

線型符号に対する新たな Mac Williams 型恒等式

熊本大・理 城本啓介 (keisuke Shimoto)

線型符号で用いられる簡単な記号をまず定義する。

$$F := \mathbb{F}_q \quad (q\text{-elements field})$$

$$V := F^n := \{(u_1, \dots, u_n) \mid u_i \in F\}$$

$$N := \{1, 2, \dots, n\}$$

$$\forall u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in V \text{ に対して}$$

$$\langle u, v \rangle := \sum_{i=1}^n u_i v_i$$

$$d(u, v) := \#\{i \in N \mid u_i \neq v_i\}$$

$$\text{supp}(u) := \{i \in N \mid u_i \neq 0\}$$

$$|u| = W_t(u) := |\text{supp}(u)|$$

Definition

$$(1) C : (\text{linear}) \text{ code} \iff C \leq V \text{ (subspace)}$$

特に、 $\dim C = k$ のとき、 $C : [n, k]$ -code といい。

($n = \dim V = \text{length of } C$)

$$(2) C^\perp : \text{dual code of } C$$

$$\iff C^\perp := \{v \in V \mid \langle u, v \rangle = 0, \forall u \in C\}$$

次に、code とその dual code の関係を恒等式により、考察すると、次の有名な2つの定理がある。

Definition

$W_C(x, y)$: Weight enumerator of C

$$\iff W_C(x, y) := \sum_{u \in C} x^{n-|u|} y^{|u|} = \sum_{r=0}^n A_r x^{n-r} y^r$$

(ここで、 x, y : 変数, $A_r := \#\{u \in C \mid |u| = r\}$)

Theorem 1 (MacWilliams (1963))

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x-y)$$

Definition

$W_{C,D}(a, b, c, d)$: Joint weight enumerator of C and D

$$\iff W_{C,D}(a, b, c, d) := \sum_{u \in C} \sum_{v \in D} a^{i(u,v)} b^{j(u,v)} c^{k(u,v)} d^{l(u,v)}$$

(ここで、 a, b, c, d : 変数,

$$i(u, v) := \#\{i \in N \mid u_i = 0, v_i = 0\},$$

$$j(u, v) := \#\{i \in N \mid u_i = 0, v_i \neq 0\},$$

$$k(u, v) := \#\{i \in N \mid u_i \neq 0, v_i = 0\},$$

$$l(u, v) := \#\{i \in N \mid u_i \neq 0, v_i \neq 0\}.)$$

Theorem 2 (MacWilliams, Mallows, Sloane (1972))

$$W_{c^+, b^+}(a, b, c, d) = \frac{1}{|C| \cdot |D|} W_{c, d}(a + t(b+c) + t^2 d, a - b + t(c-d),$$

$$a - c + t(b-d), a - b - c + d)$$

(ここで, $t = q - 1$)

以上, 2つの定理では1つまたは2つのベクトルのWeightについて考えてあるが, これを λ 個のベクトルに拡張することにより, 次の定理が得られる.

Definition $\forall \lambda \in \mathbb{N}$ に対し,

$$W_c^{(\lambda)}(x, y) := \sum_{u^{(1)}, \dots, u^{(\lambda)} \in C} x^{n - \text{sc}(u^{(1)}, \dots, u^{(\lambda)})} y^{\text{sc}(u^{(1)}, \dots, u^{(\lambda)})}$$

(ここで, $\text{sc}(u^{(1)}, \dots, u^{(\lambda)}) := \#\{i \in N \mid u_i^{(j)} \neq 0, \exists j \in \{1, 2, \dots, \lambda\}\}$
 $= |\text{supp}(u^{(1)}) \cup \dots \cup \text{supp}(u^{(\lambda)})|$)

Theorem 3 (Shiromoto (1995))

$$W_{c^+}^{(\lambda)}(x, y) = \frac{1}{|C|^\lambda} W_c^{(\lambda)}(x + (q^\lambda - 1)y, x - y)$$

Remarks (1) $\lambda = 1$ とおることにより, $W_c^{(1)}(x, y) = W_c(x, y)$ とおき, Th1の恒等式と一致する.

