

广义 Hamming 重量和等重码¹

岳殿武 胡正名*

(南京邮电学院电信工程系 南京 210003)

*(北京邮电大学信息工程系 北京 100088)

摘 要 本文将线性码的广义 Hamming 重量的概念推广到非线性码上去, 并导出了一种广义 Elias 界。对于线性等重码, 本文给出了其完整的重量谱系。

关键词 广义 Hamming 重量, 线性码, 等重码, Elias 界, 循环 Hadamard 矩阵

中图分类号 TN911.2

1 引言

由于密码方面的应用, 1991 年 V. K. Wei 提出了线性码的广义 Hamming 重量这一新的概念^[1]。从此以后, 国外一些学者对广义 Hamming 重量进行了广泛而深刻的讨论, 得到了不少有意义的结果^[2-4]。目前, 广义 Hamming 重量越来越引起编码理论界的注意。

本文将线性码的广义 Hamming 重量的研究推广到非线性码上去, 并且侧重讨论了等重码的广义 Hamming 重量情况。

2 非线性码的广义 Hamming 重量的定义

令 C 是一个 $[n, k, d]$ 的 q 元线性码, D 是 C 的一个任意子码。令 $X(D)$ 表示 D 的支集, 即 $X(D) = \{i : \exists c = (c_1, c_2, \dots, c_n) \in D, c_i \neq 0\}$ 。那么定义 C 的第 r , $(1 \leq r \leq k)$ 广义 Hamming 重量为^[1] $d_r(C) = \min\{|X(D)| : D \text{ 是 } C \text{ 的任意一个 } r \text{ 维子码}\}$; 并且称集合 $\{d_r(C) : 1 \leq r \leq k\}$ 为码 C 的重量谱系。关于 $d_r(C)$, $1 \leq r \leq k$ 有如下一个基本性质: $0 < d_1(C) < d_2(C) < \dots < d_k(C) \leq n$, 即满足严格单调性。

显然, $d_1(C) = d$ 。广义 Hamming 重量这一概念是通常最小 Hamming 重量的自然推广, 已经发现在密码、trellis 编码当中广义 Hamming 重量有其应用价值^[2]。下面我们将这一概念推广到非线性码上去。

设 $y_i = (y_{i1}, y_{i2}, \dots, y_{in}) \in F_q^n$, $i = 1, 2, \dots, k$ 。令 $X(y_1, y_2, \dots, y_k)$ 表示集合 $\{y_i : 1 \leq i \leq k\}$ 的支集。再令 $W(y_1, y_2, \dots, y_k) = |X(y_1, y_2, \dots, y_k)|$ 。显然, $W(y_i)$ 就表示通常 y_i 的 Hamming 重量。记 $y_1 y_2 = (x_1, x_2, \dots, x_n)$, 其中 $x_i = y_{1i} y_{2i} \pmod q$, 则由集合论和组合论知识可知

$$X(y_1, y_2, \dots, y_k) = \bigcup_{i=1}^k X(y_i),$$
$$W(y_1, y_2, \dots, y_k) = \sum_{i=1}^k W(y_i) - \sum_{1 \leq i < j \leq k} W(y_i y_j) + \dots + (-1)^{k-1} W(y_1 y_2 \dots y_k).$$

¹ 1995-07-04 收到, 1996-07-11 定稿
国家教委跨世纪优秀人才专项基金资助课题

显然, 对于 q 元线性码 C , 若 D 为其 r 维子码, $y_1, y_2, \dots, y_r$ 为 D -基, 则 $|X(D)| = W(y_1, y_2, \dots, y_r)$.

定义 1 设 ζ 表示一个 (n, M, d) 的 q 元非线性码, ζ 的最大线性无关码字数为 k , 则定义 ζ 第 r ($1 \leq r \leq k$) 广义 Hamming 重量为 $d_r(\zeta) = \min\{W(y_1, y_2, \dots, y_r) | y_i \in \zeta \text{ 且线性无关}, i = 1, 2, \dots, r\}$, 并称集合 $\{d_r(\zeta) : 1 \leq r \leq k\}$ 为码 ζ 的重量谱系.

