， 则 $(a_1\cdots a_k)=0$，从而 $c_{i+k+1}=\cdots=c_n=c_1=\cdots=c_i=0$，即 $\alpha=0$，即码 C 中非零码字的最长零游程为 $k-1$ 。 又 $g(x)\nmid 2(x^{n-1}+\cdots+x+1)$，则 $[2^n]\notin C$ ， 由引理 1 知，码 C 的所有非零码字的深度的最小值大于 $n-(k-1)-1=n-k$ 。 由定理 1 知，码 C 的深度谱中至少有 k 个非零值，故码 C 的深度

谱为 $\{n, n-1, \cdots, n-k+1\}$。　　证毕

引理 2　设 $\boldsymbol{c}=(c_0, c_1, \cdots, c_{n-1})$ 是 Z_4 线性循环码 C 中的码字，其对应多项式为 $\boldsymbol{c}(\boldsymbol{x})=c_0\boldsymbol{x}^{n-1}+c_1\boldsymbol{x}^{n-2}+\cdots+c_{n-1}$，则 $D^i\boldsymbol{c}$ 的 $n-i$ 个分量依序等于 $\boldsymbol{c}(\boldsymbol{x})(\boldsymbol{x}-1)^i(\bmod \boldsymbol{x}^n-1)$ 的 $\boldsymbol{x}^{n-1}, \boldsymbol{x}^{n-2}, \cdots, \boldsymbol{x}^i$ 的系数。

证明　利用 D 的定义，对 i 用数学归纳法即可证明。

在 $Z_4[x]$ 中，由于对任何非负整数 m，恒有

$$2(\boldsymbol{x}^{2^m}+1)=2(x-1)^{2^m}$$

成立，故 $(\boldsymbol{x}-1)^{2^m+1}\,\big|\,2(\boldsymbol{x}^{2^{m+1}}-1)$，则对任何自然数 $k\le 2^m+1$，恒有 $(\boldsymbol{x}-1)^k\,\big|\,2(\boldsymbol{x}^{2^{m+1}}-1)$。　　证毕

定理 3　设 $n=2^{m+1}$，$k\le 2^m+1$，则以 $g(\boldsymbol{x})=\dfrac{2(\boldsymbol{x}^n-1)}{(\boldsymbol{x}-1)^k}$ 为生成多项式的线性循环码 C 的深度谱为 $\{1,2,\cdots,k\}$。

证明　对 $\forall \boldsymbol{c}\in C$，则对应的多项式 $\boldsymbol{c}(\boldsymbol{x})=f(\boldsymbol{x})g(\boldsymbol{x})=f(\boldsymbol{x})\cdot\dfrac{2(\boldsymbol{x}^n-1)}{(\boldsymbol{x}-1)^k}(\bmod \boldsymbol{x}^n-1)$，由引理 2 知，$D^k\boldsymbol{c}$ 的 $n-k$ 个分量依序等于 $(\boldsymbol{x}-1)^k\boldsymbol{c}(\boldsymbol{x})(\bmod \boldsymbol{x}^n-1)$ 的 $\boldsymbol{x}^{n-1}, \boldsymbol{x}^{n-2}, \cdots, \boldsymbol{x}^k$ 的系数，由于 $(\boldsymbol{x}-1)^k\boldsymbol{c}(\boldsymbol{x})=(\boldsymbol{x}-1)^k\cdot f(\boldsymbol{x})\cdot\dfrac{2(\boldsymbol{x}^n-1)}{(\boldsymbol{x}-1)^k}=2f(\boldsymbol{x})\cdot(\boldsymbol{x}^n-1)\equiv 0(\bmod \boldsymbol{x}^n-1)$，即 $D^k\boldsymbol{c}=0$，故码 C 的深度最大值只能为 k。由于 $g(\boldsymbol{x})$ 是 $n-k$ 次的，故 C 的生成矩阵是 $k\times n$ 型的。由定理 1 知，C 的深度谱至少含有 k 个非零值，从而 C 的深度谱为 $\{1,2,\cdots,k\}$。　　证毕

4　结束语

本文研究了 Z_4 线性码和线性循环码的深度谱，但由于环 Z_4 中具有零因子，因此研究较为困难，如定理 2 仅给出了 4^k 型线性循环码的生成多项式 $g(x)\nmid 2(\boldsymbol{x}^{n-1}+\boldsymbol{x}^{n-2}+\cdots+\boldsymbol{x}+1)$ 的情形，而 2^k 型或 $4^{k_1}2^{k_2}$ 型的情形有待进一步研究；又如定理 3 仅是 $g(x)\nmid 2(\boldsymbol{x}^{n-1}+\cdots+\boldsymbol{x}+1)$ 的一种特殊情形，而一般的情况也有待于进一步研究。

参 考 文 献

[1] Etzion T. The depth distribution——A new characterization for linear codes. *IEEE Trans. on Info.Thory*. 1997, IT-43(4): 1361 − 1363.

[2] Mitchell C J. On integer-valued rational polynomials and depth distributions of binary codes. *IEEE Trans. on Info. Theory*, 1998, IT-44(7): 3146 − 3150.

[3] Luo Y, Fu Fangwei, Victor K V Wei. On the depth distribution of linear codes. *IEEE Trans. on Info. Theory*. 2000, IT-46(6): 2197 − 2203.

[4] 岳殿武，Shwedyk E. 纠错码的深度分布在其周期分布研究中的应用. 应用科学学报，2001, 19(3): 189 − 192.

[5] Wan Z X. Quaternary Codes, Singapore: World Scientific, 1997, 1-9: 96 − 98.

[6] 朱士信. Z_4 线性码的对称形式的 Macwilliams 恒等式. 电子与信息学报，2003, 25(7): 901 − 906.

[7] 杨善林，朱士信，童宏玺. 两种计算 Z_4 环上码字深度的递归算法. 中国科技大学学报，2004, 34(6): 655 − 660.

朱士信：　男，1962 年生，教授，主要从事代数编码理论及非线性移位寄存器序列的研究.

杨善林：　男，1948 年生，教授，博士生导师，研究方向为计算机安全与保密.

童宏玺：　男，1980 年生，研究生，研究方向为代数编码理论.