Z_k 线性码的对称形式的 MacWilliams 恒等式¹

朱士信

(合肥工业大学应用数学系 合肥 230009)
(中国科学院研究生院信息安全国家重点实验室 北京 100039)

摘 要 该文定义了 Z_k 线性码的码字的对称重量计数公式, 利用离散的 Hadamard 变换, 建立了线性码与其对偶码之间的对称形式的 MacWilliams 恒等式.

关键词 线性码, 对称重量计数公式, Hadamard 变换, MacWilliams 恒等式

中图分类号 TN911.22

1 引 言

近年来, 很多从事编码理论的研究者将研究的兴趣从有限域上的编码理论转移到模整数 k 的剩余类环 Z_k 上的编码理论^[1-3], 尤其是 Z_4 码的研究^[4-6]. 无论是域还是环上的编码理论, 利用线性码的码字的各种重量分布研究其对偶码的相应重量分布都是一个有意义的研究课题. MacWilliams 在文献 [7] 中给出了有限域 F_q 上线性码的 Hamming 重量的 MacWilliams 恒等式; Klemm 在文献 [8] 中把此恒等式推广到模 k 的剩余类环上; Conway 和 Sloane 在文献 [9] 中定义并给出了对称形式的 MacWilliams 恒等式, 本文定义 Z_k 线性码的码字的对称重量计数公式, 并建立了对称形式的 MacWilliams 恒等式.

2 基本概念及主要结论

记 $Z_k = \{0, 1, \dots, k-1\}$, $k(\geq 2)$ 为自然数, $Z_k^n = \{(x_1, \dots, x_n) | x_i \in Z_k, i = 1, \dots, n\}$, 对 $\forall X = (x_1, \dots, x_n) \in Z_k^n, Y = (y_1, \dots, y_n) \in Z_k^n$, 定义 X 和 Y 的和为

$$X + Y = (x_1 + y_1, \dots, x_n + y_n) \tag{1}$$

则 $(Z_k^n, +)$ 为交换群, 称 Z_k^n 的任一子群为长为 n 的 k 元线性码, 或称 Z_k 线性码. 对 $\forall X = (x_1, \dots, x_n), Y = (y_1, \dots, y_n) \in Z_k^n$, 定义 X 和 Y 内积为

$$X \cdot Y = x_1 y_1 + \dots + x_n y_n \tag{2}$$

如果 $X \cdot Y = 0$, 则称 X 与 Y 正交.

设 C 是 Z_k 线性码, 令

$$C^\perp = \{X \in Z_k^n | X \cdot Y = 0, \text{ 对 } \forall Y \in C\} \tag{3}$$

则容易证明 $C^\perp$ 也是一个长为 n 的 k 元线性码, 并称 $C^\perp$ 为 C 的对偶码.

对 $\forall X = (x_1, \dots, x_n) \in Z_k^n$, 定义 X 的 $a(a \in Z_k)$ 重量为 X 中分量等于 a 的分量个数, 即

$$w_a(X) = |\{i | x_i = a, 1 \leq i \leq n\}| \tag{4}$$

并称

$$w_C(Y_0, Y_1, \dots, Y_{k-1}) = \sum_{X \in C} Y_0^{w_0(X)} Y_1^{w_1(X)} \dots Y_{k-1}^{w_{k-1}(X)} \tag{5}$$

为码 C 的完全重量计数公式.

¹ 2002-03-15 收到, 2002-09-23 改回

设 $f(X)$ 是定义在 Z_k^n 上的复值函数, 对 $\forall X \in Z_k^n$, 称

$$\overline{f(X)} = \sum_{Z \in Z_k^n} (e^{i2\pi/k})^{Z \cdot X} f(Z) \quad (6)$$

为 $f(X)$ 的离散的 Hadamard 变换, 其中 $i = \sqrt{-1}$.

