

2 第2回

2.1 ハミング距離

2つのベクトル $\mathbf{v} = (v_1, v_2, \dots, v_n)$ と $\mathbf{w} = (w_1, w_2, \dots, w_n)$ のハミング距離 $D(\mathbf{v}, \mathbf{w})$ は

$$D(\mathbf{v}, \mathbf{w}) \triangleq \sum_{i=1}^n d_H(v_i, w_i)$$

によって定義される。但し,

$$d_H(v_i, w_i) \triangleq \begin{cases} 0 & v_i = w_i \\ 1 & v_i \neq w_i \end{cases}$$

ハミング距離：2つのベクトルの異なっている成分の数

(例) $\mathbf{v} = (1010111), \mathbf{w} = (0110101)$ ならば $D(\mathbf{v}, \mathbf{w}) = 3$ 。

2.2 ブロック符号

q 元 (n, k, d) ブロック符号 C とは、長さが n の q 元ベクトル $\mathbf{v}_m$ ($m = 1, 2, \dots, M = q^k$) の集合である。すなわち

$$C = \{\mathbf{v}_m \in \{0, 1, \dots, q-1\}^n : m = 1, 2, \dots, M\}$$

特に

$\mathbf{v}_m$	符号語
n	符号長
k	情報記号数
$d = \min_{i \neq j} D_H(\mathbf{v}_i, \mathbf{v}_j)$	最小距離
$r = \frac{k}{n} = \frac{\log_q M}{n}$	符号化率 (rate, code rate)

(例) 2元 $(4, 2, 2)$ 符号

$$C = \{\mathbf{v}_1 = (0000), \mathbf{v}_2 = (1110), \mathbf{v}_3 = (0011), \mathbf{v}_4 = (1001)\}$$

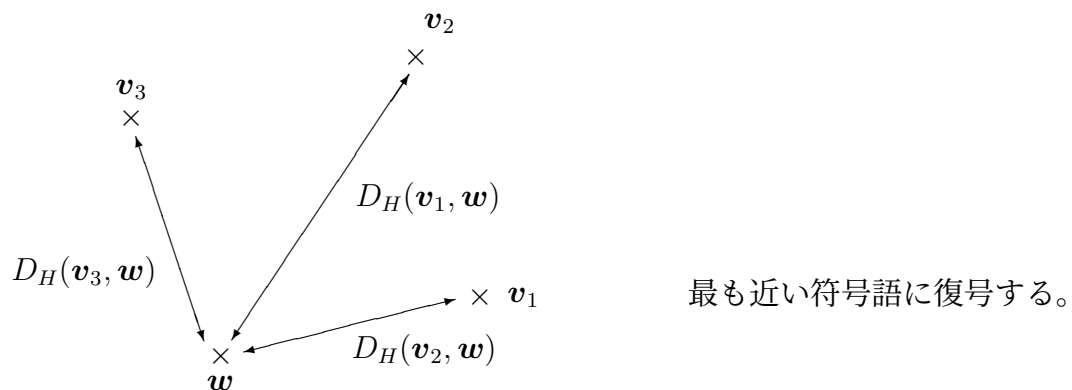
$$D_H(\mathbf{v}_1, \mathbf{v}_2) = 3, D_H(\mathbf{v}_1, \mathbf{v}_3) = 2, D_H(\mathbf{v}_1, \mathbf{v}_4) = 2$$

$$D_H(\mathbf{v}_2, \mathbf{v}_3) = 3, D_H(\mathbf{v}_2, \mathbf{v}_4) = 3, D_H(\mathbf{v}_3, \mathbf{v}_4) = 2$$

最小距離 $d = 2$ 、符号化率 $r = \frac{2}{4} = \frac{1}{2}$

2.3 最小距離復号法 (Minimum Distance Decoding)

符号 C について、符号語 $v_m \in C$ を送信、 w を受信したとする。このとき $D_H(v_j, w)$ を最小にするような符号語 $v_j \in C$ が送信されたと判定する復号法を最小距離復号法と呼ぶ。



