一阶 R-M 码陪集重量分布的线性特性*

李子臣　　张卷美

(北京邮电大学信息安全中心 126 信箱, 北京 100876)　　(焦作工学院基础部, 河南焦作 454159)

摘要　利用 Boll 函数和 Hadamard 变换给出一阶 R-M 码 $R(1,m)$ 陪集元的重量表达式, 并给出障集重量分布的线性特性和证明。

关键词　Bool 函数, 陪集　重量分布

Linear Characteristic of Weight Distribution of Elements in the Coset of One Order R-M Codes

Li Zichen

(Beijing University of Posts and Telecommunications, 126#, Beijing 100876)

Zhang Juanmei

(Jiaozou Institute of Techology, Jiaozou 454159)

Abstract　In this paper, by the Bool function and Hadmard transformation, the formula of weight distribution for the elements in the coset of one order R-M codes $R(1,m)$ is given and the linear characteristic of weight distribution in the coset and its proof are also given.

Keywords　bool function; coset; weight distribution

1　一阶 R-M 码 R(1,m)

Reed-Muller 码(简称 R-M 码)是最古老也是研究最深入的一种线性分组码[1]。

我们知道 Bool 函数[2] $f(x_1, x_2, \cdots, x_m)$ 与其真值表是相互唯一确定的, 而每一个 Bool 函数都可以用多项式表示为:

$$f(x_1, x_2, \cdots, x_m) = \sum_{a \in V^m} g(a) x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} \tag{1.1}$$

这里 $a \in V^m$ 表示 a 是 GF(2) 中的 m 维向量, $g(a) = 0$ 或 1。令 $a = (a_1, a_2, \cdots, a_m)$, 若 $a_i = 0$, $x_i^{a_i} = 1$, 若 $a_i = 1$, $x_i^{a_i} = x_i$。

Bool 函数中每一项 $x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$ 称为函数的单项式, 而整数 $\sum_{i=1}^{m} a_i = w(a)$ 称为单项式的阶数。函数所包含单项式阶数最大值称为此 Bool 函数的阶数。

定义 1.1　r 阶 R-M 码 $R(r,m)$ 就是一切阶数不超过 r 的 m 元 Bool 函数的真值表作为码字而得到的码。

由于 Bool 函数与其真值表是相互唯一确定的, 因此 Bool 函数为 $f(x_1, x_2, \cdots, x_m)$, 那么码长为 $n = 2^m$, 而任何一个阶数不超过 r 的 Bool 函数总可以表示为阶数 0、阶为 1、…、阶数为 r 的单项式之和, 因此阶

* 本文于 1997 年 1 月 20 日收到

定理 3.1　设 $f(x)$ 为一 m 元 Bool 函数，$f(x)$ 与 $R(1,m)$ 中形如 $a_0+\sum_{i=1}^{m}a_ix_i$ 的码字的 Hamming 距离

$$d\left(f(x),\ a_0+\sum_{i=1}^{m}a_ix_i\right)=1/2\left[2^m-(-1)^{a_0}\hat{F}(a)\right] \tag{3.2}$$

其中：$F(x)=(-1)^{f(x)}$，$a_0\in GF(2)$，$a\in V^m$，$a=(a_1,a_2,\cdots,a_m)$。

证明　由(3.1)式可得：

$$\hat{F}(a)=(a_1,a_2,\cdots,a_m)=\sum_{x\in V^m}(-1)^{x*a}F(x)=\sum_{x\in V^m}(-1)^{x*a+f(x)}=\sum_{x\in V^m}(-1)^{\sum_{i=1}^{m}x_ia_i+f(x)}$$

因此：$(-1)^{a_0}\hat{F}(a)=(-1)^{a_0}\sum_{x\in V^m}(-1)^{\sum_{i=1}^{m}x_ia_i+f(x)}=\sum_{x\in V^m}(-1)^{a_0+\sum_{i=1}^{m}x_ia_i+f(x)}$