引理 1

$$(1) \sum_{j=0}^{k-1} (e^{i2\pi/k})^j = 0 \quad (7)$$

$$(2) \text{ 设 } k = ml, \text{ 则 } \sum_{j=0}^{l-1} (e^{i2\pi/k})^{jm} = 0 \quad (8)$$

证明

$$(1) \sum_{j=0}^{k-1} (e^{i2\pi/k})^j = \frac{1-(e^{i2\pi/k})^k}{1-e^{i2\pi/k}} = \frac{1-e^{i2\pi}}{1-e^{i2\pi/k}} = 0;$$

$$(2) \sum_{j=0}^{l-1} (e^{i2\pi/k})^{jm} = \sum_{j=0}^{l-1} (e^{i2\pi/l})^j \stackrel{(1)}{=} 0.$$

证毕

引理 2 设 C 是 Z_k 线性码, $C^\perp$ 是 C 的对偶码, 则

$$\sum_{X \in C^\perp} f(X) = \frac{1}{|C|} \sum_{X \in C} \overline{f(X)} \quad (9)$$

证明 $\sum_{X \in C} \overline{f(X)} = \sum_{X \in C} \sum_{Z \in Z_k^n} (e^{i2\pi/k})^{X \cdot Z} f(Z) = \sum_{Z \in Z_k^n} f(Z) \sum_{X \in C} (e^{i2\pi/k})^{X \cdot Z}$

(1) 当 $Z \in C^\perp$ 时, 对 $\forall X \in C$ 有 $X \cdot Z = 0$, 则 $(e^{i2\pi/k})^{X \cdot Z} = 1$, 从而 $\sum_{X \in C} (e^{i2\pi/k})^{X \cdot Z} = |C|$;

(2) 当 $Z \notin C^\perp$ 时, 则 $\exists X \in C$, 使 $X \cdot Z = s \neq 0$.

下面分两种情况讨论:

(a) 如果存在 $X \in C$ 使 $X \cdot Z = s \neq 0$, 且 $(s, k) = d = 1$, 不妨设存在 $X \in C$ 使 $X \cdot Z = 1$, 由于 C 是线性码, 则 $jX \in C$ 使 $jX \cdot Z = j, j = 0, 1, \dots, k-1$. 又存在 $Y \in C$ 使 $Y \cdot Z = 0$, 当且仅当 $(Y + jX) \cdot Z = j, j = 0, 1, \dots, k-1$, 这说明只要 $X \cdot Z$ 取值与 k 互素, 则 $X \cdot Z$ 分别取 $0, 1, \dots, k-1$ 的次数相等;

(b) 否则 $d \neq 1$, 则存在素数 p 使 $p^r | d$ 但 $p^{r+1} \nmid d$.

令 $m = \min\{s | X \cdot Z = s, d = (s, k), p^r | d, p^{r+1} \nmid d\}$, 下面先证 $m | k$.

设 $k = ml + t$, 由于 $p^r | d$, 则 $p^r | m, p^r | k$, 则 $p^r | t$. 由于存在 $X \in C$ 使 $X \cdot Z = m$, 则 $(l+1)X \in C$ 使 $(l+1)X \cdot Z = (l+1)m = (lm+t) + (m-t) \equiv m-t \pmod{k}$. 由于 $p^r | (m-t)$, 由 m 的最小性得: $t = 0$, 从而 $k = lm$.

由于 $X \cdot Z = m$, 则 $jX \cdot Z = jm, j = 0, 1, \dots, l-1$. 又存在 $Y \in C$ 使 $Y \cdot Z = 0$, 当且仅当 $(Y + jX) \cdot Z = j, j = 0, 1, \dots, l-1$, 这说明只要 $X \cdot Z$ 取值 m , 则 $X \cdot Z$ 分别取值 $0, m, 2m, \dots, (l-1)m$ 的次数相等.

