

Pless Power Moments
and
2-weight Projective Codes

山口大学経済学部

柏木 芳美

1 はじめに

元の符号と双対符号の重さ分布の関係式としては, MacWilliams identity というものが非常によく知られていて, サマーセミナーでも 2006 年に紹介した. ここでは, 同様の関係式である Pless power moments と呼ばれるものの 2-weight projective 符号 への 1 つの応用を紹介する. 「Are 2-Weight Projective Cyclic Codes Irreducible?」(J. Wolfmann, IEEE Trans. Inf. Theory, vol.51, pp.733–737, 2005) の前半部分の紹介でもある.

私自身 Pless power moments は聞いていたのだが, まだ応用したことがなかったので一度経験したかったわけである.

2 諸定義

- q を素数巾, $\mathbb{F}_q$ を q 元体, n を自然数とする. $\mathbb{F}_q^n$ の部分空間を 符号 (code) といい, n をその符号の 長さ という. 符号の長さが n で次元が k のとき, $[n, k]$ 符号 と呼ばれる. 以下, C は常に長さ n の符号を表すこととする.

- $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}_q^n$ に対し,

$$\mathbf{x} \cdot \mathbf{y} = \sum_{k=1}^n x_k y_k$$

により内積 $\cdot$ を定める.

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{x} \cdot \mathbf{u} = 0 \text{ for } \mathbf{u} \in C\}$$

を C の 双対符号 (dual code) という. C が $[n, k]$ 符号なら $C^\perp$ は $[n, n - k]$ 符号である.

- $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ とする.

$$\text{wt}(\mathbf{x}) = \#\{i \in \{1, \dots, n\} : x_i \neq 0\}$$

を $\mathbf{x}$ の重さ(weight) という. 重さは $0, 1, \dots, n$ のいずれかの整数である.

$$\min\{\text{wt}(\mathbf{u}) : \mathbf{u} \in C \setminus \{\mathbf{0}\}\}$$

を C の最小重さという. 最小重さは大きいほど符号の誤り訂正能力が高い. 符号理論で非常に重要な概念である.

N を自然数とし, $C \neq \{\mathbf{0}\}$ とする.

$$N = \#\{\text{wt}(\mathbf{u}) : \mathbf{u} \in C \setminus \{\mathbf{0}\}\}$$

のとき, C を N -weight 符号 という.

- C を N -weight 符号とし,

$$w_1, w_2, \dots, w_N$$

を, C の元の 0 と異なる重さの全体とする.

$1 \leq i \leq N$ に対して

$$A_i = \#\{\mathbf{u} \in C : \text{wt}(\mathbf{u}) = w_i\}$$

とおき, $0 \leq j \leq n$ に対して

$$B_j = \#\{\mathbf{v} \in C^\perp : \text{wt}(\mathbf{v}) = j\}$$

とおく.

B_j の定義は標準的だが, A_i の定義は必ずしも標準的ではない (w_i の代わりに i を用いているものが多い) ので注意すること.

尚, $N = 1$ のときは, w_1 を w と書くことにする.

- $B_1 = B_2 = 0$ のとき, C を projective 符号 という. それほど例外的な符号ではない.

3 Pless Power Moments

Pless power moments と呼ばれる次の結果が知られている ([5, Pless]).

命題 1. C を N -weight $[n, k]$ 符号とし, w_i, A_i, B_j は先に定義したとおりとする. このとき, 次が成り立つ.

$$(1) \sum_{i=1}^N A_i = q^k - 1.$$

$$(2) \sum_{i=1}^N w_i A_i = \{n(q-1) - B_1\} q^{k-1}.$$

$$(3) \sum_{i=1}^N w_i^2 A_i = [n(q-1)\{n(q-1)+1\} - B_1\{q+2(n-1)(q-1)\} + 2B_2] q^{k-2}.$$

元々の Pless power moments は, B_j を用いて

$$\sum_{i=1}^N w_i^r A_i \quad (r = 0, 1, 2, \dots)$$

を表したものである. ここでは, 最初の 3 つを与えた.

(1) に関しては, $\sum_{i=1}^N A_i$ に零ベクトルの 1 個を付け加えると C の元の個数となるが, $\dim C = k$ なので, その個数は q^k となる. 従って, 成り立つことが分かる.

