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.Wei 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 Hammnig 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.Wei([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 $\mathbf{F}_q$ で表す。C を $\mathbf{F}_q$ 上の $[n,k]$ 線形符号とする。つまり、C は $\mathbf{F}_q$ 上の n 次元線形空間 $\mathbf{F}_q^n$ 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、Wei は次のように定義した。まず、C のサポートを

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

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、$|\ |$ 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 $\mathbf{F}_q^n$ 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

$$\|v\|=|\chi(v)|$$

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 $\mathbf{F}_q$ 上の $(k-1)$ 次元射影空間 $\mathbf{P}^{k-1}(=\mathbf{P})$ 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：

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

この形で、d から d_r に拡張すると次のようになる。

D を $\mathbf{F}_q^n$ 内の $r(\geq 1)$ 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

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

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にとどめる([5])。

(1) 単調性:$[n,k]$ 符号 C に対し、

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

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：$1 \le r \le k$ に対し、

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

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。

$$\{d_r(C) : 1 \le r \le k\} = \{1,2,\cdots,n\} - \{n+1-d_r(C^\perp) : 1 \le r \le n-k\}.$$

(5) 一般化グリースマ限界:r を $1 \le r \le k$ 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、

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

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

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

が成立する。

(2) $[n,k]$ Reed-Solomon 符号 C に対し

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

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 $\mathrm{BCH}(t,m)$ で表す。このとき、次が成立する。

(a) $d_2(\mathrm{BCH}(2,m)^\perp) = \frac{3}{2} d_1\left(\mathrm{BCH}(2,m)^\perp\right)$ $(m \ge 5)$,

(b) $d_2(\mathrm{BCH}(2,m)) = 8$ $(m \ge 4)$,

(c) $d_3(\mathrm{BCH}(2,m)) = 10$ $(m \ge 4)$,

(d) $d_2(\mathrm{BCH}(3,m)) = 11$ $(m \ge 4)$.

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

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

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:

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

これより、$d_2 = d_2(\mathrm{BCH}(2,m)) \ge 8$ である。従って、(b) を得るには、$d_2 \le 8$ 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 $\mathbf{F}_q$ 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き、

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

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、

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

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。

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

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

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 $m(x) \in \mathbf{F}_2[x]$, α^{-1} の最小多項式を $m_-(x) \in \mathbf{F}_2[x]$ 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

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

なる符号語から成り立っている。ここで、$\mathrm{Tr} = \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}$ 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 $\mathbf{F}_{q^m}$ 上の長さ n の線形符号とし、

$$\begin{array}{ccc} \mathrm{Tr}: \mathbf{F}_{q^m} & \longrightarrow & \mathbf{F}_q \\ \cup & & \cup \\ \alpha & \longmapsto & \mathrm{Tr}(\alpha) \end{array}$$

$$\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\alpha) = \mathrm{Tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

とする。C のトレース符号 $\mathrm{Tr}(C)$ は

$$\mathrm{Tr}(C) = \left\{(\mathrm{Tr}(\gamma_1), \cdots, \mathrm{Tr}(\gamma_n)) \in \mathbf{F}_q^n : (\gamma_1, \cdots, \gamma_n) \in C\right\}$$

で定義される $\mathbf{F}_q$ 上の長さ n の線形符号である。実は、$\mathbf{F}_q$ 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、$M(q)^\perp$ をクル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。

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

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、

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

個ある。ここで、$\tilde{h}$ は類数を表す。

Remark 3.3 $\tilde{h}$ 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次形式とするとき、

$$\tilde{h}(\Delta) = \#\left\{Q(X,Y) : \Delta = b^2 - 4ac\right\} / \mathrm{SL}_2(\mathbf{Z})\text{-同値}$$

で与えられる。$\Delta \in \mathbf{Z}$ が負で、$\Delta \equiv 0, 1 \bmod 4$ のときのみ $\tilde{h}(\Delta) \neq 0$ である。2次形式の還元の理論より、

$$\tilde{h}(\Delta) = \#\left\{ \begin{array}{r} (a,b,c) \in \mathbf{Z}^3 \ : \ b^2 - 4ac = \Delta, |b| \le a \le c, \\ b \ge 0 \ if \ a = |b| \ or \ a = c \end{array} \right\}$$

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

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

(証明) (1) $x \to \beta x$ が $\mathbf{F}_q^\times$ 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) $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_2) \ni \sigma$ は同じく $\mathbf{F}_q^\times$ 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、$c(a,1)$ $(a \in \mathbf{F}_q^\times)$ 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。

(I) m が偶数のとき。$m \ge 4$ とする。.