综合 (a) 与 (b) 知, 当 X 跑遍 C 时, $X \cdot Z$ 或者分别取值 $0, 1, \dots, k-1$ 的次数相等, 或者分别取值 $0, m, 2m, \dots, (l-1)m$ 的次数相等, 显然 m 随着 p 的变化而变化. 由引理 1 即可知, 当 $Z \notin C^\perp$ 时, $\sum_{X \in C} (e^{i2\pi/k})^{X \cdot Z} = 0$.

综合 (1), (2) 知:

$$\sum_{X \in C} \overline{f(X)} = \sum_{Z \in Z_k^n} f(Z) \sum_{X \in C} (e^{i2\pi/k})^{X \cdot Z} = \sum_{Z \in C^\perp} f(Z) \cdot |C| + \sum_{Z \notin C^\perp} f(Z) \cdot 0 = |C| \cdot \sum_{X \in C} f(X)$$

证毕

定理 1 设 C 是 Z_k 的线性码, $C^\perp$ 是 C 的对偶码, 则

$$w_{C^\perp}(Y_0, Y_1, \dots, Y_{k-1}) = \frac{1}{|C|} w_C(Z_0, Z_1, \dots, Z_{k-1}) \quad (10)$$

其中 $Z_t = \sum_{j=0}^{k-1} (e^{i2\pi/k})^{jt} Y_j$, $t = 0, 1, \dots, k-1$.

证明 对 $\forall X = (x_1, \dots, x_n) \in Z_k^n$, 令

$$f(X) = Y_0^{w_0(X)} Y_1^{w_1(X)} \dots Y_{k-1}^{w_{k-1}(X)} \quad (11)$$

对 $\forall s, t \in Z_k$, 令 $\delta_{s,t} = \begin{cases} 1, & t = s \\ 0, & t \neq s \end{cases}$, 则对 $\forall Y = (y_1, y_2, \dots, y_n) \in Z_k^n$, 有 $w_s(Y) = \delta_{s,y_1} + \delta_{s,y_2} + \dots + \delta_{s,y_n}$, 则

$$\begin{aligned} \overline{f(X)} &= \sum_{Z \in Z_k^n} (e^{i2\pi/k})^{X \cdot Z} f(Z) = \sum_{Z \in Z_k^n} (e^{i2\pi/k})^{x_1 y_1 + \dots + x_n y_n} Y_0^{w_0(Z)} Y_1^{w_1(Z)} \dots Y_{k-1}^{w_{k-1}(Z)} \\ &= \sum_{z_1 \in Z_k} (e^{i2\pi/k})^{x_1 z_1} Y_0^{\delta_{0,z_1}} Y_1^{\delta_{1,z_1}} \dots Y_{k-1}^{\delta_{k-1,z_1}} \\ &\quad \times \sum_{z_2 \in Z_k} (e^{i2\pi/k})^{x_2 z_2} Y_0^{\delta_{0,z_2}} Y_1^{\delta_{1,z_2}} \dots Y_{k-1}^{\delta_{k-1,z_2}} \dots \\ &\quad \times \sum_{z_n \in Z_k} (e^{i2\pi/k})^{x_n z_n} Y_0^{\delta_{0,z_n}} Y_1^{\delta_{1,z_n}} \dots Y_{k-1}^{\delta_{k-1,z_n}} \\ &= \sum_{j=0}^{k-1} (e^{i2\pi/k})^{j x_1} Y_j \cdot \sum_{j=0}^{k-1} (e^{i2\pi/k})^{j x_2} Y_j \dots \sum_{j=0}^{k-1} (e^{i2\pi/k})^{j x_n} Y_j \\ &= \prod_{s=0}^{k-1} \left[\sum_{j=0}^{k-1} (e^{i2\pi/k})^{s j} Y_j \right]^{w_s(X)} \end{aligned}$$