上式中 $a_0+\sum_{i=1}^{m}x_ia_i+f(x)$ 取值为 0 或 1。

因此 $(-1)^{a_0}\hat{F}(a)$ 就等于所有 V^m 中使 $a_0+\sum_{i=1}^{m}x_ia_i+f(x)$ 等于零的个数减去使 $a_0+\sum_{i=1}^{m}x_ia_i+f(x)$ 等于 1 的个数。

$$(-1)^{a_0}\hat{F}(a)=\left[2^m-\omega\left(a_0+\sum_{i=1}^{m}x_ia_i+f(x)\right)\right]-\omega\left(a_0+\sum_{i=1}^{m}a_ix_i+f(x)\right)$$

$$=2^m-2\omega\left(a_0+\sum_{i=1}^{m}a_ix_i+f(x)\right)$$

因此，$\omega\left(a_0+\sum_{i=1}^{m}a_ix_i+f(x)\right)=\frac{1}{2}\left[2^m-(-1)^{a_0}\hat{F}(a)\right]$

即，$d\left(f(x),\ a_0+\sum_{i=1}^{m}a_ix_i\right)=\frac{1}{2}\left[2^m-(-1)^{a_0}\hat{F}(a)\right]$

所以，一阶 R-M 码 $R(1,m)$ 的包含 $f(x_1x_2\cdots x_m)$ 的陪集中元素 $a_0+\sum_{i=1}^{m}a_ix_i+f(x)$ 的重量是由 a_0 和 $\hat{F}(x)$ 唯一确定。

4　一阶 R-M 码陪集重量分布的线性特性

为了讨论陪集的重量分布，引入 Hadmard 逆变换的概念。首先引入引理：

引理(4.1)　设 $a\in V^m$，则 $\sum(-1)^{a*x}=0$，其中

$$a=(a_1,a_2,\cdots,a_m),\quad x=(x_1,x_2,\cdots,x_m),\quad a*x=\sum_{i=1}^{m}a_ix_i$$

$$a_i\in GF(2),\quad x_i\in GF(2),\quad i=1,2,\cdots,m$$

证明　对于向量 $a=(a_1,a_2,\cdots,a_m)$，设 $D_a=\{i\mid a_i=1,\ 1\le i\le m\}$，令 $t=|D_a|$。则

$$\sum_{x\in V^m}(-1)^{a*x}=\sum_{x_a\in V^t}(-1)^{\omega(x_a)}=C_t^1-C_t^2+\cdots(-1)^tC_t^t=0$$

所以，$\sum_{x\in V^m}(-1)^{a*x}=0$。

定理 4.1　设 $F(x)$ 是取值为 1 和 -1 的函数，$x=(x_1,x_2,\cdots,x_m)$，$x_i\in GF(2)$ $(i=1,2,\cdots,m)$，$\hat{F}(x)$ 是 $F(x)$ 的 Hadmard 变换，则

$$F(x)=\frac{1}{2^m}\sum_{u\in V^m}(-1)^{u*x}\hat{F}(u) \tag{4.1}$$

证明　由 Hadmard 变换的定义可得，$\hat{F}(x)=\sum_{x\in V^m}(-1)^{u*x}F(x)$，将上式代入(4.1)式的右端

$$\sum_{u\in V^m}(-1)^{u*x}\hat{F}(u)=\sum_{u\in V^m}(-1)^{u*x}\left[\sum_{y\in V^m}(-1)^{y*u}F(y)\right]$$

$$d\left(g(x),\ b_0+\sum_{i=1}^{m}b_ix_i\right)=\frac{1}{2}[2^m-(-1)^{b_0}\hat{F}_g(b)]$$

其中 $\hat{F}_f(a)$, $\hat{F}_g(b)$ 分别是相应于 $F_f(x)=(-1)^{f(x)}$, $F_g(x)=(-1)^{g(x)}$ 的 Hadmard 变换。由(4.1)式可得:

$$F_f(x)=\frac{1}{2^m}\sum_{a\in V^m}(-1)^{a*x}\hat{F}_f(a)=\frac{1}{2^m}\sum_{b\in V^m}(-1)^{b*x}\hat{F}_g(b)$$

由 $g(x)=f(x+B)$

$$F_g(x)=F_f(x+B)=\frac{1}{2^m}\sum_{a\in V^m}(-1)^{a*x}(-1)^{a*B}\hat{F}_g(a)$$

因此, $\frac{1}{2^m}\sum_{b\in V^m}(-1)^{b*x}\hat{F}_g(b)=\frac{1}{2^m}\sum_{a\in V^m}(-1)^{a*x}(-1)^{a*B}\hat{F}_f(a)$。

