代数系と符号理論　第4回板書プリント

植松友彦 2007.4.24

1　【復習】ハミング符号と拡大ハミング符号の最小距離

補題 1.2.3. (教科書 p.8 参照)

C を (n,k) 符号とし、H をそのパリティ検査行列であるとしよう。C の最小距離は、H の 1 次従属な列の最小個数に等しい。

[補題の解釈] H の任意の $d-1$ 個の列が全て **1** 次独立で、H の d 個の列の中には **1** 次従属なものと **1** 次独立なものがあれば、最小距離は d である。

(7,4)2 元ハミング符号の場合 (第 3 回板書プリント p.2 参照)

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

2 元体は **0** と **1** しか含まないので、与えられたベクトルの組が **1** 次従属になるのは、それらのベクトルの総和が零になるときだけである。

1. 零ベクトルがないので、任意の 1 列は 1 次独立である。
2. どの 2 列を加えても零ベクトルにはならないので、任意の 2 列は 1 次独立である。
3. 1 列目、2 列目、3 列目を加えると零ベクトルになるので、3 列の中には 1 次従属のものがある。従って、最小距離は 3 である。

(8,4)2 元拡大ハミング符号の場合 (第 3 回板書プリント p.2 参照)

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

1. 零ベクトルがないので、任意の 1 列は 1 次独立である。
2. どの 2 列を加えても零ベクトルにはならないので、任意の 2 列は 1 次独立である。
3. 任意の 3 列を加えると 1 番下の要素は常に 1 となるため、任意の 3 列も全て 1 次独立である。
4. 1 列目、2 列目、3 列目、8 列目を加えると零ベクトルになるので、4 列の中には 1 次従属のものがある。従って、最小距離は 4 である。

2　ハミング限界

[定理 **1.3.1**](ハミング限界) C が要素数 q の有限体上の (n,k) 符号であり、t 重誤り訂正可能であれば、

$$\sum_{j=0}^{t}(q-1)^j\binom{n}{j} \leq q^{n-k}$$

でなければならない。

(証明)　重み t 以下の有限体 F 上の n 次元の点（ベクトル）の総数は、

$$S_t = 1+(q-1)\binom{n}{1}+(q-1)^2\binom{n}{2}+\cdots+(q-1)^t\binom{n}{t}$$

である。これは、符号語を中心とする半径 t の球に含まれる点の個数に等しい。t 個の誤りが訂正できるためには、各符号語を中心とした半径 t の球に共通部分があってはならないから、

$$S_t \cdot q^k \leq q^n$$

が成り立たねばならず、ハミング限界が得られる。□

特に、2 元ハミング符号については、$n=2^m-1$, $k=n-m$, $t=1$ から

$$\binom{n}{0}+\binom{n}{1} = 1+n = 2^m = 2^{n-k}$$

となり、ハミング限界の等号が成り立つ。等号を満たす符号のことを完全符号という。尚、2 元の完全符号としては、繰り返し符号、単一パリティ検査符号、ハミング符号、Golay 符号の 4 種類しかない。

3　重み分布

符号の誤り訂正能力について、最小距離以上の情報が必要な場合は重み分布を用いる。

[定義 **1.4.1**] 符号の重み分布とは、重み w の符号語の個数を A_w としたとき、ベクトル $A=(A_0,A_1,\cdots,A_n)$ のことである。また、重み分布母関数とは、

$$A(z)=\sum_{w=0}^{n}A_w z^w$$

で定まる。

線形符号の場合、A_w は任意の符号語から距離 w にある符号語の総数でもあることに注意しておく。

定理 1.4.1 (MacWilliams 恒等式)
$A(z)$ が (n,k)2 元符号 C の重み分布関数ならば、双対符号 $C^{\perp}$ の重み分布関数 $B(z)$ と $A(z)$ の間には、

$$B(z)=2^{-k}(1+z)^n A\left(\frac{1-z}{1+z}\right)$$

が成り立つ。

(各自教科書の証明を読んでおくこと)

