

一般化ハミング重さと線形符号

平松, 豊一 / Hiramatsu, Toyokazu

(出版者 / Publisher)

法政大学工学部

(雑誌名 / Journal or Publication Title)

法政大学工学部研究集報 / 法政大学工学部研究集報

(巻 / Volume)

38

(開始ページ / Start Page)

11

(終了ページ / End Page)

15

(発行年 / Year)

2002-03

(URL)

<https://doi.org/10.15002/00003781>

一般化ハミング重さと線形符号

Generalized Hamming weights and linear codes

平松豊一†

Toyokazu HIRAMATSU

Let C be a linear code. V.K.Weï proved in [5] that the performance of C , when used on the wire-tap channel of Type II, is determined by the generalized Hamming weights of C . In this report, the second generalized Hamming weights of cyclic codes are discussed. Its main tool is the theory of elliptic curves over finite fields.

Key Words: generalized Hamming weight, elliptic curves, Kloosterman codes

1 Introduction

1990年にV.K.Weï([5])によって導入された一般化ハミング重さの定義から始めよう。 p を素数とし、 $q = p^r$ ($r \geq 1$)とおく。 q 個の元からなる有限体を F_q で表す。 C を F_q 上の $[n, k]$ 線形符号とする。つまり、 C は F_q 上の n 次元線形空間 F_q^n の k 次元部分空間に他ならない($n \geq k$)。さて、 C の一般化ハミング重さを、Weïは次のように定義した。まず、 C のサポートを

$$S(C) = \{i : \exists v = (\dots, v_i, \dots) \in C, v_i \neq 0\}$$

とし、 C の r 次元一般化ハミング重さ $d_r(C)$ ($1 \leq r \leq k$)を

$$d_r(C) = \min\{|S(D)|; D \text{ は } C \text{ の } r \text{ 次元部分空間}\}$$

で定義する。ここで、 $| \cdot |$ は有限集合の元の個数を表す。 $\{d_r(C) : 1 \leq r \leq k\}$ を C の重さ階層(hierarchy)という。特に、 $d_1(C)$ は C の最小(ハミング)重さ d と一致し、 $d_r (= d_r(C))$ はその一般化になっている。最小重さ d が、符号 C にとって最も重要なパラメータの一つであることはよく知られた事実である。しかし、この定義からは d_r が d の自然な一般化になっていることは数学的に仲々読みとれない。そこで、ここでは、 d_r のもっと自然な幾何学的表現を求めてみよう。そのために、まず、 d の表現から始める。

線形空間 F_q^n は次のような自然なハミングノルムをもつ。それは

$$S(v) = \{i : v_i \neq 0\}$$

とするとき

$$\|v\| = |S(v)|$$

で定義される。そのとき、 d は

$$d = \min\{\|v\| : v \in C, v \neq 0\}$$

であった。さて、 q 元線形符号は $[n, k]$ システムであり、それは F_q 上の $(k-1)$ 次元射影空間 $P^{k-1}(=P)$ 内の n 個

(重複も許して)の点の集まり X 、これを射影システムという、の研究に他ならない。このとき、 C のパラメータ d は次のように表される：

$$n - d = \max\{|X \cap H| : H \text{ は } P \text{ 内の超平面}\}.$$

この形で、 d から d_r に拡張すると次のようになる。

D を F_q^n 内の r (≥ 1)次元部分空間とし、

$$S(D) = \{i : \exists v \in D, v_i \neq 0\},$$

$$\|D\| = |S(D)|$$

と定義する。このとき、

$$d_r = d_r(C) = \min\{\|D\| : D \subset C, \dim D = r\}$$

であったが、射影的システムの立場から

$$n - d_r = \max\{|X \cap \Pi| : \Pi \text{ は } P \text{ 内の余次元 } r \text{ の射影部分空間}\}$$

と定義される。余次元1のときが d 、1以上のときが d_r となる。以上のように、一般化ハミング重さは数学的には符号 C の最小重さ d のごく自然な一般化になっているが、工学的にみて、 d_r が線形符号の重要なパラメータに成り得るかどうかは、今後の課題であろう。

以下の節で、 d_r について、その基本性質、重さ階層等について論じてゆく。

2 Basic properties of generalized Hamming weights

一般化ハミング重さは美しい数学的構造をもつ。ここでは、その代表的なものをリストアップするとどめる([5])。

(1) 単調性: $[n, k]$ 符号 C に対し、

$$1 \leq d < d_2 < \dots < d_k \leq n$$

が成立する。

†システム制御工学科

(2) $[n, k, d]$ 符号 C の検査行列を H とする。そのとき、 $d_r = s$ であるための必要かつ充分な条件は次の (a) と (b) が成立することである :