显然, 若 ζ 是线性码, 则该定义与 V. K. Wei 所给出的线性码广义 Hamming 重量定义是一致的. 容易发现, 对于非线性码 ζ , 其广义 Hamming 重量 $d_r(\zeta)$ 满足单调性, 即 $0 < d_1(\zeta) \leq d_2(\zeta) \leq \dots \leq d_k(\zeta) \leq n$, 但它不一定满足严格单调性. 例如, 让 C_w^n 表示码长为 n 、Hamming 重量均为 w 所有二元向量构成的非线性码. 对于 C_w^n , 当 $w \geq 3$ 时, 有 $d_1(C_w^n) = w$, $d_2(C_w^n) = w + 1$.

因为 $a = (\overbrace{1, 1, \dots, 1}^w, 0, \dots, 0)$, $b = (0, \overbrace{1, 1, \dots, 1}^w, 0, \dots, 0)$ 以及 $c = (\overbrace{1, 1, \dots, 1}^{w-1}, 0, 1, 0, \dots, 0)$ 是 C_w^n 中码字且线性无关, 所以 $d_3(C_w^n) = w + 1 = d_2(C_w^n)$, 不满足严格单调性.

3 广义 Elias 界

记 $A(n, d) = \max\{|\zeta| | \zeta \text{ 码长为 } n, \text{ 最小距离至少为 } d\}$, $A(n, d, w) = \max\{|\zeta| | \zeta \text{ 码长为 } n, \text{ 码字重均为 } w, \text{ 最小距离至少为 } d\}$. 研究 $A(n, d)$ 和 $A(n, d, w)$ 一直是编码理论研究中最基本工作之一^[5]. 关于 $A(n, d)$ 和 $A(n, d, w)$ 有一个 Elias 界^[6], 它是

$$A(n, d) \leq [q^n A(n, d, w)] / \left[(q-1)^w \binom{n}{w} \right].$$

记 $A(n, D) = \max\{|\zeta| | \zeta \text{ 码长为 } n, d(\zeta) \geq d, d_i(\zeta) \geq d_i, 2 \leq i \leq k\}$, $A(n, D, w) = \max\{|\zeta| | \zeta \text{ 码长为 } n; d_i(\zeta) \geq d_i, 2 \leq i \leq k; d(\zeta) \geq d; W(C) = w, \forall c \in \zeta\}$, 这里 $D = \{d, d_2, d_3, \dots, d_k\}$, 而 $d(\zeta)$ 表示码 ζ 的最小距离. $A(n, D)$ 与 $A(n, D, w)$ 表示满足给定距离结构和重量 (广义 Hamming 重量) 结构最大码的大小. 当 $D = \{d\}$ 时, $A(n, D)$ 和 $A(n, D, w)$ 就分别是 $A(n, d)$ 和 $A(n, d, w)$. 下面给出一种广义 Elias 界.

$$\text{定理 1} \quad A(n, D) \leq [q^n A(n, D, w)] / \left[(q-1)^w \binom{n}{w} \right].$$

证明 设 ζ 是满足 $|\zeta| = A(n, D)$ 的一个码, 令

$$\delta(x, y) = \begin{cases} 1, & x \in \zeta, d(x, y) = w; \\ 0, & \text{其他.} \end{cases}$$

这里 $x, y \in F_q^n$, $d(x, y)$ 表示 x, y 之间 Hamming 距离. 因为

$$\begin{aligned} \sum_{x, y \in F_q^n} \delta(x, y) &= \sum_{x \in \zeta} (q-1)^w \binom{n}{w} = (q-1)^w \binom{n}{w} A(n, D) \\ &= \sum_{y \in F_q^n} \sum_{x \in \zeta} \delta(x, y) \leq \sum_{y \in F_q^n} A(n, D, w) = q^n A(n, D, w). \end{aligned}$$

故有

$$A(n, D) \leq [q^n A(n, D, w)] / \left[(q-1)^w \binom{n}{w} \right]. \quad \text{证毕}$$

文献 [1] 留下几个未解决的问题. 其中之一是推广 Griesmer 界、Hamming 界、Elias 界等界问题. 定理 1 给出了一种广义 Elias 界.

4 等重码的第二广义 Hamming 重量

对于 $x = (x_1, x_2, \dots, x_n) \in F_q^n$, 记 $\bar{x} = (\bar{x}_1, \dots, \bar{x}_n)$, 其中 $\bar{x}_i$ 满足: $\bar{x}_i = 0$, 若 $x_i \neq 0$; $\bar{x}_i = 1$, 若 $x_i = 0$. 我们容易推出非线性码 ζ 第 2 个广义 Hamming 重量 $d_2(\zeta)$ 如下几种表示形式.

$$d_2(\zeta) = \min\{W(x) + W(y) - W(xy) | x, y \in \zeta, \text{且不相容}\},$$

$$d_2(\zeta) = \min\{d(x, y) + W(xy) | x, y \in \zeta, \text{且不相容}\},$$

$$d_2(\zeta) = n - \max\{W(\bar{x}\bar{y}) | x, y \in \zeta, \text{且不相容}\}.$$

定理 2 令 ζ 表示每个码字重量为 w 的等重码 (n, m, d) . 则 ζ 最小距离为偶数, 第 2 广义 Hamming 重量 $d_2(\zeta) = d/2 + w$.