[例 **1**] $(n,1)$ 繰り返し符号を考えよう。繰り返し符号の生成行列は、

$$G = [11\cdots1]$$

であり、重み分布関数は、

$$A(z) = 1 + z^n$$

となる。双対符号のパリティ検査行列は

$$H = [11\cdots1]$$

となり、双対符号は単一パリティ検査符号となる。従って、n が偶数のときの重み分布は

$$B(z) = \begin{cases} 1 + \binom{n}{2}z^2 + \binom{n}{4}z^4 + \cdots + \binom{n}{n}z^n & (n \text{ が偶数}) \\ 1 + \binom{n}{2}z^2 + \binom{n}{4}z^4 + \cdots + \binom{n}{n-1}z^{n-1} & (n \text{ が奇数}) \end{cases}$$

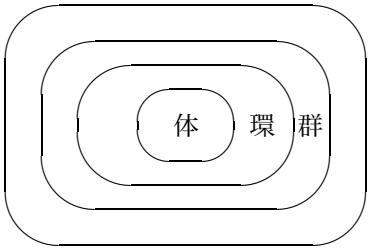
となる。MacWilliams の恒等式によれば、

$$\begin{aligned} B(z) &= 2^{-1}(1+z)^n \left\{1 + \left(\frac{1-z}{1+z}\right)^n\right\} \\ &= \frac{1}{2}\left\{(1+z)^n + (1-z)^n\right\} \end{aligned}$$

が得られる。これは上の事実と一致する。

4 抽象代数の基礎

符号理論の数学的基盤（抽象代数）群 (group)、環 (ring)、体 (field) について述べる。



4.1 群

群 G は、次の 4 つの性質を満足する任意の 2 項演算 $\circ$ をもつ集合である。

G1 $\forall a, b \in G$ ならば $a \circ b \in G$（閉包）

G2 $\forall a, b, c \in G$ ならば $a \circ (b \circ c) = (a \circ b) \circ c$ （結合則）

G3 $\exists e \in G, \forall a \in G$ について $a \circ e = e \circ a = a$ （単位元）

G4 $\forall a \in G$ に対し $\exists b \in G$、$a \circ b = b \circ a = e$ （逆元）

[例] 整数の集合は演算 $+$（加法）のもとで群をなす。

[例] （置換群）集合 $\{1,2,3\}$ から自分自身への全単射を $\{1,2,3\}$ 上の置換という。置換全体の集合を S_3 とする。2 つの置換 $\tau, \sigma \in S_3$ とするとき、置換の積 $\tau \circ \sigma$ を

$$\tau \circ \sigma(i) \longmapsto \tau(\sigma(i))$$

によって定義する。このとき S_3 は群をなす。τ を

$$\begin{pmatrix} 1 & 2 & 3 \\ \tau(1) & \tau(2) & \tau(3) \end{pmatrix}$$

によって表示する（k 列目は、k が $\tau(k)$ に置換されることを意味する）ことにすれば、

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

となり、明らかに $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ は単位元、$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ は自分自身が逆元、$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \overset{\text{逆元}}{\longleftrightarrow} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ なので群をなす。

群 G に属する元の個数を「（群の）位数」と呼ぶ。

$$\text{位数} \begin{cases} \text{有限} & : \quad \text{有限群} \\ \text{無限} & : \quad \text{無限群} \end{cases}$$

$\forall a, b \in G$ に対し、$a \circ b = b \circ a$ が成り立つとき、すなわち交換法則が成り立つ群を「可換群（アーベル群)」という。

[定理 2.1] 任意の群 G に対し、単位元および各元の逆元は、それぞれ唯一存在する。また $(a^{-1})^{-1} = a$ である。但し、a^{-1} は a の逆元を表す。

(証明) 2 つの異なる単位元 e と e' が存在するとすれば

$$e \overset{G3}{=} e \circ e' \overset{G3}{=} e'$$

から $e = e'$ である。$\forall a \in G$ に対し、2 つの逆元 b, b' が存在するとすれば、

$$b \overset{G3}{=} b \circ e \overset{G4}{=} b \circ (a \circ b') \overset{G2}{=} (b \circ a) \circ b' \overset{G4}{=} e \circ b' \overset{G3}{=} b'$$