- (a) H の任意の $s-1$ 列からなる行列の階数は $s-r$ 以上である。
- (b) H の s 列からなる行列で階数が $s-r$ となるものがある。

(3) 一般化シングルトン限界 : $1 \leq r \leq k$ に対し、

$$d_r \leq n - k + r$$

が成立する。

(4) 双対性: C を $[n, k]$ 符号とし、 C^\perp をその双対符号とする。そのとき、次が成立する。

$$\begin{aligned} \{d_r(C) : 1 \leq r \leq k\} \\ = \{1, 2, \dots, n\} - \{n+1-d_r(C^\perp) : 1 \leq r \leq n-k\}. \end{aligned}$$

(5) 一般化グリースマ限界: r を $1 \leq r \leq k$ に固定する。そして、 $[n, k]$ 符号 C で $d_r = d$ であったとする。そのとき、

$$n \geq d + \sum_{i=1}^{k-r} \left\lceil \frac{q-1}{q^i(q^r-1)} d \right\rceil$$

が成立する。

3 Generalized Hamming weights of cyclic codes

この節では、前半で代表的な巡回符号の一般化ハミング重さについて、既知の結果をリストアップする。また、後半では、まず、クルスターマン符号の一般化ハミング重さを求め、次に新しい結果である高次元クルスターマン符号の一般化ハミング重さ特に d_2 についての結果を報告する。まず、いくつかの結果をリストアップする :

(1) $[2^m - 1, 2^m - m - 1]$ ハミング符号 H_m とその双対符号 H_m^\perp に対し

$$\begin{aligned} d_r(H_m^\perp) &= \sum_{i=1}^r 2^{m-i}, \\ d_{2^i+x-i-1}(H_m) &= 2^i + x \quad (1 \leq i \leq m-1, 0 < x < 2^i) \end{aligned}$$

が成立する。

(2) $[n, k]$ Reed-Solomon 符号 C に対し

$$d_r(C) = n - k + r \quad (1 \leq r \leq k)$$

が成立する。

(3) 長さ $2^m - 1$ の原始的 t 重誤り訂正 2 元 BCH 符号を $BCH(t, m)$ で表す。このとき、次が成立する。

$$(a) \quad d_2(BCH(2, m)^\perp) = \frac{3}{2}d_1(BCH(2, m)^\perp) \quad (m \geq 5),$$

$$(b) \quad d_2(BCH(2, m)) = 8 \quad (m \geq 4),$$

$$(c) \quad d_3(BCH(2, m)) = 10 \quad (m \geq 4),$$

$$(d) \quad d_2(BCH(3, m)) = 11 \quad (m \geq 4).$$

Remark 3.1 $q = 2^m$ ($m \geq 4$) とし、 α を F_q の原始元とする。長さ $n = q - 1$ の 2 重誤り訂正 BCH 符号 $BCH(2, m)$ は検査行列

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \end{pmatrix}$$

をもち、次元 $= q - 1 - 2m$ で、最小重さ $d = 5$ である(嵩, 1968)。そこでまず、§2 の (5) より、次のグリースマ限界を得る:

$$d_r \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{2^i} \right\rceil.$$

これより、 $d_2 = d_2(BCH(2, m)) \geq 8$ である。従って、(b) を得るには、 $d_2 \leq 8$ を示せばよいことになる(その証明は例えば [4])。

次に、Melas 符号 $M(q)$ の双対符号として得られるクルスターマン符号 $M(q)^\perp$ の一般化ハミング重さを決定してみよう ([3])。

まず、次のことを注意する。 C を F_q 上の $[n, k]$ 線形符号とする。 D を C の r 次元部分空間とすると、

$$w(D) = |S(D)|$$

とおいて、 $w(D)$ を D の重さということがある。 C が特に binary なら、

$$2^{r-1}w(D) = \sum_{d \in D} w(d)$$

が成立する。ここで、 $w(d)$ は d のハミング重さを表す。従って、このときは、

$$d_r(C) = \frac{1}{2^{r-1}} \min \left\{ \sum_{d \in D} w(d) : D \text{ は } C \text{ の } r \text{ 次元部分空間} \right\} \quad \dots (3.1)$$

と表すことができる。

さて、Melas 符号 $M(q)$ とその双対符号 $M(q)^\perp$ の定義から始めよう。

$q = 2^m$ ($m \geq 3$) とし、 α を F_q の原始元とする。長さ $n = q - 1$ の Melas 符号 $M(q)$ は検査行列

$$H = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \alpha^{-1} & \dots & \alpha^{-(n-1)} \end{pmatrix}$$