定理 1 (n, k, d) 符号 C は、 t 個以下の全ての誤りを訂正できる。但し、

$$2t + 1 \leq d$$

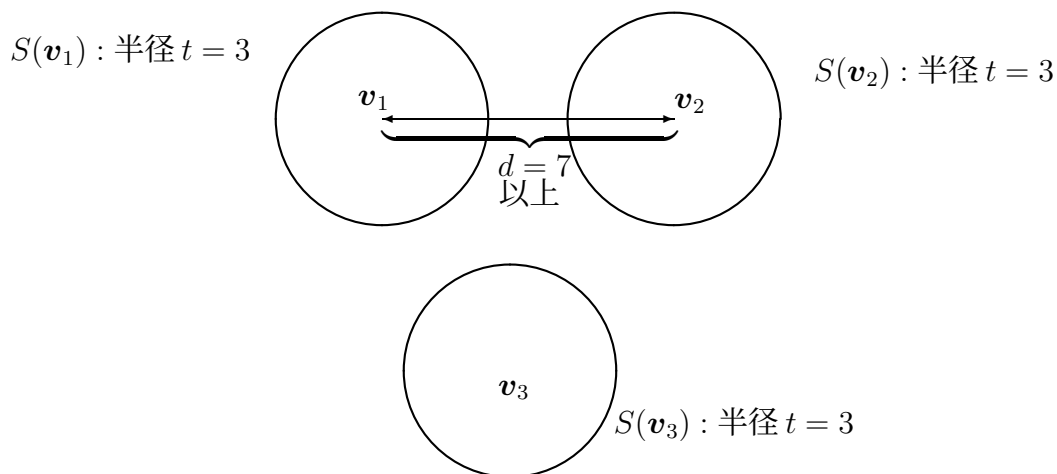
である。例えば

$$d = 5 \quad 2t + 1 \leq 5 \mapsto t \leq 2$$

$$d = 7 \quad 2t + 1 \leq 7 \mapsto t \leq 3$$

$$d = 6 \quad 2t + 1 \leq 6 \mapsto t \leq 2.5$$

証明 $d = 7, t = 3$ とすると



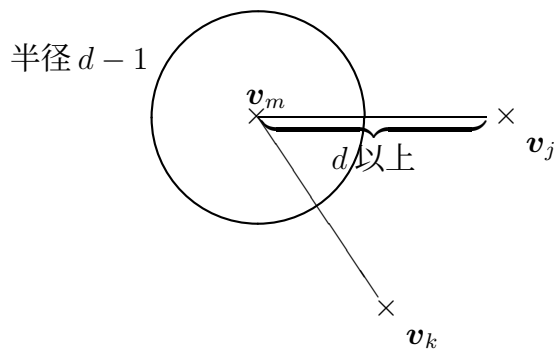
各符号語 v_m を中心に半径 t の球 $S(v_m)$ をつくと、 $d \geq 2t + 1$ から $S(v_m)$ は互いに共通部分（交わり）がない。従って、符号語 v_m を送信して、 t 個以内の誤りが生じて受信語 e を得た場合、 $w \in S(v_m)$ であるが、 $w \notin S(v_j)$ ($j \neq m$) である。従って、 $D_H(v_m, w) \leq t$ かつ $D_H(v_j, w) > t$ ($j \neq m$) が成り立つので、最小距離復号法によって、 t 個までの誤りが訂正できることが分る。 $\square$

(例) 繰り返し符号 $C = \{(00000), (11111)\}$

この符号の最小距離は5である。従って、2個までの誤りを訂正できる。事実(00000)を送信して(01001)を受信したとすれば、最小距離復号法によって(00000)に復号される。

定理 2 (n, k, d) 符号 C は $d - 1$ 個以下の全ての誤りを検出できる。

証明 誤りの検出は受信語 w が $w \in C$ であるか否かによって行われる。最小距離が d なので、送信した符号語 v_m に誤りが生じて他の符号語 v_j になる為には、少なくとも d 個以上の誤りが生じなければならない。従って、 $d - 1$ 個以下の誤りは必ず検出できる。



(例) 先の例の繰り返し符号では(00000)がもう1つの符号語(11111)に誤る為には5個の誤りが生じなければならない。

(例) 単一パリティ検査符号 $(n, n - 1, 2)$

符号語 v に生じた1個の誤りを検出できる。もう少し考えると、全ての奇数個の誤りを検出できる。

2.4 誤り訂正符号の評価尺度

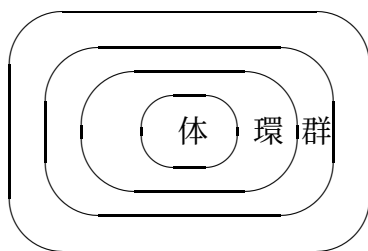
与えられた (n, k) に対して、最小距離 d を最大にする符号を最良符号と呼ぶ。(最良符号のデータベース：)

$$\frac{k}{n} \xleftrightarrow[\text{トレードオフ}]{\quad} \frac{d}{n}$$

実用的には最小距離 d が大きくかつ復号法の容易な符号が望まれる。(BCH 符号、リードソロモン符号)

2.5 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。



2.6 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 $+$ 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

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

によって定義する。このとき S_3 は群をなす。 τ の表示を

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

とすれば、

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

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、 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \xleftrightarrow{\text{逆元}} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ なので群をなす。

G の元の数：位数

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

$\forall a, b \in G$ に対し、 $a \circ b = b \circ a$ が成り立つとき、可換群（アーベル群）という。

定理 3 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。

(証明) 2つの異なる単位元 e と e' が存在するとすれば

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

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、

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

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。 □