2009,**29A**(4):891–897

Acta Mathematica Scientia
数学物理学报

http://actams.wipm.ac.cn

四元 $\mathcal{ZRM}$ 码的研究 *

裴军莹　王海华　崔杰

(苏州大学数学科学学院　江苏苏州 215006)

摘要: 为了讨论二元 Reed-Muller 码的 $\mathbb{Z}_4$ 线性, 文献中先后介绍了两类 $\mathbb{Z}_4$ 线性码, 分别记为 $\mathcal{ZRM}(r,m)$ 与 $\mathcal{QRM}(r,m)$, 它们在 Gray 映射下的二元像记为 $ZRM(r,m)$ 与 $QRM(r,m)$. 该文系统地讨论了这两类 $\mathbb{Z}_4$ 线性码. 计算了 $\mathcal{ZRM}(r,m)$ 与 $\mathcal{QRM}(r,m)$ 的类型, 证明当 $3 \le r \le m-1$ 时, $ZRM(r,m)$ 是二元线性码, 而 $QRM(r,m)$ 是非线性的; 并且, 由 $QRM(r,m)$ 张成的二元线性码恰是 $ZRM(r,m)$. 最后, 对于非线性码 $QRM(r,m)$, 讨论了它的秩与核.

关键词: Reed-Muller 码; Gray 映射; 二元像; $\mathcal{ZRM}$ 码; $\mathcal{QRM}$ 码.

MR(2000) 主题分类: 11T71　**中图分类号**: O157.4　**文献标识码**: A

文章编号: 1003-3998(2009)04-891-07

1 引言

(I) 二元 Reed-Muller 码.

令 $AG(m,2)$ 是有限域 $\mathbb{F}_2$ 上的 m 维仿射空间, $\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{m-1}$ 是它的标准基. 对于 $0 \le j \le 2^m-1$, 设 j 的 2-adic 展开式为 $j = \sum\limits_{i=0}^{m-1} \xi_{ij} 2^i$, 其中 $\xi_{ij} \in \mathbb{F}_2$, 令 $\mathbf{x}_j = \sum\limits_{i=0}^{m-1} \xi_{ij}\mathbf{u}_i$, 则 $\mathbf{x}_j$ 表示仿射空间 $AG(m,2)$ 中的所有点. 记 $n = 2^m$, 令 E 为 $m \times n$ 矩阵, 其列向量为 $\mathbf{x}_j, 0 \le j \le 2^m-1$. 对于 $i = 0,1,\cdots,m-1$, 用 $\mathbf{v}_i$ 表示 E 的第 i 行, 则 $\mathbf{v}_i$ 就是 $AG(m,2)$ 中的超平面 $A_i = \{\mathbf{x}_j \in AG(m,2) \mid \xi_{ij} = 1\}$ 的特征函数, 而 $AG(m,2)$ 的特征函数为全 1 向量 $\mathbf{1} = (1,1,\cdots,1)$. 对于任意的 $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$, 定义运算 $\mathbf{ab} = (a_0b_0, a_1b_1, \cdots, a_{n-1}b_{n-1})$. 我们知道, 所有乘积 $\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_s}$, $0 \le s \le m$ 是 $\mathbb{Z}_2$ 线性无关的, 构成 $\mathbb{F}_2^n$ 的一组基, 其中当 $s = 0$ 时, 我们约定乘积表示向量 $\mathbf{1}$.

对于 $0 \le r \le m$, 以所有乘积 $\mathbf{v}_{i_1}\mathbf{v}_{i_2}\cdots\mathbf{v}_{i_s}$ $(0 \le s \le r)$ 作为一组基所张成的线性码称为 r 阶二元 Reed-Muller 码, 记为 $RM(r,m)$. 显然, $RM(r,m)$ 的维数为 $1 + \binom{m}{1} + \cdots + \binom{m}{r}$. 以信息率来说, Reed-Muller 码并不是一种很好的码, 但它的优点是易于解码, 从而有着广泛的实际应用. 关于 Reed-Muller 码的详细介绍, 见参考文献 [1].

(II) $\mathbb{Z}_4$ 线性码与 Gray 映射.

令 $\mathbb{Z}_4$ 是整数环模 4 的剩余类环, $\mathbb{Z}_4^n$ 是 $\mathbb{Z}_4$ 上 n 元向量的集合. $\mathbb{Z}_4^n$ 中的任一 $\mathbb{Z}_4$ 子模 $\mathcal{C}$ 就称为一个 $\mathbb{Z}_4$ 线性码, $\mathcal{C}$ 的类型定义为它作为 Abel 群的类型.