から $b = b'$ である。最後に、

$$(a^{-1})^{-1} \circ (a^{-1}) = e$$

なので、$(a^{-1})^{-1}$ は a^{-1} の逆元である。他方、$a \circ a^{-1} = e$ は明らかなので、逆元の一意性より、

$$(a^{-1})^{-1} = a$$

である。 □

4.2 部分群

ある群 G の部分集合 H が群をなすとき、H を部分群という。H が群の部分群であることを証明するには、H が群の性質 $G1$ と $G4$ を満足することのみを示せば良い。

[例] G 自身は G の部分群である。また、e を G の単位元とするとき、$H = \{e\}$ は G の部分群である。明らかに、$e \circ e = e$ から $G1$ と $G4$ を満足する。

[例] 偶数の集合 $\{0, \pm 2, \pm 4, \cdots\}$ は通常の整数の加法において部分群である。

4.3 巡回群

有限群 G の要素 h に対して

$$h, h \circ h = h^2, h \circ h \circ h = h^3, \cdots$$

を作ると、必ず $h^n = e$ を満たす整数 n が存在する。なぜならば G は有限群だから必ず $h^j = h^i$ となる i と $j (j > i)$ が存在する。このとき、右から $(h^{-1})^i$ を乗じると

$$\underbrace{h \circ \cdots \circ h}_{j \text{ 個}} \circ \underbrace{h^{-1} \circ \cdots \circ h^{-1}}_{i \text{ 個}} = \underbrace{h \circ \cdots \circ h}_{i \text{ 個}} \circ \underbrace{h^{-1} \circ \cdots \circ h^{-1}}_{i \text{ 個}}$$

すなわち

$$h^{j-i} = e$$

が得られるからである。

特に、$h^n = e$ をみたす最小の n を h の位数 (order) と呼ぶ。また

$$H = \{h, h^2, h^3, \cdots, h^n = e\}$$

は G の部分群であり、h によって生成される巡回群 (cyclic group) と呼ぶ。また逆に、ある元 x のべき x^i $(i = 1, 2, \cdots)$ によって群 G の全ての元が表されるならば、x を群 G の生成元という。

H が群をなすことは、次のようにして分かる。

G1:

$$h^i \circ h^j = h^{i+j} = \begin{cases} h^{i+j} \in H & (i + j \leq n) \\ h^{i+j-n} \in H & (i + j > n) \end{cases}$$

G4: h^i の逆元は h^{n-i} である。なぜなら

$$h^i \circ h^{n-i} = h^n = e$$

[例 **2**] $G = \{1, 2, 3, 4, 5, 6\}$ において、演算 $x \circ y$ を $x \circ y = xy \bmod 7$ で定める。

- $h = 2$ とすると
  $h^2 = 2 \times 2 = 4$
  $h^3 = 2 \times 2 \times 2 = 8 = 1 \pmod 7$
  従って、$h = 2$ によって生成される巡回群 $H = \{2, 4, 1\}$

- $h = 4$ とすると
  $h^2 = 4 \times 4 = 2$
  $h^3 = 2 \times 4 = 1 \pmod 7$
  $h = 4$ によって生成される巡回群 $H = \{4, 2, 1\}$

- $h = 6$ とすると
  $h^2 = 6 \times 6 = 1 \pmod 7$
  $h = 6$ によって生成される巡回群 $H = \{6, 1\}$

- $h = 3$ とすると
  $h^2 = 3 \times 3 = 2 \pmod 7$
  $h^3 = 2 \times 3 = 6$
  $h^4 = 6 \times 3 = 4 \pmod 7$
  $h^5 = 4 \times 3 = 5 \pmod 7$
  $h^6 = 5 \times 3 = 1 \pmod 7$
  $h = 3$ によって生成される巡回群 $H = \{3, 2, 6, 4, 5, 1\} = G$

一般に、位数 n の群 G の元の位数は n の約数であり、従って、G の元から作られる巡回群の位数もまた n の約数である。