由完全重量计数公式的定义及引理 1 可得

$$\begin{aligned} w_{C^\perp}(Y_0, Y_1, \dots, Y_{k-1}) &= \sum_{X \in C^\perp} Y_0^{w_0(X)} Y_1^{w_1(X)} \dots Y_{k-1}^{w_{k-1}(X)} = \sum_{X \in C^\perp} f(X) \\ &= \frac{1}{|C|} \sum_{X \in C} \overline{f(X)} = \frac{1}{|C|} \sum_{X \in C} \left[\left(\sum_{j=0}^{k-1} (e^{i2\pi/k})^{0 \cdot j} Y_j \right)^{w_0(X)} \right. \\ &\quad \times \left. \left(\sum_{j=0}^{k-1} (e^{i2\pi/k})^{1 \cdot j} Y_j \right)^{w_1(X)} \dots \left(\sum_{j=0}^{k-1} (e^{i2\pi/k})^{(k-1) \cdot j} Y_j \right)^{w_{k-1}(X)} \right] \\ &= \frac{1}{|C|} \sum_{X \in C} Z_0^{w_0(X)} Z_1^{w_1(X)} \dots Z_{k-1}^{w_{k-1}(X)} = \frac{1}{|C|} w_C(Z_0, Z_1, \dots, Z_{k-1}) \end{aligned}$$

其中 $Z_t = \sum_{j=0}^{k-1} (e^{i2\pi/k})^{t \cdot j} Y_j$, $t = 0, 1, \dots, k-1$.

证毕

设 C 是码长为 n 的 Z_k 线性码, 对 $\forall X = (x_1, \dots, x_n) \in C$, 定义 X 的 Hamming 重量为

$$w_H(X) = w_1(X) + w_2(X) + \dots + w_{k-1}(X) = |\{i | x_i \neq 0, i = 1, \dots, n\}| \quad (12)$$

定义 C 的 Hamming 重量计数公式为

$$\text{Ham}_C(X, Y) = \sum_{X \in C} X^{n-w_H(X)} Y^{w_H(X)} \quad (13)$$

推论 设 C 是长为 n 的 Z_k 线性码, $C^\perp$ 是 C 的对偶码, 则

$$\text{Ham}_{C^\perp}(X, Y) = \frac{1}{|C|} \text{Ham}_C(X + (k-1)Y, X - Y) \quad (14)$$

证明 在 $w_C(Y_0, Y_1, \dots, Y_{k-1})$ 中, 令 $X = Y_0, Y = Y_1 = Y_2 = \dots = Y_{k-1}$, 得到 $\text{Ham}_C(X, Y)$, 则

$$\text{Ham}_{C^\perp}(X, Y) = w_{C^\perp}(X, Y, \dots, Y) = \frac{1}{|C|} w_C(Z_0, Z_1, \dots, Z_{k-1})$$

其中

$$\begin{aligned} Z_0 &= Y_0 + Y_1 + \dots + Y_{k-1} = X + (k-1)Y \\ Z_t &= \sum_{j=0}^{k-1} (e^{i2\pi/k})^{jt} Y_j = X + Y \sum_{j=1}^{k-1} (e^{i2\pi t/k})^j = X + Y \left(\sum_{j=0}^{k-1} (e^{i2\pi t/k})^j - 1 \right) \\ &= X + Y \left(\frac{1 - (e^{i2\pi t/k})^k}{1 - e^{i2\pi t/k}} - 1 \right) = X + Y(0 - 1) \\ &= X - Y, \quad t = 1, \dots, k-1 \end{aligned}$$

即

$$\begin{aligned} \text{Ham}_{C^\perp}(X, Y) &= \frac{1}{|C|} w_C(X + (k-1)Y, X - Y, \dots, X - Y) \\ &= \frac{1}{|C|} \text{Ham}_C(X + (k-1)Y, X - Y) \quad \text{证毕} \end{aligned}$$

由于定理 1 的结论中含有复数 i , 为了便于应用, 定义 Z_k 线性码 C 的对称重量计数公式 swe 如下:

当 $k = 2m$ 时

$$\text{swe}_C(Y_0, Y_1, \dots, Y_m) = \sum_{X \in C} Y_0^{w_0(X)} Y_1^{w_1(X) + w_{k-1}(X)} \dots Y_{m-1}^{w_{m-1}(X) + w_{k-(m-1)}(X)} Y_m^{w_m(X)} \quad (15)$$

当 $k = 2m + 1$ 时

$$\text{swe}_C(Y_0, Y_1, \dots, Y_m) = \sum_{X \in C} Y_0^{w_0(X)} Y_1^{w_1(X) + w_{k-1}(X)} \dots Y_m^{w_m(X) + w_{k-m}(X)} \quad (16)$$

$$\text{显然 } \text{swe}_C(Y_0, Y_1, \dots, Y_m) = \begin{cases} w_C(Y_0, Y_1, \dots, Y_{m-1}, Y_m, Y_{m-1}, \dots, Y_1), & k = 2m \\ w_C(Y_0, Y_1, \dots, Y_m, Y_m, \dots, Y_1), & k = 2m + 1 \end{cases} .$$

定理 2 设 C 是长为 n 的 Z_k 线性码, $C^\perp$ 是 C 的对偶码, 则

$$\text{swe}_{C^\perp}(Y_0, Y_1, \dots, Y_m) = \frac{1}{|C|} \text{swe}_C(Z_0, Z_1, \dots, Z_m) \quad (17)$$

$$\text{其中 } Z_0 = \begin{cases} Y_0 + 2 \sum_{j=1}^{m-1} Y_j + Y_m, & k = 2m \\ Y_0 + 2 \sum_{j=1}^m Y_j, & k = 2m + 1 \end{cases}$$

$$Z_t = \begin{cases} Y_0 + 2 \sum_{j=1}^{m-1} \cos \frac{jt \cdot 2\pi}{k} \cdot Y_j + \cos(\pi t) \cdot Y_m, & k = 2m, \\ Y_0 + 2 \sum_{j=1}^m \cos \frac{jt \cdot 2\pi}{k} Y_j, & k = 2m + 1, \end{cases} \quad t = 1, 2, \dots, m.$$

证明 设 $k = 2m$, 由对称重量计数公式的定义及定理得

$$\text{swe}_{C^\perp}(Y_0, Y_1, \dots, Y_m) = w_{C^\perp}(Y_0, Y_1, \dots, Y_{m-1}, Y_m, Y_{m-1}, \dots, Y_1) = \frac{1}{|C|} w_C(Z_0, Z_1, \dots, Z_{k-1})$$

其中 $Z_t = \sum_{j=0}^{k-1} (e^{i2\pi/k})^{jt} Y_j$, 由于 $Y_{m+1} = Y_m, \dots, Y_{k-1} = Y_1$, 因此容易证明 $Z_{k-t} = Z_t$, $t = 1, 2, \dots, m$. 从而, $\text{swe}_{C^\perp}(Y_0, Y_1, \dots, Y_m) = \frac{1}{|C|} w_C(Z_0, Z_1, \dots, Z_{k-1})$
 $= \frac{1}{|C|} w_C(Z_0, Z_1, \dots, Z_{m-1}, Z_m, Z_{m-1}, \dots, Z_1) = \frac{1}{|C|} \text{swe}_C(Z_0, Z_1, \dots, Z_m)$.

当 $k = 2m + 1$ 时, 证明完全类似. 证毕

最后, 我们通过一个具体例子, 说明定理 2 的应用.