收稿日期: 2007-11-05; 修订日期: 2008-12-18

* 基金项目: 国家自然科学基金 (60603016) 与 973 重大项目 (2006CB 805900) 资助

定义三个由 $\mathbb{Z}_4$ 到 $\mathbb{Z}_2$ 的映射

$$\alpha: 0 \longmapsto 0,\ 1 \longmapsto 1,\ 2 \longmapsto 0,\ 3 \longmapsto 1;$$
$$\beta: 0 \longmapsto 0,\ 1 \longmapsto 0,\ 2 \longmapsto 1,\ 3 \longmapsto 1;$$
$$\gamma: 0 \longmapsto 0,\ 1 \longmapsto 1,\ 2 \longmapsto 1,\ 3 \longmapsto 0.$$

这三个映射可以自然地推广到 $\mathbb{Z}_4^n$ 上，我们把推广后的映射仍分别记为 α, β, γ. 定义

$$\phi: \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n},\ \mathbf{c} \longmapsto \phi(\mathbf{c}) = (\beta(\mathbf{c}), \gamma(\mathbf{c}))$$

为 Gray 映射. 显然，对于任意的 $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_4^n$, 有

$$\phi(\mathbf{x}+\mathbf{y}) = \phi(\mathbf{x}) + \phi(\mathbf{y}) + \phi(2\alpha(\mathbf{x})\alpha(\mathbf{y})). \tag{1}$$

令 $\mathcal{C}$ 是一个 $\mathbb{Z}_4$ 线性码， $\phi(\mathcal{C})$ 称为 $\mathcal{C}$ 在 Gray 映射下的二元像. 下面这个引理给出了 $\phi(\mathcal{C})$ 是线性码的一个判别条件.

引理 1[2] 令 $\mathcal{C}$ 是 $\mathbb{Z}_4$ 线性码， $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_m$ 是 $\mathcal{C}$ 的一组生成元，且 $C = \phi(\mathcal{C})$. 则 C 是线性码当且仅当对于任意的 $1 \le i \le j \le m$, $2\alpha(\mathbf{x}_i)\alpha(\mathbf{x}_j) \in \mathcal{C}$.

令 C 是一个二元线性码，若 C 是某个 $\mathbb{Z}_4$ 线性码 $\mathcal{C}$ 在 Gray 映射下的二元像，则称 C 是 $\mathbb{Z}_4$ 线性的. 为了讨论二元 Reed-Muller 码的 $\mathbb{Z}_4$ 线性， Hammons 等人 [3] 与 Wan[2] 介绍了两类 $\mathbb{Z}_4$ 线性码，分别记为 $\mathcal{ZRM}(r,m)$ 与 $\mathcal{QRM}(r,m)$. 下面，我们给出它们的定义.

令 $G(r,m)$ 表示 $RM(r,m)$ 的生成矩阵，我们约定 $RM(-1,m) = RM(m+1,m) = \{\mathbf{0}\}$, 且生成矩阵 $G(-1,m) = G(m+1,m) = (\mathbf{0})$. 对于任意的 $0 \le r \le m$, 定义 $\mathcal{QRM}(r,m)$ 是长度为 2^m 的 $\mathbb{Z}_4$ 线性码，其生成矩阵为

$$\begin{pmatrix} G(r-1,m) \\ 2G(r,m) \end{pmatrix}.$$

令 $QRM(r,m) = \phi(\mathcal{QRM}(r,m))$ 是它的二元像. 定义 $\mathcal{ZRM}(r,m)$ 是由 $RM(r-1,m)$ 与 $2RM(r,m)$ 的码元在 $\mathbb{Z}_4^n$ 中所张成的长度为 2^m 的 $\mathbb{Z}_4$ 线性码，即

$$\mathcal{ZRM}(r,m) = \langle RM(r-1,m),\ 2RM(r,m)\rangle_4.$$

我们把它的二元像记为 $ZRM(r,m)$.

Hammons 等人 [3] 证明了对于 $r = 0, 1, 2, m$ 及 $m+1$, $\mathcal{ZRM}(r,m)$ 的二元像恰是 Reed-Muller 码 $RM(r,m+1)$, 并猜想对于其余的 r, $RM(r,m+1)$ 不是 $\mathbb{Z}_4$ 线性的. 这一猜想最终由 Hou 等人 [4] 证明. 对于相同的 r, Wan[2] 证明 $\mathcal{QRM}(r,m)$ 的二元像也是 $RM(r,m+1)$. 因此，当 $r = 0, 1, 2, m$ 及 $m+1$ 时，这两类 $\mathbb{Z}_4$ 线性码是完全一样的. 本文系统地研究了这两类 $\mathbb{Z}_4$ 线性码，表明当 $3 \le r \le m-1$ 时，它们是完全不同的. 在第 2 节中，我们计算了 $\mathcal{ZRM}(r,m)$ 与 $\mathcal{QRM}(r,m)$ 的类型, 证明它们的二元像 $ZRM(r,m)$ 是线性的, 而 $QRM(r,m)$ 是非线性的，但 $QRM(r,m)$ 所张成的线性码恰是 $ZRM(r,m)$. 最后，在第 3 节中对于非线性码 $QRM(r,m)$, 讨论了它的秩与核.