をもつ 2 元巡回符号のことである。これは、次のように云っても同じである: α の最小多項式を $m(x) \in \mathbb{F}_2[x]$, α^{-1} の最小多項式を $m_-(x) \in \mathbb{F}_2[x]$ とするとき、 $M(q)$ は $m(x)m_-(x)$ で生成される巡回符号のことである。 $M(q)$ の次元は $q-1-2m$, 最小距離は m が偶数なら 3, m が奇数なら 5 である。その双対 $M(q)^\perp$ は

$$c(a, b) = \left(\text{Tr} \left(ax + \frac{b}{x} \right)_{x \in \mathbb{F}_q^\times} \right) \quad (a, b \in \mathbb{F}_q)$$

なる符号語から成り立っている。ここで、 $\text{Tr} = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}$ とする。従って、 $M(q)^\perp$ や $M(q)$ は α のえらび方によらない。

Remark 3.2 トレース符号について。

C を \mathbb{F}_{q^m} 上の長さ n の線形符号とし、

$$\begin{array}{ccc} \text{Tr} : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_q \\ \psi & & \psi \\ \alpha & \longmapsto & \text{Tr}(\alpha) \end{array}$$

$$\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \text{Tr}(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{m-1}}$$

とする。 C のトレース符号 $\text{Tr}(C)$ は

$$\text{Tr}(C) = \{ (\text{Tr}(\gamma_1), \dots, \text{Tr}(\gamma_n)) \in \mathbb{F}_q^n : (\gamma_1, \dots, \gamma_n) \in C \}$$

で定義される \mathbb{F}_q 上の長さ n の線形符号である。実は、 \mathbb{F}_q 上の巡回符号は常にトレース符号として表せることが知られている。

我々は、 $M(q)^\perp$ をクラスターマン符号と呼ぶことにする。以下で、 $M(q)^\perp$ の 2 次一般化ハミング重さ $d_2(M(q)^\perp)$ を求めてみよう。

まず、 $M(q)^\perp$ の最小重さ d についての結果 (Lachaud and Wolfmann) を述べておこう。

$$t_{\min} = \min\{t \in \mathbb{Z} : t^2 < 4q, t \equiv 1 \pmod{4}\}$$

とおく。そのとき、

定理 3.1 $M(q)^\perp$ の最小重さ d は

$$d = \frac{q-1+t_{\min}}{2}$$

で与えられ、 d を重さにもつ符号語は、

$$(q-1)\bar{h}(t_{\min}^2 - q)$$

個ある。ここで、 \bar{h} は類数を表す。

Remark 3.3 \bar{h} は次のように定義される。

$$Q(X, Y) = aX^2 + bXY + cY^2$$

を正定値整 2 次形式とすると、

$$\bar{h}(\Delta) = \#\{Q(X, Y) : \Delta = b^2 - 4ac\} / \text{SL}_2(\mathbb{Z})\text{-同値}$$

で与えられる。 $\Delta \in \mathbb{Z}$ が負で、 $\Delta \equiv 0, 1 \pmod{4}$ のときの $\bar{h}(\Delta) \neq 0$ である。2 次形式の還元理論より、

$$\bar{h}(\Delta) = \#\left\{ (a, b, c) \in \mathbb{Z}^3 : \begin{array}{l} b^2 - 4ac = \Delta, |b| \leq a \leq c, \\ b \geq 0 \text{ if } a = |b| \text{ or } a = c \end{array} \right\}$$

で、 $\bar{h}(\Delta)$ を計算することができる。

補題 3.2 $c(a, b)$ を $M(q)^\perp$ 内の重さ d の符号語とする。そのとき、次の (1), (2) が成り立つ。

(1) $\mathbb{F}_q^\times \ni \beta$ に対し、 $c(\beta a, \beta^{-1} b)$ も重さ d である。

(2) $\text{Gal}(\mathbb{F}_q/\mathbb{F}_2) \ni \sigma$ に対し、 $c(\sigma(a), \sigma(b))$ も重さ d である。

(証明) (1) $x \rightarrow \beta x$ が \mathbb{F}_q^\times の置換を与える。従って、 $c(\beta a, \beta^{-1} b)$ は $c(a, b)$ と同値であり、重さは変わらない。

(2) $\text{Gal}(\mathbb{F}_q/\mathbb{F}_2) \ni \sigma$ は同じく \mathbb{F}_q^\times の置換故 Tr は σ の作用で不変である: $w(c(a, b)) = w(c(\sigma(a), \sigma(b)))$

この補題より、 $c(a, 1)$ ($a \in \mathbb{F}_q^\times$) の形の符号語の中に最小重さをもつものがある。

さて、以上を踏まえて、 $d_2(M(q)^\perp)$ を決定しよう。

(1) m が偶数のとき、 $m \geq 4$ とする。

このとき、明らかに \mathbb{F}_q は 1 の原始 3 乗根 ρ を含む。

定理 3.3 $m(\geq 4)$ を偶数とする(このとき、 d は偶数)。このとき、 $M(q)^\perp$ の 2 次元部分符号で、そのすべての nontrivial な符号語が最小重さをもつものがある。