例 容易验证 $C = \{(6, 3), (3, 6), (0, 0)\}$ 是长为 2 的 Z_9 线性码,

$$w_C(Y_0, Y_1, \dots, Y_8) = Y_0^2 + 2Y_3Y_6$$

则

$$\text{swe}_C(Y_0, Y_1, \dots, Y_8) = Y_0^2 + 2Y_3^2$$

由定理 2 知

$$\begin{aligned} \text{swe}_{C^\perp}(Y_0, Y_1, \dots, Y_8) &= \frac{1}{|C|} \text{swe}_{C^\perp}(Z_0, Z_1, \dots, Z_8) = \frac{1}{3} (Z_0^2 + 2Z_3^2) \\ &= \frac{1}{3} [(Y_0 + 2Y_1 + 2Y_2 + 2Y_3 + 2Y_4)^2 + 2(Y_0 - Y_1 - Y_2 + 2Y_3 - Y_4)^2] \\ &= Y_0^2 + 2Y_1^2 + 2Y_2^2 + 4Y_3^2 + 2Y_4^2 + 4Y_0Y_3 + 4Y_1Y_2 + 4Y_1Y_4 + 4Y_2Y_4 \end{aligned}$$

上述计算说明, 我们可以不必求出 $C^\perp$, 便可清楚 $C^\perp$ 的重量分布; 另一方面, 我们可以先求出 $C^\perp$, 再按定义求 $C^\perp$ 的对称重量分布如下:

$C^\perp$ 是由 $G = \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}$ 生成的, 即

$$G = \{(0, 0), (1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (7, 7), (8, 8), (0, 3), (1, 4), (2, 5), (3, 6), (4, 7), (5, 8), (6, 0), (7, 1), (8, 2), (0, 6), (1, 7), (2, 8), (3, 0), (4, 1), (5, 2), (6, 3), (7, 4), (8, 5)\}$$

再由对称重量计数公式的定义可得:

$$\text{swe}_{C^\perp}(Y_0, Y_1, \dots, Y_8) = Y_0^2 + 2Y_1^2 + 2Y_2^2 + 4Y_3^2 + 2Y_4^2 + 4Y_0Y_3 + 4Y_1Y_2 + 4Y_1Y_4 + 4Y_2Y_4$$

结果完全一致.

参 考 文 献

- [1] M. Harada, On the Hamming weight enumerators of self-dual codes over $Z_k[J]$, Finite Fields and Their Applications, 1999, 5(1), 26–34.
- [2] C. Carlet, Z_{2^k} -Linear codes [J], IEEE Trans. on Info. Theory, 1998, IT-44(4), 1543–1547.
- [3] S. Ling, P. Solé, Duadic over $Z_{2^k}[J]$, IEEE Trans. on Info. Theory, 2001, IT-47(4), 1581–1589.
- [4] E. Rains, Bounds for self-dual codes over $Z_4[J]$, Finite Fields and Their Applications, 2000, 6(2), 146–163.
- [5] P. Langevin, Duadic Z_4 -codes[J], Finite Field and Their Applications, 2000, 6(3), 309–326.
- [6] J. Wolfmsnn, Binary images of cyclic codes over $Z_4[J]$, IEEE Trans. on Info. Theory, 2001, IT-47(5), 1773–1777.
- [7] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code[J], Bell syst. Tech. J., 1963, 42(1), 79–84.
- [8] M. Klemm, Veber die Identität von MacWilliams für die Gewichtsfunktion von codes[J], Arch. Math., 1987, 49(2), 400–406.
- [9] J. H. Conway, N. J. A. sloane, Self-dual codes over the integers modul 4[J], J. Comb. Th., series A, 1993, 62(1), 30–45.

A SYMMETRIZED MacWilliams IDENTITY OF
 Z_k -LINEAR CODE

Zhu Shixin

*(Dept. of Applied Mathematics, Hefei University of Technology, Hefei 230009, China)**(State Key Lab of Info. Security, Graduate School of Academia Sinica, Beijing 100039, China)*

Abstract A symmetrized weight enumerator of Z_k -linear code is defined in this paper. By using discrete Hadamard transform, a symmetrized MacWilliams identity between Z_k -linear code and its dual code is given.

Key words Linear code, Symmetrized weight enumerator, Hadamard transform, MacWilliams identity

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