2 $\mathcal{ZRM}(r,m)$ 码与 $\mathcal{QRM}(r,m)$ 码

下面假定 $3 \le r \le m-1$.

对于任意的 $\mathbf{x},\mathbf{y}\in\mathbb{Z}_2^n$, 它们在 $\mathbb{Z}_2^n$ 中的加法记为 $\mathbf{x}+_b\mathbf{y}$. 将它们看成 $\mathbb{Z}_4$ 上的向量，为了区别，把它们在 $\mathbb{Z}_4^n$ 中的加法记为 $\mathbf{x}+\mathbf{y}$. 容易验证，对于任意的 $\mathbf{x}_1,\mathbf{x}_2,\cdots,\mathbf{x}_s\in\mathbb{Z}_2^n$,

$$\mathbf{x}_1+_b\mathbf{x}_2+_b\cdots+_b\mathbf{x}_s=(\mathbf{x}_1+\mathbf{x}_2+\cdots+\mathbf{x}_s)+2\sum_{1\le i<j\le s}\mathbf{x}_i\mathbf{x}_j. \tag{2}$$

定理 2 设 $\langle RM(r-1,m)\rangle_4$ 是由 $RM(r-1,m)$ 中的码元生成的 $\mathbb{Z}_4$ 线性码, 则 $\mathcal{ZRM}(r,m)=\langle RM(r-1,m)\rangle_4$. 并且, $\mathcal{ZRM}(r,m)$ 的类型为 $4^{k_1}2^{k_2-k_1}$, 其中 $k_1=1+\binom{m}{1}+\cdots+\binom{m}{r-1}$, $k_2=1+\binom{m}{1}+\cdots+\binom{m}{t}$, $t=\min\{2r-2,m\}$.

证 考虑与 $\mathcal{ZRM}(r,m)$ 相关联的两个 $\mathbb{Z}_2$ 线性码

$$C_1=\{\alpha(\mathbf{c})\mid\mathbf{c}\in\mathcal{ZRM}(r,m)\},$$

$$C_2=\{\beta(\mathbf{c})\mid\mathbf{c}\in\widetilde{\mathcal{ZRM}}(r,m)\},$$

其中 $\widetilde{\mathcal{ZRM}}(r,m)=\{\mathbf{c}\in\mathcal{ZRM}(r,m)\mid 2\mathbf{c}=\mathbf{0}\}$ 是 $\mathcal{ZRM}(r,m)$ 的子码. 显然, $C_1=RM(r-1,m)$, 故 $\dim C_1=1+\binom{m}{1}+\cdots+\binom{m}{r-1}=k_1$.

下面, 我们计算 C_2 的维数. 对任意的子集 $J\subseteq\{1,2,\cdots,m\}$ 满足 $\mid J\mid\le\min\{2r-2,m\}$, 存在子集 I_1, I_2 使得 $I_1\cup I_2=J$, 且 $\mid I_1\mid\le r-1,\mid I_2\mid\le r-1$, 故由 (2) 式得

$$\prod_{i\in I_1}\mathbf{v}_i+_b\prod_{i\in I_2}\mathbf{v}_i=\prod_{i\in I_1}\mathbf{v}_i+\prod_{i\in I_2}\mathbf{v}_i+2\prod_{i\in J}\mathbf{v}_i.$$

由于 $|I_1|\le r-1$, $|I_2|\le r-1$, 则 $\prod\limits_{i\in I_1}\mathbf{v}_i,\prod\limits_{i\in I_2}\mathbf{v}_i\in RM(r-1,m)$, 且 $\prod\limits_{i\in I_1}\mathbf{v}_i+_b\prod\limits_{i\in I_2}\mathbf{v}_i\in RM(r-1,m)$. 从而

$$2\prod_{i\in J}\mathbf{v}_i=\Big(\prod_{i\in I_1}\mathbf{v}_i+_b\prod_{i\in I_2}\mathbf{v}_i\Big)-\prod_{i\in I_1}\mathbf{v}_i-\prod_{i\in I_2}\mathbf{v}_i\in\langle RM(r-1,m)\rangle_4\subseteq\mathcal{ZRM}(r,m),$$

故 $2\prod\limits_{i\in J}\mathbf{v}_i\in\widetilde{\mathcal{ZRM}}(r,m)$, 则 $\prod\limits_{i\in J}\mathbf{v}_i\in C_2$. 令 $t=\min\{2r-2,m\}$. 我们知道，所有的乘积 $\prod\limits_{i\in J}\mathbf{v}_i$, $|J|\le t$, 是 $RM(t,m)$ 的一组基，故 $RM(t,m)\subseteq C_2$.