4 1-weight Projective 符号

次の結果はよく知られている．この命題の符号は projective simplex 符号と呼ばれる．

命題 2. C を次元が k で長さが $n = \frac{q^k - 1}{q - 1}$ の projective 符号とする．このとき、 C は 1-weight 符号 で唯 1 つの 0 と異なる重さは q^{k-1} である．

1-weight 符号を考えるときは、次の命題が鍵となる．

命題 3. C を $[n, k]$ 符号とする． C が 1-weight 符号で $B_1 = 0$ ならば、

$$n = \lambda \frac{q^k - 1}{q - 1}, \quad w = \lambda q^{k-1}, \quad B_2 = \frac{\lambda(\lambda - 1)}{2}(q^k - 1)$$

となる自然数 λ が存在する．

証明. 命題 1(1) より $A_1 = q^k - 1$ ．よって、 $B_1 = 0$ なので、命題 1(2) より $w(q^k - 1) = wA_1 = n(q - 1)q^{k-1}$ ． q^{k-1} と $q^k - 1$ は互いに素なので、 q^{k-1} は w を割る．従って、 $w = \lambda q^{k-1}$ となる自然数 λ が存在する．従って、 $\lambda q^{k-1}(q^k - 1) = w(q^k - 1) = n(q - 1)q^{k-1}$ より、 $n = \lambda \frac{q^k - 1}{q - 1}$ となる．命題 1(3) に、これらの値を代入すると、

$$\lambda^2 q^{2(k-1)}(q^k - 1) = [\lambda(q^k - 1)\{\lambda(q^k - 1) + 1\} + 2B_2]q^{k-2}$$

となる．よって、

$$\lambda^2 q^k(q^k - 1) = \lambda^2(q^{2k} - 2q^k + 1) + \lambda(q^k - 1) + 2B_2$$

より

$$2B_2 = \lambda^2(q^k - 1) - \lambda(q^k - 1) = \lambda(\lambda - 1)(q^k - 1)$$

が得られる. □

系 4. C を $[n, k]$ 符号とする. C が 1-weight projective 符号ならば,

$$n = \frac{q^k - 1}{q - 1}, \quad w = q^{k-1}$$

となる.

証明. $B_2 = 0$ なので, 命題 3 の B_2 より $\lambda = 1$ となる. 従って, 命題 3 より結論が言える. □

5 2-weight Projective 符号

命題 5. C を $[n, k]$ 符号とする. C が 2-weight projective 符号ならば次が成り立つ.

$$\begin{aligned} n^2(q-1) - \{q(w_1 + w_2) - 1\}n + \frac{(q^k - 1)w_1w_2}{(q-1)q^{k-2}} &= 0, \quad (1) \\ A_1 &= \frac{(q^k - 1)w_2 - n(q-1)q^{k-1}}{w_2 - w_1}, \\ A_2 &= \frac{n(q-1)q^{k-1} - (q^k - 1)w_1}{w_2 - w_1}. \end{aligned}$$

証明. C は 2-weight で $B_1 = B_2 = 0$ なので, 命題 1 は

$$A_1 + A_2 = q^k - 1, \quad (2)$$

$$w_1 A_1 + w_2 A_2 = n(q-1)q^{k-1}, \quad (3)$$

$$w_1^2 A_1 + w_2^2 A_2 = n(q-1)\{n(q-1) + 1\}q^{k-2} \quad (4)$$

となる. ここで, 整数 a_0, a_1 を

$$a_0 = w_1 w_2, \quad a_1 = -(w_1 + w_2)$$

により定めると

$$(x - w_1)(x - w_2) = a_0 + a_1 x + x^2 \quad (5)$$

となる. ただし, x は変数. $a_0(2) + a_1(3) + (4)$ を計算すると

$$\begin{aligned} & a_0(A_1 + A_2) + a_1(w_1 A_1 + w_2 A_2) + w_1^2 A_1 + w_2^2 A_2 \\ &= A_1(a_0 + a_1 w_1 + w_1^2) + A_2(a_0 + a_1 w_2 + w_2^2) \end{aligned} \quad (6)$$

$$\begin{aligned} &= a_0(q^k - 1) + a_1 n(q-1)q^{k-1} + n(q-1)\{n(q-1) + 1\}q^{k-2} \\ &= n^2(q-1)^2 q^{k-2} + (a_1 q + 1)n(q-1)q^{k-2} + a_0(q^k - 1) \\ &= \left[n^2(q-1) - \{q(w_1 + w_2) - 1\}n + \frac{(q^k - 1)w_1 w_2}{(q-1)q^{k-2}} \right] (q-1)q^{k-2} \end{aligned} \quad (7)$$