(2) $\lambda = 2$ とおることにより, $W_c^{(2)}(x, y) = W_{c, c}(x, y, y, y)$ とおき

1). Th2の恒等式と一致する。

つまり、Th3は、Th1, Th2の拡張になっている。

Example H_3 : binary Hamming code of length 3

$$H_3 = \{000, 110, 101, 011\}, \quad H_3^\perp = \{000, 111\} \quad \text{511}$$

$$W_{H_3}^{(\lambda)}(x, y) = x^3 + 3(2^\lambda - 1)xy^2 + (4^\lambda - 3 \cdot 2^\lambda + 2)y^3$$

$$W_{H_3^\perp}^{(\lambda)}(x, y) = x^3 + (2^\lambda - 1)y^3$$

$$\begin{aligned} \text{こゝで、} & \frac{1}{|H_3|^\lambda} W_{H_3}^{(\lambda)}(x + (2^\lambda - 1)y, x - y) \\ & = \dots = x^3 + (2^\lambda - 1)y^3 \quad \text{となり} \end{aligned}$$

$$W_{H_3^\perp}^{(\lambda)}(x, y) = \frac{1}{|H_3|^\lambda} W_{H_3}^{(\lambda)}(x + (2^\lambda - 1)y, x - y) \text{ が成立する。}$$

(Theorem 3 の証明の概略)

$D \subseteq V$, $R \subseteq N$ に対して.

$$D(R) := \{u \in D \mid \text{supp}(u) \subseteq R\}$$

$$D^* := \text{Hom}_F(D, F) \cong V/D^\perp \quad \text{とあると}$$

$$0 \longrightarrow C^\perp(R) \xrightarrow{\text{inc}} V(R) \xrightarrow{f} C^* \xrightarrow{\text{res}} C(N-R)^* \longrightarrow 0$$

: exact (Tomoyuki Yoshida) とある。

$$\text{こゝで、} f: v \longmapsto (\hat{v}: u \longmapsto \langle u, v \rangle)$$

$$\therefore |C| \cdot |C^{\perp}(R)| = |V(R)| \cdot |C(N-R)| \quad \text{--- ①}$$

また、 $\tilde{W}_c^{(\lambda)}(x, y) := \sum_{R \in \mathcal{N}} |C(R)|^{\lambda} x^{n-|R|} y^{|R|} \quad (\forall \lambda \in \mathbb{R})$ とおくと、

$$\tilde{W}_{C^{\perp}}^{(\lambda)}(x, y) = \frac{1}{|C|^{\lambda}} \sum_{R \in \mathcal{N}} |V(R)|^{\lambda} \cdot |C(N-R)|^{\lambda} x^{n-|R|} y^{|R|} \quad (\because \text{①})$$

$$= \frac{1}{|C|^{\lambda}} \tilde{W}_c^{(\lambda)}(q^{\lambda} y, x)$$

また、二項定理を用いると、 $\tilde{W}_c^{(\lambda)}(x, y) = W_c^{(\lambda)}(x+y, y)$

$$\therefore W_{C^{\perp}}^{(\lambda)}(x, y) = \tilde{W}_{C^{\perp}}^{(\lambda)}(x-y, y)$$

$$= \frac{1}{|C|^{\lambda}} W_c^{(\lambda)}(q^{\lambda} y, x-y)$$

$$= \frac{1}{|C|^{\lambda}} W_c^{(\lambda)}(x + (q^{\lambda} - 1)y, x-y) //$$

次に、証明の所で定義した $\tilde{W}_c^{(\lambda)}(x, y)$ について、両辺を λ で微分し、 $\lambda = 0$ を代入すると、次のようになる。

$$\left. \frac{\partial}{\partial \lambda} \tilde{W}_c^{(\lambda)}(x, y) \right|_{\lambda=0} = \frac{1}{\log_2 e} \sum_{R \in \mathcal{N}} \dim C(R) x^{n-|R|} y^{|R|}$$

ここで、 $W_c^{\dim}(x, y) := \sum_{R \in \mathcal{N}} \dim C(R) x^{n-|R|} y^{|R|}$ とおくと、

Theorem 4 (T. Yoshida, Shiromoto (1995))

$$W_{C^{\perp}}^{\dim}(x, y) = (x+y)^{n-1} \{ (n-k)y - kx \} + W_c^{\dim}(y, x)$$