另一方面，令 $\mathcal{D}=2RM(t,m)$. 对于任意的 $\mathbf{x}\in\widetilde{\mathcal{ZRM}}(r,m)$, $\mathbf{x}$ 可以写成 $\mathbf{x}=\mathbf{x}_1+\mathbf{x}_2$, 其中 $\mathbf{x}_1\in\langle RM(r-1,m)\rangle_4\cap\widetilde{\mathcal{ZRM}}(r,m)$, $\mathbf{x}_2\in\langle 2RM(r,m)\rangle_4=2RM(r,m)$. 由于 $t\ge r$, 故 $\mathbf{x}_2\in\mathcal{D}$. 假设

$$\mathbf{x}_1=\lambda_1\mathbf{y}_1+\lambda_2\mathbf{y}_2+\cdots+\lambda_s\mathbf{y}_s, \tag{3}$$

其中 $\lambda_i\in\mathbb{Z}_4$, $\mathbf{y}_i\in RM(r-1,m)$. 对于 $i=1,2,\cdots,s$, 假设

$$\begin{aligned}\mathbf{y}_i&=\prod_{l\in I_{i1}}\mathbf{v}_l+_b\prod_{l\in I_{i2}}\mathbf{v}_l+_b\cdots+_b\prod_{l\in I_{i,h_i}}\mathbf{v}_l\\&=\prod_{l\in I_{i1}}\mathbf{v}_l+\prod_{l\in I_{i2}}\mathbf{v}_l+\cdots+\prod_{l\in I_{i,h_i}}\mathbf{v}_l+2\sum_{1\le j<k\le h_i}\prod_{l\in I_{ij}\cup I_{ik}}\mathbf{v}_l,\end{aligned} \tag{4}$$

其中 $|I_{ij}|\le r-1$. 由于对任意的 $1\le j<k\le h_i$, $|I_{ij}\cup I_{ik}|\le\min\{2r-2,m\}=t$, 故 $2\sum\limits_{1\le j<k\le h_i}\prod\limits_{l\in I_{ij}\cup I_{ik}}\mathbf{v}_l\in\mathcal{D}$. 由 (3) 和 (4) 式，可设

$$\mathbf{x}=\lambda_1'\prod_{l\in I_1}\mathbf{v}_l+\lambda_2'\prod_{l\in I_2}\mathbf{v}_l+\cdots+\lambda_w'\prod_{l\in I_w}\mathbf{v}_l+\mathbf{c},$$

其中 $\lambda_i' \in \mathbb{Z}_4$, $\mathbf{c} \in \mathcal{D}$, 且 $I_1, \cdots, I_w$ 是 $\{1, 2, \cdots, m\}$ 的不同子集，满足 $|I_i| \leq r-1$, 则

$$2\mathbf{x} = 2\lambda_1' \prod_{l \in I_1} \mathbf{v}_l + 2\lambda_2' \prod_{l \in I_2} \mathbf{v}_l + \cdots + 2\lambda_w' \prod_{l \in I_w} \mathbf{v}_l = \mathbf{0}.$$

由于 $\prod\limits_{l \in I_1} \mathbf{v}_l, \cdots, \prod\limits_{l \in I_w} \mathbf{v}_l$ 是 $\mathbb{Z}_4$ 自由的，故 $2\lambda_i' = 0$, 即 $\lambda_i' = 2\mu_i$ 对某个 $\mu_i \in \mathbb{Z}_4$, 则

$$\mathbf{x} = 2\mu_1 \prod_{l \in I_1} \mathbf{v}_l + 2\mu_2 \prod_{l \in I_2} \mathbf{v}_l + \cdots + 2\mu_w \prod_{l \in I_w} \mathbf{v}_l + \mathbf{c} \in \mathcal{D}.$$

因此， $\widetilde{\mathcal{ZRM}}(r, m) \subseteq \mathcal{D}$, 故 $C_2 = \beta(\widetilde{\mathcal{ZRM}}(r, m)) \subseteq \beta(\mathcal{D}) = RM(t, m)$.

由上可知， $C_2 = RM(t, m)$, 故 $\dim C_2 = 1 + \binom{m}{1} + \cdots + \binom{m}{t} = k_2$. 因此， $\mathcal{ZRM}(r, m)$ 的类型为 $4^{k_1} 2^{k_2 - k_1}$.

显然， $\langle RM(r-1, m) \rangle_4 \subseteq \mathcal{ZRM}(r, m)$. 在上面的讨论中，用 $\langle RM(r-1, m) \rangle_4$ 替换 $\mathcal{ZRM}(r, m)$, 同理可得 $\langle RM(r-1, m) \rangle_4$ 的类型也为 $4^{k_1} 2^{k_2 - k_1}$, 故

$$\mathcal{ZRM}(r, m) = \langle RM(r-1, m) \rangle_4. \qquad \blacksquare$$

定理 3 $\mathcal{QRM}(r, m)$ 的类型为 $4^{k_1'} 2^{k_2' - k_1'}$, 其中

$$k_1' = 1 + \binom{m}{1} + \cdots + \binom{m}{r-1}, \quad k_2' = 1 + \binom{m}{1} + \cdots + \binom{m}{r}.$$