式(5)より式(6)は0となる. 従って, 式(7)より式(1)が示される. $\square$

命題 5 を使うと, 次のちょっと面白い結果が得られる.

命題 6. C を 2-weight projective 符号とし, D を C の部分符号 (部分空間) で 2-weight projective とする. このとき, $D = C$ となる.

証明. $\dim C = r$, $\dim D = s$ とする. 命題 5 の式 (1) を考える. D は C の部分符号なので, D に対しても重さは w_1, w_2 となる. 従って, $n^2(q-1) - \{q(w_1+w_2)-1\}n$ は C に対しても D に対しても同じである. よって,

$$q^2 - \frac{1}{q^{r-2}} = \frac{q^r - 1}{q^{r-2}} = \frac{q^s - 1}{q^{s-2}} = q^2 - \frac{1}{q^{s-2}}$$

となる. 従って, $r = s$ なので $C = D$ となる. $\square$

参考として, 2-weight projective 符号の重さに関しては次が知られている ([1]).

命題 7. p を素数とし, q が p の巾とする. C が 2-weight projective 符号ならば, C の元の 0 と異なる重さは

$$p^s u \quad \text{あるいは} \quad p^s(u+1)$$

の形である. ただし, s は 0 以上の整数で u は自然数である.

6 補足

6.1 元の Pless Power Moments

$0 \leq i \leq n$ に対して

$$\tilde{A}_i = \#\{\mathbf{u} \in C : \text{wt}(\mathbf{u}) = i\}$$

とおく. $1 \leq i \leq N$ ならば,

$$A_i = \tilde{A}_{w_i}$$

となっている．本来の Pless power moments は次の形をする ([2] あるいは [5]).

命題 8. C を $[n, k]$ 符号とし, r を 0 以上の整数としたとき, 次が成り立つ.

$$\sum_{i=0}^n i^r \tilde{A}_i = \sum_{i=0}^n (-1)^i B_i \left\{ \sum_{\nu=0}^r \nu! S(r, \nu) q^{k-\nu} (q-1)^{\nu-i} \binom{n-j}{n-\nu} \right\},$$

$$\sum_{i=0}^n (n-i)^r \tilde{A}_i = \sum_{i=0}^n B_i \left\{ \sum_{\nu=0}^r \nu! S(r, \nu) q^{k-\nu} \binom{n-j}{n-\nu} \right\}.$$

ここで,

$$S(r, \nu) = \frac{1}{\nu!} \sum_{j=1}^{\nu} (-1)^{\nu-1} \binom{\nu}{j} j^r$$

は第 2 種の Stirling 数と呼ばれる．

6.2 MacWilliams Identity

x, y を変数として

$$W_C(x, y) = \sum_{i=0}^n \tilde{A}_i x^{n-i} y^i$$

とおく．サマーセミナーでも紹介したことがあるが ([3]), 次の結果はよく知られている ([4] あるいは [2]).

命題 9. C を符号としたとき, 次が成り立つ.

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

参考文献

- [1] P. Delsarte, Weights of linear codes and strongly regular normed spaces, *Discr. Math.*, vol.3, pp.47–64, 1972.
- [2] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, 2003.
- [3] Y. Kashiwagi, Proof of the MacWilliams Identity, *Proc. 22nd Summer Seminar on Lie Alg. Related Topics*, pp.36–46, 2006.
- [4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
- [5] V. Pless, Power moment identities on weight distributions in error-correcting codes, *Inf. Contr.*, vol.6, pp.147–152, 1962.
- [6] J. Wolfmann, Are 2-weight projective cyclic codes irreducible? *IEEE Trans. Inf. Theory*, vol.51, pp.733–737.