(証明) $c(a, 1)$ が最小重さ d をもつ符号語であったとする。このとき、これに $\rho \in \mathbb{F}_q^\times$ をほどこした $c(\rho a, \rho^2)$ も最小重さ d をもつ符号語である。 $c(a, 1)$ と $c(\rho a, \rho^2)$ は \mathbb{F}_2 上 1 次独立だから、この 2 つの符号語を base として $M(q)^\perp$ の 2 次元部分符号が得られる。このとき、

$$c(a, 1) + c(\rho a, \rho^2) = c(\rho^2 a, \rho) \quad (\rho^{-2} = \rho)$$

から、その和 $c(\rho^2 a, \rho)$ も最小重さをもつ符号語である。

系 $m(\geq 4)$ を偶数とする。そのとき、

$$\begin{aligned} d_2(M(q)^\perp) &= \frac{3}{2}d(M(q)^\perp) \\ &= \frac{3}{4}(q-1+t_{\min}). \end{aligned}$$

(証明) §2 の (5) より

$$d_2(M(q)^\perp) \geq \frac{3}{2}d(M(q)^\perp)$$

である。従って、

$$d_2(M(q)^\perp) \leq \frac{3}{2}d(M(q)^\perp)$$

以上は、通常のクルスターマン符号 $M(q)^\perp$ の一般化ハミング重さ(特に、 $d_2(M(q)^\perp)$)についての結果であるが、以下では高次元クルスターマン符号([1])の一般化ハミング重さについて考えてみよう。まず、高次元クルスターマン符号を導入し、その最小重さについて既知の結果をまとめておく。

$l \geq 2$ として、次の写像を定義する。 $q = p^m$ ($m \geq 2$) で

$$\begin{array}{ccc} \varphi_l: \mathbb{F}_q^l & \longrightarrow & \mathbb{F}_q^{(q-1)^{l-1}} \\ \cup & & \cup \\ a & \longmapsto & \left(\text{Tr}(a, x)_{x \in (\mathbb{F}_q^x)^{l-1}} \right) \end{array}$$

ここで、 $a = (a_1, \dots, a_l)$, $x = (x_1, \dots, x_{l-1})$ に対し

$$\text{Tr}(a, x) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a_1 x_1 + \dots + a_{l-1} x_{l-1} + a_l (x_1 \dots x_{l-1})^{-1}).$$

このとき、像 $\varphi_l(\mathbb{F}_q^l)$ を $l-1$ 次元の高次元クルスターマン符号と呼び、 $C_l(q)$ で表す。 $C_2(q) = M(q)^\perp$ である。 $l \neq 2$ のとき、 $C_l(q)$ は $[(q-1)^{l-1}, lm]$ 線形符号である。 $C_l(2^m)$ の最小重さ $d(l, m)$ については、次の結果がある([1])。 $m = 2$, $l \geq 8$; $m = 3$, $l \geq 5$; $m \geq 4$, $l \geq 6$ のとき、

$$d(l, m) = \frac{1}{2} \{ (2^m - 1)^{l-1} - (2^m - 1)^{l-3} \}.$$

そこで、 $C_l(2^m)$ の r 次一般化ハミング重さを $d_r(l, m)$ で表し、 $d(l, m)$ と $d_2(l, m)$ との関係調べてみると、我々の結果は、 m と l のある条件のもとで、

$$d_2(C_l(2^m)) = \frac{3}{2} d(C_l(2^m))$$

が成立するというものである。その証明はほんざつで長くになるので、[2]にゆずることにする。

参考文献

- [1] K.Chinen, T.Hiramatsu, Hyper-Kloosterman sums and their applications to the coding theory, *Applicable Algebra in Engineering, Communication and Computing*, vol.12(2001), pp.381-390.
- [2] T.Hiramatsu, G.Köhler, On the generalized Hamming weights of hyper-Kloosterman codes, submitted.
- [3] G.van der Geer, M.van der Vlugt, Generalized Hamming weights of Melas codes and dual Melas codes, *SIAM J.Disc.Math.*, vol.7, no. 4(1994), 554-559.
- [4] G.van der Geer, M.van der Vlugt, On generalized Hamming weights of BCH codes, *IEEE Trans.IT.*, vol.40, no. 2(1994), 543-546.
- [5] V.K.Wei, Generalized Hamming weights for linear codes, *IEEE Trans.IT.*, vol.37, no. 5(1991), 1412-1417.