上式对于任意的 x 都成立, 所以系数应相同, 即

$$\{\hat{F}_g(b)\ |b\in V^m\}=\{(-1)^{a*B}\hat{F}_f(a)\ |a\in V^m\}$$

$$\{(-1)^{b_0}\hat{F}_g(b)\ |b_0\in(0,1),\ b\in V^m\}=\{(-1)^{b_0+a*B}\hat{F}_f(a)\})\ |b_0\in(0,1),\ a\in V^m\}$$

由 b_0 的任意性

$$\{(-1)^{b_0}\hat{F}_g(b)\ |b_0\in(0,1),\ b\in V^m\}=\{(-1)^{a_0}\hat{F}_f(a)\})\ |a_0\in(0,1),\ a\in V^m\}$$

因此 $f(x)$ 和 $g(x)$ 的陪集有相同的重量分布。

$x+B$ 是线性变换的加常量变换, 所以 Bool 函数 $f(x)$ 的自变量同任一个 m 维向量相加不改变此 Bool 函数在一阶 R-M 码中相应陪集的重量分布。

综合定理(4.3)和(4.4)可得陪集重量分布的线性特性。

定理 4.5　任何 m 维 Bool 函数自变量同 $GF(2)$ 上的可逆的 m 阶矩阵和任何一个 m 维向量的线性组合不改变 Bool 函数在一阶 R-M 码中陪集的重量分布。

参 考 文 献

1　MacWilliams F J and Sloane N J. The Theory of Error-Correcting Codes. North-Holland, 1977

2　齐忠涛. 一类 Bool 函数的若干性质. 科学通报, 1987, 32(6)

3　杨义先, 林须端. 编码密码学. 北京: 人民邮电出版社, 1992

4　肖国镇, 卿斯汉. 编码理论. 北京: 国防工业出版社, 1993

(上接第 52 页)

参 考 文 献

1　曾五一. 关于动态投入产出优化模型应用的研究. 系统工程, 1985(2): 29～37

2　刘起运. 经济系统规划方法和模型. 北京: 中国统计出版社, 1993

3　陈锡康. 投入产出技术的发展趋势与国际动态. 系统工程理论与实践, 1991, 11(2)

4　赵新良等. 动态投入产出. 沈阳: 辽宁人民出版社, 1988

5　伊格尼齐奥著. 单目标和多目标系统线性规划. 闵仲求等译. 上海: 同济大学出版社, 1986

6　Adem Rose & William Miernyk. Input-output Analysis: The First Fifty Years. Economic Systems Research, 1989(1): 233～235

数不超过 r 的单项式的个数就是信息位的个数, 设为 k, 则

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r} \tag{1.2}$$

所有阶数不超过 r 的Bool函数的个数就是码字的个数, 设为 N, $N = 2^k$。

一阶R-M 码 $R(1,m)$ 就是一切阶数为 0 或 1 的 m 元Bool函数的真值表作为码字而得到的码。

Bool函数 $f(x_1, x_2, \cdots, x_m)$ 一切阶数 0 或 1 的单项式为 $1, x_1, x_2, \cdots, x_m$, 因此阶数不超过 1 的Bool函数是由 $1, x_1, x_2, \cdots, x_m$ 的线性组合。$R(1,m)$ 的生成矩阵为:

$$G = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & & & & \\ \vdots & & H & & \\ 1 & & & & \end{pmatrix} \tag{1.3}$$

其中 G 是 $(m+1)\times 2^m$ 矩阵, H 的第一列, 第二列, $\cdots$, 第 $2^m - 1$ 列分别是整数 $1, 2, \cdots, 2^{m-1}$ 的二进制表示的列向量。

定义 1.2 以(1.3)式右边矩阵为生成矩阵的线性分组码称为一阶R-M 码 $R(1,m)$。

2 陪集、陪集元和陪集重量分布

陪集的概念是线性分组码中的一个重要概念[3,4]。

定义 2.1 设 C 是一个 (n,k) 线性分组码, a 是任意一个 n 维二进向量, 则称向量集合

$$a + C = \{a \oplus c \mid c \in C\} \tag{2.1}$$

为码 C 的一个陪集, 其中$\oplus$是对应分量模 2 相加。

由线性码的线性特性可得, 若 $a \in C$ 则 $a + C = C$, 若 $a \notin C$, 则 $a + C \neq C$。

任何 $a \in V^m$ 有陪集 $a + C$, 考虑 a 与 $C(n,k)$ 中的码字 b 之间的Hamming 距离 $d(a,b)$, 即 $\omega(a \oplus b)$。

