卡氏积码的 MDR 码和自对偶码

刘修生
（黄石理工学院 数理学院，湖北 黄石 435003）

摘 要：定义了 $Z_{r_1}, Z_{r_2}, \cdots, Z_{r_s}$ 上线性码 $C_1, C_2, \cdots, C_s$ 的卡氏积码。利用子模同构定理，研究了在 $Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_s}$ 上卡氏积码 $C_1 \times C_2 \times \cdots \times C_s$ 的秩与在 $Z_{r_1}, Z_{r_2}, \cdots, Z_{r_s}$ 码 $C_1, C_2, \cdots, C_s$ 的秩的关系，借助这一关系，得到了 MDR 码的卡氏积仍为 MDR 码和自对偶码的卡氏积码也为自对偶码。

关键词：秩；卡氏积码；极大距离码；中国剩余定理
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1000-436X(2010)03-0123-03

MDR codes and self-dual codes on Cartesian product codes

LIU Xiu-sheng
(School of Math. and Physics, Huangshi Institute Technology, Huangshi 435003, China)

Abstract: A Cartesian product code of the linear codes $C_1, \cdots, C_s$ in $Z_{r_1}, \cdots, Z_{r_s}$ was defined. According to the theorem of submodulo isomorphism, the relationship between the rank of the Cartesian product code $C_1 \times C_2 \times \cdots \times C_s$ over $Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_s}$ and $C_1, C_2, \cdots, C_s$ codes over $Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_s}$ were studied. Furthermore, it can include that Cartesian product code of MDS codes is MDR code, and so do the self -dual.

Key words: rank; Cartesian product; maximum distance with respect to rank codes; the Chinese remainder theorem

1 引言

在环 Z_k 中的一个长度为 n 的码 C 是 Z_k^n 上的一个子集。如果这个码 C 还是 Z_k^n 上的子模，则称 C 是 Z_k 上的线性码。特别地，如果码 C 是 Z_k^n 的自由子模，就说码 C 是自由的。文中所涉及的码均假设为线性码，对环绕空间附加标准内积 $[v,\omega] = \sum v_i \omega_i$。用 $C^{\perp} = \left\{ v \middle| [v,\omega] = 0, \forall \omega \in C \right\}$ 来定义码 C 的正交码。为了方便读者，叙述已有的符号如下：

$d_H(C)$ 表示码 C 的 Hamming 距离。

$W_H(C)$ 表示码 C 的 Hamming 重量。

若 C 为线性码，则 $d_H(C) = \min\left\{ W_H(c) \middle| \forall c \in C \right\}$。

由文献[1]知，Z_k^n 上任何一个有限生成子模 R 同构于：

$$\frac{Z_k}{f_1 Z_k} \times \frac{Z_k}{f_2 Z_k} \times \cdots \times \frac{Z_k}{f_n Z_k}$$

这里 f_i 是正整数且满足 $f_1 | f_2 | \cdots | f_n | k$。称 $\left\{ i \middle| f_i \neq 1 \right\}$ 为有限生成子模 R 的秩，记为 $\mathrm{rank}(R)$。注意这个有限生成子模 R 的元素个数为 $\prod_{i=1}^{n} f_i$。

文献[1]证明了：若 C 是 Z_k 上长度为 n 的码，则 $d_H(C) \leqslant n - \mathrm{rank}(C) + 1$。

为此，引进了如下定义[2]。

定义 1 如果 Z_k 上长度为 n 的线性码 C 满足：

$$d_H(C) = n - \mathrm{rank}(C) + 1$$

则称 C 是关于秩的一个极大距离码，简称 C 是 MDR 码。对于 Z_{p^k} 上的 MDR 码(p 为素数)，文献[3]给出了一个对偶和一个矩阵刻划。对于一般的整数 m，

收稿日期：2008-04-25；修回日期：2009-12-29

设它的标准分解式为 $m=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$。本文的目的是：由 $Z_{p_1^{k_1}},\cdots,Z_{p_s^{k_s}}$ 上的码 $C_1,\cdots,C_s$ 的特征来刻划 Z_m 上码 C。

2 中国剩余定理

设 r 和 k 是整数，且 $k|r$，定义如下：

$$\begin{aligned} Z_r^n &\to Z_k^n \\ \psi_k(\alpha_1,\cdots,\alpha_n) &\to \psi_k(\alpha_1,\cdots,\alpha_n) \\ &=(\alpha_1(\bmod k),\cdots,\alpha_n(\bmod k)) \end{aligned}$$

设 $m=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$ 是 m 的标准分解式，令 $r_1=p_1^{k_1},r_2=p_2^{k_2},\cdots,r_s=p_s^{k_s}$。定义：

$$Z_m^n \mapsto Z_{r_1}^n\times Z_{r_2}^n\times\cdots\times Z_{r_s}^n$$

$$\psi v=(\alpha_1,\cdots,\alpha_n)\mapsto \psi(v):=(\psi_{r_1}(v),\psi_{r_2}(v),\cdots,\psi_{r_s}(v))$$