证 考虑与 $\mathcal{QRM}(r, m)$ 相关联的两个 $\mathbb{Z}_2$ 线性码

$$C_1 = \{\alpha(\mathbf{c}) \mid \mathbf{c} \in \mathcal{QRM}(r, m)\},$$

$$C_2 = \{\beta(\mathbf{c}) \mid \mathbf{c} \in \widetilde{\mathcal{QRM}}(r, m)\},$$

其中 $\widetilde{\mathcal{QRM}}(r, m) = \{\mathbf{c} \in \mathcal{QRM}(r, m) \mid 2\mathbf{c} = \mathbf{0}\}$. 显然， C_1 的生成矩阵为 $(G(r-1, m))$, 故 $C_1 = RM(r-1, m)$, 则 $\dim C_1 = 1 + \binom{m}{1} + \cdots + \binom{m}{r-1} = k_1'$; 并且， $\widetilde{\mathcal{QRM}}(r, m)$ 的生成矩阵为 $(2G(r, m))$, 故 C_2 的生成矩阵为 $(G(r, m))$, 则 $C_2 = RM(r, m)$, 从而 $\dim C_2 = 1 + \binom{m}{1} + \cdots + \binom{m}{r} = k_2'$. 因此， $\mathcal{QRM}(r, m)$ 的类型为 $4^{k_1'} 2^{k_2' - k_1'}$. $\blacksquare$

注 当 $3 \leq r \leq m-1$ 时， $t = \min\{2r-2, m\} \neq r$, 故由定理 2 与 3 知 $\mathcal{ZRM}(r, m)$ 与 $\mathcal{QRM}(r, m)$ 具有不同的类型，故是不同的两类 $\mathbb{Z}_4$ 线性码.

定理 4 令 C 是长度为 n 的 $\mathbb{Z}_2$ 线性码， $\mathcal{C} = \langle C \rangle_4$ 是由 C 在 $\mathbb{Z}_4^n$ 中张成的 $\mathbb{Z}_4$ 线性码，则二元像 $\phi(\mathcal{C})$ 是长度为 $2n$ 的 $\mathbb{Z}_2$ 线性码.

证 对于任意的 $\mathbf{x}, \mathbf{y} \in C$, 由 (2) 式可得

$$2\alpha(\mathbf{x})\alpha(\mathbf{y}) = 2\mathbf{x}\mathbf{y} = (\mathbf{x} +_b \mathbf{y}) - (\mathbf{x} + \mathbf{y}) \in \mathcal{C},$$

故由引理 1 知 $\phi(\mathcal{C})$ 是线性的. $\blacksquare$

由定理 2 与 4 知

推论 5 二元像 $ZRM(r, m) = \phi(\mathcal{ZRM}(r, m))$ 是长度为 2^{m+1} 的 $\mathbb{Z}_2$ 线性码. 并且， $\dim ZRM(r, m) = k_1 + k_2$, 其中 k_1 与 k_2 由定理 2 给出.

定理 6 二元像 $QRM(r, m) = \phi(\mathcal{QRM}(r, m))$ 是长度为 2^{m+1} 的二元非线性码.

证 否则，对于任意的 $\mathbf{x}, \mathbf{y} \in \mathcal{QRM}(r, m)$, 由引理 1 得 $2\alpha(\mathbf{x})\alpha(\mathbf{y}) \in \widetilde{\mathcal{QRM}}(r, m)$, 其中 $\widetilde{\mathcal{QRM}}(r, m) = \{\mathbf{c} \in \mathcal{QRM}(r, m) \mid 2\mathbf{c} = \mathbf{0}\}$. 由定理 3 的证明知 $\widetilde{\mathcal{QRM}}(r, m) = 2RM(r, m)$.

令 I_1, I_2 是 $\{1,2,\cdots,m\}$ 的子集，满足 $|I_1|=|I_2|=r-1$, 且 $|I_1\cup I_2|>r$. 令 $\mathbf{x}=\prod\limits_{i\in I_1}\mathbf{v}_i$, $\mathbf{y}=\prod\limits_{i\in I_2}\mathbf{v}_i$, 则 $\mathbf{x},\mathbf{y}\in\mathcal{QRM}(r,m)$, 而 $2\alpha(\mathbf{x})\alpha(\mathbf{y})=2\prod\limits_{i\in I_1\cup I_2}\mathbf{v}_i\notin 2RM(r,m)$, 矛盾. ∎

尽管 $ZRM(r,m)$ 是线性的，而 $QRM(r,m)$ 是非线性码，但下面这个定理表明二者也有一定的联系. 事实上，由 $QRM(r,m)$ 张成的线性码恰是 $ZRM(r,m)$.