证明 $\forall x, y \in \zeta$, 有 $d(x, y) = W(x) + W(y) - 2W(xy) = 2w - 2W(xy)$, 设 $x^*, y^* \in \zeta$, 使 $d(x^*, y^*) = d$. 则由上式可知 d 为偶数. 因为 $d \leq d(x, y)$, 故 $W(xy) \leq w - d/2$. 这样我们有

$$\begin{aligned} W(x, y) &= W(x) + W(y) - W(xy) = 2w - W(xy) \\ &\geq 2w - (w - d/2) = w + d/2, \end{aligned}$$

又因为 $W(x^*, y^*) = w + d/2$, 故有 $d_2(\zeta) = d/2 + w$.

证毕

5 线性等重码的重量谱系

在数字通信的 ARQ 差错控制设备中各种等重码被广泛地用作检错码. 这是因为等重码的编译码设备和检错码设备很简单. 此外等重码还有优良检错性能, 既适用于 BSC 信道, 又适用非对称信道. 正是由于等重码在理论和实践中都具有十分重要价值, 所以近几年来它受到了国内外学者的重视 [7,8].

在给出线性等重码重量谱系之前, 我们先介绍几个概念.

定义 2 ζ 是一个码, 将 ζ 所有码字按行排列, 并使之形成一个矩阵 A , 我们称 A 为码 ζ 的码矩阵.

定义 3 设 C 是一个二进制的 $[n, k, d]$ 线性码. 如果 C 中含有全零码字而且一切非零码字的重量均为 d , 那么就称 C 为一个线性等重码.

定义 4 (1) 设 A 和 B 是两个 $2^k \times n$ 阶码矩阵, 如果存在 $2^k \times 2^k$ 阶置换矩阵 P 和 $n \times n$ 阶置换矩阵 Q 使得 $A = PBQ$, 那么就称 A 与 B 等价. (2) A 如上, D 是 $2^k \times (rn)$ 阶码矩阵,

如果 D 与 $A \otimes \overbrace{(1, 1, \dots, 1)}^r$ 等价, 那么就称 A 与 D 是克罗内克等价的. 此处 $\otimes$ 表示矩阵的克罗内克乘积. (3) A 如上, E 是 $2^k \times (rn + s)$ 阶码矩阵, 如果存在与 A 克罗内克等价的 $2^k \times (rn)$ 阶码矩阵 F 使得 $E = (F; 0)$, 那么就称 E 与 A 弱等价. 此处 0 是一个 $2^k \times s$ 阶的零阵.

定义 5 设 H 是 $2^k \times 2^k$ 阶 0, 1 Walsh-Hadamard 矩阵 (即将普通的 ± 1 值 W-H 矩阵中的 1 变为 0, -1 变为 1). 如果把去掉全零列后的 $2^k \times (2^k - 1)$ 阶矩阵看成一个码矩阵, 那么就得到一个线性的 $[2^k - 1, k, 2^{k-1}]$ 等重码. 称此码为 Walsh-Hadamard 码.

定理 3 [8] (1) 线性 $[n, k, d]$ 等重码 C 满足: $2^{k-1} | d$, d 为其最小距离, k 为其维数. (2) 线性 $[n, k, d]$ 等重码 C 弱等价于一个 $[2^k - 1, k, 2^{k-1}]$ Walsh-Hadamard 码.

定义 6 [2] 一个线性 $[n, k, d]$ 码 C 被称为是满足链条件, 如果存在 C 的 k 个子码 $D_r, 1 \leq r \leq k$ 满足 $d_r(C) = |X(D_r)|, D_{r-1} \subset D_r, 2 \leq r \leq k$. 并且 D_r 的维数为 r .

对于一个 $[n, k, d]$ 的线性码 C , 有^[1] $n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$, 我们称之为 Griesmer 界. 研究一个线性码是否满足链条件、达到 Griesmer 界, 对于我们了解该码的性能、结构以及研究乘积码的广义 Hamming 重量很有益处.