定义 2.2 设 a 为一个 n 维二进向量, C 是一个 (n,k) 线性分组码, $\epsilon_1, \epsilon_2, \cdots, \epsilon_k$ 分别是 C 的生成矩阵中第一行, 第二行, $\cdots$, 第 K 行, 任意 $x = (x_1, x_2, \cdots, x_m) \in V^m$, 称 $a \oplus \sum_{i=1}^{k} x_i \epsilon_i$ 为陪集 $a + C$ 的一个陪集元, 称Hamming 重量 $\omega\left(a \oplus \sum_{i=1}^{k} x_i \epsilon_i\right)$ 为 $a + C$ 中的元素 $a \oplus \sum_{i=1}^{k} x_i \epsilon_i$ 的重量, 称 $\left\{\omega\left(a \oplus \sum_{i=1}^{k} x_i \epsilon_i\right) \mid x \in V^m\right\}$ 为陪集 $a + C$ 的重量分布。明显若 $a \in C$, 那么陪集 $a + C$ 的重量分布就是线性分组码 C 的重量分布。

定义 2.3 设 $F(x)$ 是取值为 1 和 -1 的函数, $x = (x_1, x_2, \cdots, x_m) \in V^m$, $x_i \in GF(2)$, $i = 1, 2, \cdots, m$, 称 $\hat{F}(u) = \hat{F}(u_1, u_2, \cdots, u_m) = \sum_{x \in V^m} (-1)^{x*u} F(x)$ 为函数 $F(x)$ 的Hadmard 变换。

对于一阶R-M 码 $R(1,m)$ 中的任何一个码字都可以表示为 $a_0 + \sum_{i=1}^{m} a_i x_i$, $a_0 \in GF(2)$, $a_i \in GF(2)$, $i = 1, 2, \cdots, m$。对任何一 m 元Bool函数 $f(x) = f(x_1, x_2, \cdots, x_m)$, 称 $d\left(f(x), a_0 + \sum_{i=1}^{m} a_i x_i\right) = \omega\left(f(x) + a_0 + \sum_{i=1}^{m} a_i x_i\right)$ 为一阶R-M 码 $R(1,m)$ 的陪集元 $f(x) + a_0 + \sum_{i=1}^{m} a_i x_i$ 的Hamming 重量, 而 $\left\{\omega\left(f(x) + a_0 + \sum_{i=1}^{m} a_i x_i\right) \mid a_0 \in GF(2), a_i \in GF(2)\right\}$ 称为陪集的重量分布。

3 陪集元的重量表达式

令 $F(x) = (-1)^{f(x)}$, 则 $\hat{F}(x)$ 是取值为 1 和 -1 的函数 $F(x)$ 的Hadmard 变换

$$\hat{F}(u) = \hat{F}(u_1, u_2, \cdots, u_m) = \sum_{x \in V^m} (-1)^{x*u} F(x) = \sum_{x \in V^m} (-1)^{x*u + f(x)} \tag{3.1}$$

$$= \sum_{y\in V^m}\left\{\left[\sum_{u\in V^m}(-1)^{(x\odot y)*u}\right]F(y)\right\}$$

若 $y = x$, 则 $x \oplus y = 0$, $(x \oplus y) * u = 0$, $\sum_{u\in V^m}(-1)^{(x\odot y)*u} = 2^m$。

若 $y \neq x$, 则 $x \oplus y \neq 0$, 由上述引理, $\sum_{u\in V^m}(-1)^{(x\odot y)*u} = 0$

所以, $\sum_{u\in V^m}(-1)^{u*x}\hat{F}(u) = F(x)2^m$ 即 $F(x) = \frac{1}{2^m}\sum_{u\in V^m}(-1)^{u*x}\hat{F}(u)$。

由定理 3.1 可见, 一阶 R-M 码包含 $f(x) = f(x_1, x_2, \cdots, x_m)$ 的陪集重量分布是由 $(-1)^{f(x)}$ 的 Hadmard 逆变换的系数完全确定。