定理 7 令 $\langle QRM(r,m)\rangle_2$ 是由 $QRM(r,m)$ 张成的线性码，则

$$\langle QRM(r,m)\rangle_2=ZRM(r,m).$$

证 显然，$\langle QRM(r,m)\rangle_2\subseteq ZRM(r,m)$. 对于任意的子集 $I\subseteq\{1,2,\cdots,m\}$ 满足 $|I|\le r-1$, 有 $\prod\limits_{i\in I}\mathbf{v}_i\in\mathcal{QRM}(r,m)$, 故

$$\phi\Big(\prod_{i\in I}\mathbf{v}_i\Big)=\Big(\mathbf{0},\prod_{i\in I}\mathbf{v}_i\Big)\in\langle QRM(r,m)\rangle_2. \tag{5}$$

对任意子集 $J\subseteq\{1,2,\cdots,m\}$ 满足 $|J|\le\min\{2r-2,m\}$, 存在子集 $I_1,I_2\subseteq\{1,2,\cdots,m\}$ 使得 $|I_1|\le r-1,|I_2|\le r-1$, 且 $I_1\cup I_2=J$, 则 $\prod\limits_{i\in I_1}\mathbf{v}_i$, $\prod\limits_{i\in I_2}\mathbf{v}_i\in\mathcal{QRM}(r,m)$. 由 (1) 式得

$$\phi\Big(2\prod_{i\in I_1}\mathbf{v}_i\prod_{i\in I_2}\mathbf{v}_i\Big)=\phi\Big(\prod_{i\in I_1}\mathbf{v}_i+\prod_{i\in I_2}\mathbf{v}_i\Big)-_b\phi\Big(\prod_{i\in I_1}\mathbf{v}_i\Big)-_b\phi\Big(\prod_{i\in I_2}\mathbf{v}_i\Big)\in\langle QRM(r,m)\rangle_2,$$

故

$$\phi\Big(2\prod_{i\in I_1}\mathbf{v}_i\prod_{i\in I_2}\mathbf{v}_i\Big)=\phi\Big(2\prod_{i\in J}\mathbf{v}_i\Big)=\Big(\prod_{i\in J}\mathbf{v}_i,\prod_{i\in J}\mathbf{v}_i\Big)\in\langle QRM(r,m)\rangle_2. \tag{6}$$

由于向量 $(\mathbf{0},\prod\limits_{i\in I}\mathbf{v}_i)$ 与 $(\prod\limits_{i\in J}\mathbf{v}_i,\prod\limits_{i\in J}\mathbf{v}_i)$, 其中 $|I|\le r-1$, $|J|\le\min\{2r-2,m\}$, 是 $\mathbb{Z}_2$ 线性无关的，故由 (5) 和 (6) 式知 $\dim\langle QRM(r,m)\rangle_2\ge\sum\limits_{i=0}^{r-1}\binom{m}{i}+\sum\limits_{i=0}^{t}\binom{m}{i}=\dim ZRM(r,m)$. 因此，$\langle QRM(r,m)\rangle_2=ZRM(r,m)$. ∎

定理 7 的证明过程实际上给出了二元线性码 $ZRM(r,m)$ 的生成矩阵.

推论 8 令 $t=\min\{2r-2,m\}$, 则二元像 $ZRM(r,m)$ 是长度为 2^{m+1} 的二元线性码，其生成矩阵为

$$\begin{pmatrix}0 & G(r-1,m)\\ G(t,m) & G(t,m)\end{pmatrix}.$$

3 $QRM(r,m)$ 的秩与核

Pujol 与 Rifa[5] 对二元非线性码定义了秩与核的概念. 令 C 是 $\mathbb{Z}_2^n$ 的子集，$\langle C\rangle_2$ 是由 C 张成的线性码，则 $\langle C\rangle_2$ 的维数称为 C 的秩. 假定 $\mathbf{0}\in C$, 令

$$\ker C=\{\mathbf{x}\in C\mid\mathbf{x}+C=C\},$$

称为 C 的核. 显然，$\ker C$ 是包含在 C 中的一个线性码. 这一节中，我们将讨论二元非线性码 $QRM(r,m)$ 的秩与核. 由定理 7 知 $\langle QRM(r,m)\rangle_2=ZRM(r,m)$, 故我们有

定理 9 二元非线性码 $QRM(r,m)$ 的秩为 k_1+k_2, 其中 k_1, k_2 由定理 2 给出.

引理 10 当 $3 \le r \le m-1$ 时，令 $\mathcal{C}_1$ 是 $\mathcal{QRM}(r,m)$ 的子码，其生成矩阵为

$$\begin{pmatrix} G(1,m) \\ 2G(r,m) \end{pmatrix},$$

则 $\phi(\mathcal{C}_1)$ 是长度为 2^{m+1} 的二元线性码，其生成矩阵为

$$\begin{pmatrix} 0 & G(1,m) \\ G(r,m) & G(r,m) \end{pmatrix}. \tag{7}$$

故 $\dim\,\phi(\mathcal{C}_1) = k_2' + (m+1)$, 其中 k_2' 由定理 3 给出.