定理 4 对于任意线性 $[n, k, 2^{k-1}r]$ 等重码 C , 有 (1) 其第 i 广义 Hamming 重量为 $d_i(C) = r(2^{k-1} + 2^{k-2} + \dots + 2^{k-i})$, $1 \leq i \leq k$. (2) C 满足链条件. (3) 若 $n = (2^k - 1)r$, C 达到了 Griesmer 界.

证明 (1) 设 C_1 表示 Walsh-Hadamard $[2^k - 1, k, 2^{k-1}]$ 码. 记 $C_2 = C_1 \cup \{c + (1, 1, \dots, 1) | \forall c \in C_1\}$, 则 C_2 就是一阶 RM 码 $R(1, k)$ 的删余码 $R^*(1, k)$. 这样我们易知 C_1 实质上就是 Hamming $[2^k - 1, 2^k - 1 - k, 3]$ 码的对偶码^[5]. 因为 C 弱等价于一个 $[2^k - 1, k, 2^{k-1}]$ Walsh-Hadamard 码——码 C_1 , 则 $d_i(C) = r \cdot d_i(C_1)$, $1 \leq i \leq k$. 再由文献[1]推论 3 知, $d_i(C_1) = 2^{k-1} + 2^{k-2} + \dots + 2^{k-i}$. 故 $d_i(C) = r(2^{k-1} + 2^{k-2} + \dots + 2^{k-i})$, $1 \leq i \leq k$.

(2) 因为 Hamming 码的对偶码满足链条件^[2], 所以存在 C_1 的 k 个子码 D_i , $1 \leq i \leq k$, 满足 $\dim(D_i) = i$, $|X(D_i)| = d_i(C_1)$, $D_{i-1} \subset D_i$. 定义 $D_i^* = \{c \otimes \overbrace{(1, 1, \dots, 1)}^r | \forall c \in D_i\}$, 其中 $\otimes$ 表示矩阵克罗内克乘积. 不难发现: $\dim(D_i^*) = i$, $|X(D_i^*)| = d_i(C)$, $D_{i-1}^* \subset D_i^*$. 再由定理 3 和弱等价定义知 C 必满足链条件.

(3) 若 $n = (2^k - 1)r$, 则 $n = \sum_{i=0}^{k-1} \lceil d/2^i \rceil = \sum_{i=0}^{k-1} r \cdot 2^{k-1-i} = (2^k - 1)r$. 故 C 达到了 Griesmer 界. 证毕

参 考 文 献

- [1] Wei V K. Generalized Hamming weights for linear codes. IEEE Trans. on IT, 1991, IT-37(5): 1412-1418.
- [2] Wei V K, et al. On the generalized Hamming weights of product codes. IEEE Trans. on IT, 1993, IT-39(5): 1709-1713.
- [3] Helleseth H, et al. Bounds on the minimum support weights. IEEE Trans. on IT, 1995, IT-41(2): 432-439.
- [4] Yang K, et al. On the weight hierarchy of geometric Goppa codes. IEEE Trans. on IT, 1994, IT-40(3): 913-920.
- [5] MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes. Amsterdam, North-Holland publish company, 1977, Chapter 1, Chapter 17..
- [6] Elias P. Error-free coding, IEEE Trans. on IT, 1954, IT-4(1): 29-37.
- [7] 王新梅. 最佳 $(n, 2, w)$ 二进制等重检错码的存在性及其猜想. 中国科学, 1987, 17(11): 1225-1232.

- [8] 杨义先, 胡正名. 线性等重码的结构分析. 电子学报, 1990, 18(6): 1-8.

GENERALIZED HAMMING WEIGHTS AND CONSTANT WEIGHT CODES

Yue Dianwu Hu Zhengming*

(*Nanjing University of Posts and Telecommunications, Nanjing 210003*)

*(*Beijing University of Posts and Telecommunications, Beijing 100088*)

Abstract This paper generalizes the definition of generalized Hamming weights for linear codes to nonlinear codes, derives a generalized Elias bound, and gives the weight hierarchy of linear constant weight codes.

Key words Generalized Hamming weights, Linear codes, Constant weight codes, Elias bound, Circulant Hadamard matrix

岳殿武: 男, 1965 年生, 博士, 从事差错控制码与信息安全研究工作.

胡正名: 男, 1931 年生, 教授, 博士生导师, 从事应用数学和信息科学的教学和科研工作.