则由中国剩余定理知 ψ 是一个环同构[4]。

对于 Z_m 中长度为 n 的码 C，定义：

$$C_i=\{\psi_{r_i}(v)|v=(\alpha_1,\cdots,\alpha_n)\in C\},\quad i=1,2,\cdots,s$$

则易验证 C_i 是 Z_{r_i} 的码，且 ψ 在 C 上的限制 ψ_C 定义为：

$$\begin{aligned} C &\mapsto C_1\times C_2\times\cdots\times C_s \\ \psi_C c &\mapsto \psi_C(c):=(\psi_{r_1}(c),\psi_{r_2}(c),\cdots,\psi_{r_s}(c)) \end{aligned}$$

是码 C 与码 $C_1\times C_2\times\cdots\times C_s$ 的一个同构，其中 $C_1\times C_2\times\cdots\times C_s$ 称为码 $C_1,C_2,\cdots,C_s$ 的卡氏积码。

由上述可见，研究 Z_m 上的码 C 可转化为研究码 $C_1,C_2,\cdots,C_s$ 的卡氏积码。

3 卡氏积码

设 $r_1,r_2,\cdots,r_s$ 是两两互质的正整数，$C_1,C_2,\cdots,C_s$ 分别是 $Z_{r_1},\cdots,Z_{r_s}$ 上的码。由上定义，这 s 个码的卡氏积码为 $C_1\times C_2\times\cdots\times C_s=\{(c_1,c_2,\cdots,c_s)|c_i\in C_i,1\leqslant i\leqslant s\}$。

引理 1 记号如上，有：

$$\mathrm{rank}((C_1\times C_2\times\cdots\times C_s))=\max\{\mathrm{rank}(C_i)\}$$

证明 由子模同构定理知 $C_1,C_2,\cdots,C_s$ 分别同构于：

$$\frac{Z_{r_1}}{f_1^1Z_{r_1}}\times\frac{Z_{r_1}}{f_2^1Z_{r_1}}\times\cdots\times\frac{Z_{r_1}}{f_n^1Z_{r_1}}$$

$$\frac{Z_{r_2}}{f_1^2Z_{r_1}}\times\frac{Z_{r_2}}{f_2^2Z_{r_1}}\times\cdots\times\frac{Z_{r_2}}{f_n^2Z_{r_1}}$$

$$\frac{Z_{r_s}}{f_1^sZ_{r_s}}\times\frac{Z_{r_s}}{f_2^sZ_{r_s}}\times\cdots\times\frac{Z_{r_s}}{f_n^sZ_{r_s}}$$

其中，对于每一个 $i\in\{1,2,\cdots,s\}$，$f_1^i,f_2^i,\cdots,f_n^i$ 是正整数，且 $f_1^i\,|\,f_2^i\,|\cdots|\,f_n^i\,|\,r_i$。

由整除的性质知，$C_1\times C_2\times\cdots\times C_s$ 也同构于：

$$\frac{Z_{r_1r_2\cdots r_s}}{f_1^1f_1^2\cdots f_1^sZ_{r_1r_2\cdots r_s}}\times\frac{Z_{r_1r_2\cdots r_s}}{f_2^1f_2^2\cdots f_2^sZ_{r_1r_2\cdots r_s}}\times\cdots\times\frac{Z_{r_1r_2\cdots r_s}}{f_n^1f_n^2\cdots f_n^sZ_{r_1r_2\cdots r_s}}$$

从而，按秩的定义知，$\mathrm{rank}((C_1\times C_2\times\cdots\times C_s))=\max\{\mathrm{rank}(C_i)\}$。

引理 2 记号如上，则

$$d_H(C_1\times C_2\times\cdots\times C_s)=\min\{d_H(C_i)\}$$

证明

$$\begin{aligned} d_H(C_1\times C_2\times\cdots\times C_s)&=\min\{d_H(c_1,c_2,\cdots,c_s)|c_i\in C_i\}\\ &=\min\{d_H(0,\cdots,0,c_i,0,\cdots,0)|c_i\in C_i\}\\ &=\min d_H(C_i) \end{aligned}$$

定理 1 设 $C_1,C_2,\cdots,C_s$ 分别是 $Z_{r_1},\cdots,Z_{r_s}$ 上的码，如果对于每一个 i，C_i 是一个 MDR 码，则 $C=C_1\times C_2\times\cdots\times C_s$ 是 MDR 码。

证明 由于 $C_1,C_2,\cdots,C_s$ 是 MDR 码，所以有：

$$d_H(C_i)=n-\mathrm{rank}(C_i)+1,i=1,2,\cdots,s$$

从而：

$$\begin{aligned} d_H(C)&=\min\{d_H(C_i)\}=\min\{n-\mathrm{rank}(C_i)+1|1\leqslant i\leqslant s\}\\ &=n-\max\{\mathrm{rank}(C_i)|1\leqslant i\leqslant s\}+1\\ &=n-\mathrm{rank}(C)+1 \end{aligned}$$