证 由引理 1, 容易验证 $\phi(\mathcal{C}_1)$ 是线性的. 同定理 3 的证明一样，我们可得 $\mathcal{C}_1$ 的类型为 $4^{m+1}2^{k_2'-(m+1)}$, 故 $\dim\phi(\mathcal{C}_1) = k_2' + (m+1)$. 显然

$$\phi(\mathbf{1}) = (\mathbf{0},\mathbf{1}) \in \phi(\mathcal{C}_1),$$

$$\phi(\mathbf{v}_i) = (\mathbf{0},\mathbf{v}_i) \in \phi(\mathcal{C}_1), \quad i = 1,2,\cdots,m.$$

并且，对于任意子集 $J \subseteq \{1,2,\cdots,m\}$ 满足 $|J| \le r$, 我们知道 $2\prod\limits_{i\in J}\mathbf{v}_i \in \mathcal{C}_1$, 故

$$\phi\Big(2\prod_{i\in J}\mathbf{v}_i\Big) = \Big(\prod_{i\in J}\mathbf{v}_i, \prod_{i\in J}\mathbf{v}_i\Big) \in \phi(\mathcal{C}_1).$$

由于向量 $(\mathbf{0},\mathbf{v}_i)$, $i = 1,2,\cdots,m$, $(\mathbf{0},\mathbf{1})$ 与 $(\prod\limits_{i\in J}\mathbf{v}_i, \prod\limits_{i\in J}\mathbf{v}_i)$, $|J| \le r$ 线性无关，故这 $k_2' + (m+1)$ 个向量组成 $\phi(\mathcal{C}_1)$ 的一组基，则 (7) 式是 $\phi(\mathcal{C}_1)$ 的生成矩阵. ∎

定理 11 $QRM(r,m)$ 的核具有生成矩阵如 (7) 式，故 $\ker(QRM(r,m))$ 的维数为 $k_2' + (m+1)$, 其中 k_2' 由定理 3 给出.

证 对于任意的 $\mathbf{c} = \phi(\mathbf{x}) \in QRM(r,m)$, 由 (1) 式可得 $\mathbf{c} \in \ker(QRM(r,m))$ 当且仅当对于任意的 $\mathbf{b} = \phi(\mathbf{y}) \in QRM(r,m)$, 有

$$\begin{aligned} \mathbf{c} +_b \mathbf{b} &= \phi(\mathbf{x}) +_b \phi(\mathbf{y}) = \phi(\mathbf{x}+\mathbf{y}) +_b \phi(2\alpha(\mathbf{x})\alpha(\mathbf{y})) \\ &= \phi(\mathbf{x}+\mathbf{y}+2\alpha(\mathbf{x})\alpha(\mathbf{y})) \in QRM(r,m), \end{aligned}$$

即 $\mathbf{x}+\mathbf{y}+2\alpha(\mathbf{x})\alpha(\mathbf{y}) \in \mathcal{QRM}(r,m)$, 从而 $2\alpha(\mathbf{x})\alpha(\mathbf{y}) = 2\mathbf{xy} \in \mathcal{QRM}(r,m)$. 因此，令 $\mathcal{C} = \phi^{-1}(\ker(QRM(r,m)))$, 则 $\mathbf{x} \in \mathcal{C}$ 当且仅当对于任意的 $\mathbf{y} \in \mathcal{QRM}(r,m)$, $2\mathbf{xy} \in \mathcal{QRM}(r,m)$. 易知 $\mathcal{C}$ 是 $\mathcal{QRM}(r,m)$ 的一个 $\mathbb{Z}_4$ 线性子码. 事实上，对于任意的 $\mathbf{x}_1,\mathbf{x}_2 \in \mathcal{C}$ 及 $\mathbf{y} \in \mathcal{QRM}(r,m)$, 我们有 $2\mathbf{x}_1\mathbf{y}, 2\mathbf{x}_2\mathbf{y} \in \mathcal{QRM}(r,m)$, 故 $2(\mathbf{x}_1+\mathbf{x}_2)\mathbf{y} \in \mathcal{QRM}(r,m)$, 则 $\mathbf{x}_1+\mathbf{x}_2 \in \mathcal{C}$. 我们要确定 $\ker(QRM(r,m))$, 只要确定 $\mathcal{C}$ 就可以了.