设 $f(x)$ 和 $g(x)$ 是两个 Bool 函数, 对于 $R(1, m)$ 码 $f(x)$ 和 $g(x)$ 有相应的陪集重量分布, $d\left(f(x), a_0 + \sum_{i=1}^{m}a_ix_i\right)$ 和 $d\left(g(x), b_0 + \sum_{i=1}^{m}b_ix_i\right)$, 下面给出两个 Bool 函数重量分布相同的条件。

定理 4.2 设 m 元 Bool 函数 $f(x)$ 和 $g(x)$ 满足关系 $g(x) = f(Ax)$, 其中 A 是 $GF(2)$ 中的一个 $m \times m$ 阶可逆矩阵, 那么 $R(1,m)$ 的包含 $f(x)$ 的陪集和包含 $g(x)$ 的陪集具有相同的重量分布。

证明 由 (3.2) 式可得:

$$d\left(f(x), a_0 + \sum_{i=1}^{m}a_ix_i\right) = \frac{1}{2}[2^m - (-1)^{a_0}\hat{F}_f(a)]$$

$$d\left(g(x), b_0 + \sum_{i=1}^{m}b_ix_i\right) = \frac{1}{2}[2^m - (-1)^{b_0}\hat{F}_g(b)]$$

其中 $\hat{F}_f(a)$, $\hat{F}_g(b)$ 分别是相应于 $F_f(x) = (-1)^{f(x)}$, $F_g(x) = (-1)^{g(x)}$ 的 Hadmard 变换。由 (4.1) 式可得:

$$F_f(x) = \frac{1}{2^m}\sum_{a\in V^m}(-1)^{a*x}\hat{F}_f(a)$$

$$F_g(x) = \frac{1}{2^m}\sum_{b\in V^m}(-1)^{b*x}\hat{F}_g(b)$$

$$g(x) = f(Ax),\ F_g(x) = F_f(Ax) = \frac{1}{2^m}\sum_{a\in V^m}(-1)^{a*x}\hat{F}_f(aA^{-1})$$

令: $b \triangleq aA$, $a = bA^{-1}$

由 A 的可逆性可知: b 取遍 V^m 中的元素时 a 相应也取遍 V^m 中的元素。

$$F_g(x) = \frac{1}{2^m}\sum_{b\in V^m}(-1)^{b'*x}\hat{F}_f(bA^{-1}) \text{ 而 } F_g(x) = \frac{1}{2^m}\sum_{b\in V^m}(-1)^{b*x}\hat{F}(b)$$

因此, $\sum_{b\in V^m}(-1)^{b'*x}\hat{F}_f(bA^{-1}) = \sum_{b\in V^m}(-1)^{b*x}\hat{F}(b)$

上式中等式两边是 x 的函数, 对任何的 x 都成立, 因此系数应该相等, 即:

$$\{\hat{F}_g(b) \mid b \in V^m\} = \{\hat{F}_f(bA^{-1}) \mid b' \in V^m\}$$

$$\{\hat{F}_g(b) \mid b \in V^m\} = \{\hat{F}_f(a)\} \mid a \in V^m\}$$

至此证明了两个 Bool 函数在满足 $g(x) = f(Ax)$ 条件下相应的陪集重量分布是相同的, 其中 A 是可逆矩阵。如果将 Bool 函数 $f(x)$ 的自变量 x 为 Ax 看成是线性变换的左边数乘运算, 那么上述结论可叙述为 Bool 函数自变量的左边数乘变换不改变其相应的陪集重量分布。

下面来看一阶 R-M 码的另一种线性变换。

定理 4.3 设 m 元 Bool 函数 $f(x)$ 和 $g(x)$ 满足关系 $g(x) = f(x + B)$ 其中 B 是 $GF(2)$ 上的 m 维向量, 那么 $R(1,m)$ 的包含 $f(x)$ 的陪集和包含 $g(x)$ 的陪集有相同的陪集分布。

证明 由 (3.2) 式可得:

$$d\left(f(x), a_0 + \sum_{i=1}^{m}a_ix_i\right) = \frac{1}{2}[2^m - (-1)^{a_0}\hat{F}_f(a)]$$