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

定理 3.3 $m(\ge 4)$ 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 $\rho \in \mathbf{F}_q^\times$ 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 $\mathbf{F}_2$ 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、

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

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 $m(\ge 4)$ 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

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

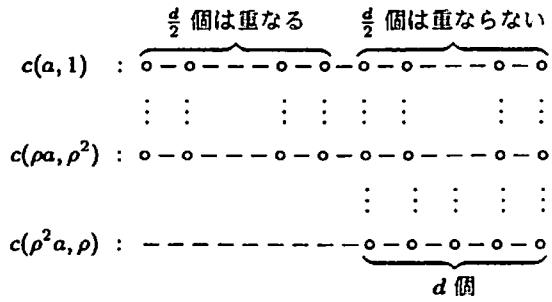
である。従って、

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

を示せばよい。定理 3.3 で定義した $M(q)^{\perp}$ の 2 次元部分符号 D に対し、

$$|S(D)| = \frac{3}{2}d(M(q)^{\perp})$$

を示せばよい。このことは (3.1) を使えば trivial であるが、定義からでも下図を参照すれば明らかである：



$$|S(D)| = \frac{d}{2} + \frac{d}{2} + \frac{d}{2} = \frac{3}{2}d$$

■

(II) m が奇数のとき。

m が偶数のときより事情は複雑であるが、有限体上の楕円曲線を利用すると、次の結果を得る。まず、

定理 3.4 $c(a,1)$ を $M(q)^{\perp}$ 内の最小重さをもつ符号語とする。このとき、$\mathrm{Tr}(\sigma(a)a^{-1}) = 0$ となるような $\sigma \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_2)$ があるならば

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

が成立する。

(証明) $\sigma \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_2)$, $\beta \in \mathbf{F}_q$ $(\beta \neq 0,1)$ をとり、$c(a,1)$ と $c(\beta\sigma(a),\beta^{-1})$ を考える。このとき、ある $\gamma \in \mathbf{F}_q$ $(\gamma \neq 0,1)$ をとって

$$c(a,1) + c(\beta\sigma(a),\beta^{-1}) = c(\gamma a,\gamma^{-1})$$

となるようにしたい。以下で、上式をみたすような σ と β をみつけよう:

$$\begin{cases} a + \beta\sigma(a) = \gamma a, \\ 1 + \beta^{-1} = \gamma^{-1}. \end{cases}$$

上式より、γ を消去して、β の 2 次方程式

$$\beta^2 + \beta = \frac{a}{\sigma(a)}$$

を得る。この 2 次方程式が解 $\beta \in \mathbf{F}_q$ $(\beta \neq 0,1)$ をもつための必要かつ十分な条件は

$$\mathrm{Tr}\left(\frac{a}{\sigma(a)}\right) = 0,$$

i.e.,

$$\mathrm{Tr}\left(\frac{\sigma^{-1}(a)}{a}\right) = 0.$$

この条件のもとで、$c(a,1)$ と $c(\beta\sigma(a),\beta^{-1})$ から得られる 2 次元部分符号の nontrivial なすべての元が最小重さをもつ。よって、以下は定理 3.3 の系の証明のときと同様にすればよい。

■

系 $M(q)^{\perp}$ が、最小重さ d をもつ符号語 $c(a,1)$ を含みかつ $\mathrm{Tr}(a) = 0$ が満たされているとき、

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

が成立する。

(証明) $\mathrm{Tr}(a) = 0$ から、定理 3.4 の条件が容易にみたされる。

■

さて、上で与えられた条件 $\mathrm{Tr}(a) = 0$ を $t_{\min}$ の条件に書きかえよう。

符号語

$$c(a,1) = (\mathrm{Tr}(ax + \frac{1}{x})_{x \in \mathbf{F}_q^{\times}})$$

に対し、アファイン方程式

$$y^2 + y = ax + \frac{1}{x}$$

によって、$\mathbf{F}_q$ 上で定義される楕円曲線 E_a を対応させる。このとき、E_a 上の $\mathbf{F}_q$-有理点の全体は、幾何学的に定義された加法で、アーベル群 $E_a(\mathbf{F}_q)$ を作り、その位数が $q+1-t_{\min}$ であることが知られている。更に、次の定理が成立する:

定理 3.5(G.van der Geer and M.van der Vlugt[1])
$q = 2^m$ とする。このとき

$$E_a(\mathbf{F}_q) \text{ が位数 } 8 \text{ の点をもつ} \iff \mathrm{Tr}(a) = 0$$

が成立する。

系 $t_{\min} \equiv 1 \bmod 8$ (つまり、$d \equiv 0 \bmod 4$)のとき、

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

が成立する。

(系の証明) $t_{\min} \equiv 1 \bmod 8$ とする。$m \geq 3$ だから、$E_a(\mathbf{F}_q)$ の位数は 8 の倍数である。従って、位数 8 の部分群をもつ。これより、$E_a(\mathbf{F}_q)$ は位数 8 の点をもつことがわかる。従って、定理 3.5 より

$$\mathrm{Tr}(a) = 0.$$

よって、定理 3.4 の系より結論を得る。

■

[1] G.van der Geer and M.van deer Vlugt: Kloosterman sums and the p-torsion of Jacobians,Math.Ann., 290(1991),549-563

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

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

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

$$\mathrm{Tr}(a,x) = \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(a_1x_1 + \cdots + a_{l-1}x_{l-1} + a_l(x_1\cdots x_{l-1})^{-1}).$$

このとき、像 $\varphi_l(\mathbf{F}_q^l)$ を $l-1$ 次元の高次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、

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

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 $d_2(l,m)$ との関係を調べてみると、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。その証明ははんざつで長くなるので、[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 Hammnig 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.