故 C 是 MDR 码。

定理 1 反之不然。

例如 设 C 是 Z_6 上具有生成矩阵：

$$\boldsymbol{G}=\begin{pmatrix}1&0&0&1\\0&3&0&3\\0&0&3&3\end{pmatrix}$$

的 MDR 码，显然 $C_1=\{\psi_2(c)|c\in C\}$ 是 Z_2 上的 MDR 码，但：

$$C_1=\{\psi_3(c)|c\in C\}=\{(0,0,0,0),(1,0,0,1),(2,0,0,2)\}$$

不是 Z_3 上的 MDR 码。

定理 2　设 $C=C_1\times C_2\times\cdots\times C_s$，则 $C^{\perp}=C_1^{\perp}\times C_2^{\perp}\times\cdots\times C_s^{\perp}$。

证明　设 $u=(u_1,u_2,\cdots,u_s)\in C_1^{\perp}\times C_2^{\perp}\times\cdots\times C_s^{\perp}$，则：

$$u_1\in C_1^{\perp},u_2\in C_2^{\perp},\cdots,u_s\in C_s^{\perp}$$

从而 $\forall v_1\in C_1,v_2\in C_2,\cdots,v_s\in C_s$，有：

$$[u_1,v_1]=0,[u_2,v_2]=0,\cdots,[u_s,v_s]=0$$

于是对于任意 $v=(v_1,v_2,\cdots,v_s)\in C$，有：

$$[u,v]=[u_1,v_1]+[u_2,v_2]+\cdots+[u_s,v_s]=0$$

故 $u\in C^{\perp}$，因此 $C_1^{\perp}\times C_2^{\perp}\times\cdots\times C_s^{\perp}\subset C^{\perp}$。

反过来，若 $\omega=(\omega_1,\omega_2,\cdots,\omega_s)\in C^{\perp}$，则对任意 $v=(v_1,v_2,\cdots,v_s)\in C$，有：

$$[\omega,v]=[\omega_1,v_1]+[\omega_2,v_2]+\cdots+[\omega_s,v_s]=0$$

取 $v_2=\cdots=v_s=0,v_1$ 为 C_1 中任意元，则 $[\omega,v]=[\omega_1,v_1]=0$，故 $\omega_1\in C_1^{\perp}$。

取 $v_1=v_3=\cdots=v_s=0,v_2$ 为 C_2 中任意元，则 $[\omega,v]=[\omega_2,v_2]=0$。

同理有 $\omega_2\in C_2^{\perp}$，如此类推，有 $\omega_3\in C_3^{\perp},\cdots\omega_s\in C_s^{\perp}$。

因此，$\omega\in C_1^{\perp}\times C_2^{\perp}\times\cdots\times C_s^{\perp}$。从而 $C^{\perp}\subset C_1^{\perp}\times C_2^{\perp}\times\cdots\times C_s^{\perp}$。

综合得：$C^{\perp}=C_1^{\perp}\times C_2^{\perp}\times\cdots\times C_s^{\perp}$。

推论 1　$C=C_1\times C_2\times\cdots\times C_s$ 自对偶码的充要条件为 $C_1,C_2,\cdots,C_s$ 都是自对偶码。

证明　充分性显然。下面证明必要性。

对于每一个 C_i，证明 $C_i=C_i^{\perp}$。

事实上，对任意的 $c_i\in C_i^{\perp}$，有 $(0,\cdots,0,c_i,0,\cdots,0)\in C_1^{\perp}\times\cdots\times C_i^{\perp}\times\cdots\times C_s^{\perp}$。由 $C=C_1\times C_2\times\cdots\times C_s$ 为自对偶码知，$(0,\cdots,0,c_i,0,\cdots,0)\in C_1\times\cdots\times C_i\times\cdots\times C_s$。故 $c_i\in C_i$，从而，$C_i^{\perp}\subset C_i$。

反过来，$\forall c_i\in C_i$，则：

$$\begin{aligned}&(0,\cdots,0,c_i,0,\cdots,0)\in C_1\times\cdots\times C_i\times\cdots\times C_s\\&=C_1^{\perp}\times\cdots\times C_i^{\perp}\times\cdots\times C_s^{\perp}\end{aligned}$$

故又有 $c_i\in C_i^{\perp}$，从而 $C_i\subset C_i^{\perp}$。

综合得 $C_i=C_i^{\perp}$。因此 $C_1,C_2,\cdots,C_s$ 都是自对偶码。

参考文献：

[1] SHIROMOTO K. A singleton bound for codes over finite rings[J]. Journal of Alagebraic Combinatorices,2000,(12): 95-98.

[2] DOUGHERTY S T, SHIROMOTO K. MDR codes over Z_k[J]. IEEE Transactions on Information Theory, 2000,46(1): 265-269.

[3] SHIROMOTO K. Note on MDS codes over the integers modulo P^m[J]. Hokkaido Math Journal, 2000, 29:119-148.

[4] DOUGHIERTY S T, HARADA M, SOLE P. Self-dual odes over rings and the Chinese remainder theorem[J]. Hokkaido Math Journal, 1999, 28: 253-283.

作者简介：

刘修生（1960-），男，湖北大冶人，黄石理工学院数理学院院长、教授、硕士生导师，主要研究方向为群与代数编码、多重线性代数等。