令 $\mathcal{C}_1$ 是引理 10 中给出的 $\mathcal{QRM}(r,m)$ 的子码. 对于任意的 $\mathbf{y} \in \mathcal{QRM}(r,m)$, 设

$$\mathbf{y} = \sum_{i=1}^{s}\prod_{k\in I_i}\mathbf{v}_k + \sum_{j=1}^{w}2\prod_{k\in J_j}\mathbf{v}_k,$$

其中 $|I_i| \le r-1$, $|J_j| \le r$. 对于 $l = 1,2,\cdots,m$, 由于

$$2\mathbf{v}_l\mathbf{y} = \sum_{i=1}^{s}2\prod_{k\in I_i\cup\{l\}}\mathbf{v}_k \in \mathcal{QRM}(r,m)$$

及

$$2\mathbf{1}\mathbf{y} = 2\mathbf{y} \in \mathcal{QRM}(r,m),$$

故 $\mathbf{v}_l \in \mathcal{C}$, $l = 1,2,\cdots,m$, 且 $\mathbf{1} \in \mathcal{C}$. 显然， $2\prod_{i\in J}\mathbf{v}_i \in \mathcal{C}, |J| \le r$. 因此， $\mathcal{C}_1 \subseteq \mathcal{C}$.

另一方面，对于任意的

$$\mathbf{x} = \sum_{i=1}^{s}\prod_{k\in I_i}\mathbf{v}_k + \sum_{j=1}^{w}2\prod_{k\in J_j}\mathbf{v}_k \in \mathcal{C}, \tag{8}$$

其中 I_i, J_j 是 $\{1,2,\cdots,m\}$ 的不同子集，满足 $|I_i| \le r-1$, $|J_j| \le r$. 不失一般性，我们设 $|I_1|$ 是 $I_i, i = 1,2,\cdots,s$ 中势最大的子集. 若 $|I_1| \ge 2$, 则存在子集 $I \subseteq \{1,2,\cdots,m\}\backslash I_1$ 满足 $|I| \le r-1$, 且 $|I \cup I_1| = r+1$. 令 $\mathbf{y} = \prod_{k\in I}\mathbf{v}_k$, 则 $\mathbf{y} \in \mathcal{QRM}(r,m)$, 而

$$2\mathbf{x}\mathbf{y} = 2\prod_{k\in I_1\cup I}\mathbf{v}_k + 2\sum_{i=2}^{s}\Big(\prod_{k\in I_i\cup I}\mathbf{v}_k\Big).$$

注意到 $I_1 \cup I \ne I_i \cup I$, 对任意的 $i = 2,\cdots,s$. 事实上，若 $I_1 \cup I = I_i \cup I$ 对某个 $i = 2,\cdots,s$, 则 $I_1 \subseteq I_i$, 而 I_1 的势最大，故 $I_1 = I_i$, 矛盾. 由于 $|\, I_1 \cup I \,| = r+1$, 故 $2\mathbf{x}\mathbf{y} \notin \mathcal{QRM}(r,m)$, 与 $\mathcal{C}$ 中码元应满足的条件矛盾. 因此，在 (8) 式中， $|I_i| \le 1$, $i = 1,2,\cdots,s$, 故 $\mathbf{x} \in \mathcal{C}_1$.

由上可知， $\mathcal{C} = \phi^{-1}(\ker(QRM(r,m))) = \mathcal{C}_1$, 故 $\ker(QRM(r,m)) = \phi(\mathcal{C}_1)$. ∎

参 考 文 献

[1] van Lint J H. Introduction to Coding Theory. New York: Springer-Verlag, 1982: 47–52

[2] Wan Zhexian. Quaternary Codes. Singappre: World Scientific Publiding Co.Pte.Ltd, 1998: 53–61

[3] Hammons A R, Kumar P V, Calderbank A R, et al. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans Inform Theory, 1994, **40**: 301–319

[4] Hou J X D, Lahtonen T, Koponen S. The Reed-Muller code $R(r,m)$ is not $\mathbb{Z}_4$-linear for $3 \le r \le m-2$. IEEE Trans Inform Theory, 1998, **44**: 798–799

[5] Pujol J, Rifa J. Translation invariant propelinear codes. IEEE Trans Inform Theory, 1997, **43**: 590–598

Study on Quaternary $\mathcal{ZRM}$ Codes

Pei Junying Wang Haihua Cui Jie

(*Department of Mathematics, Soochow University, Jiangsu Suzhou 215006*)

Abstract: In the literature two classes of $\mathbb{Z}_4$ linear codes were defined to discuss the $\mathbb{Z}_4$ linearity of binary Reed-Muller codes, they are denoted by $\mathcal{ZRM}(r,m)$ and $\mathcal{QRM}(r,m)$, and their binary images under the Gray map are denoted by $ZRM(r,m)$ and $QRM(r,m)$ respectively. In this correspondence, the types of $\mathcal{ZRM}(r,m)$ and $\mathcal{QRM}(r,m)$ are computed respectively. When $3 \le r \le m-1$, it is shown that the binary image $ZRM(r,m)$ is linear while $QRM(r,m)$ is nonlinear. Moreover, the linear code spanned by $QRM(r,m)$ is proved to be $ZRM(r,m)$. Finally, the rank and the kernel are determined for the nonlinear code $QRM(r,m)$.

Key words: Reed-Muller code; Gray map; Binary image; $\mathcal{ZRM}$ code; $\mathcal{QRM}$ code.

MR(2000) Subject Classification: 11T71