代数系と符号理論 (O) 第2回板書プリント

制作：植松友彦

2014.4.9

授業中の食事は禁止する !!

1　第 1 回の復習

教科書を見ないでこれらの説明ができること。

- ベクトル空間
- ベクトル空間の基底
- 部分空間
- 有限体 $\mathbb{F}$
- 2 元体 $\mathbb{F}_2$
- ブロック符号
- 符号長
- 符号語
- 伝送速度
- (n, k) 線形符号
- 線形符号の性質 (4 つ)

2　生成行列と組織符号

定義 2.1 (生成行列)

(n, k) 線形符号 C の生成行列 G は、行ベクトルが C の基底となっている $k \times n$ 行列である。基底の選び方は複数存在するので、G もまた複数存在することに注意する。

符号化規則

$$\text{情報ベクトル } \boldsymbol{u} \Longrightarrow \text{符号語 } \boldsymbol{c} = \boldsymbol{u}G$$

行基本操作

(1) 任意の 2 つの行を交換する。

(2) 任意の行に F の元を乗じたものを他の任意の行に加える。

(3) 任意の行に F の零でない元を乗じる。

線形符号 C の任意の生成行列に対し、行基本操作を施したものもまた C の生成行列になっている。

組織符号

情報記号に対応する記号とパリティ検査記号に対応する記号を明確に分離できる符号のことを「組織符号 (systematic code)」と呼ぶ。

$$G = [I_k \ P] \tag{1}$$

の形式の生成行列は、組織線形符号を与えるものの典型的な例である (最初の k 記号は情報記号、後ろの $n-k$ 記号はパリティ検査記号)。

式 (1) の形の生成行列の作り方

2 元線形符号の生成行列 G が与えられたとき、組織線形符号を与える生成行列を求めるには、原則として行基本変形を用いれば良い。

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{\text{1 行目を 2 行目と 3 行目に加える}} \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$\xrightarrow{\text{2 行目と 3 行目を交換する}} \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{\text{2 行目を 1 行目に加える}} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow{\text{3 行目を 1 行目に加える}} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

しかし、行基本変形だけでは、式 (1) の形の生成行列が得られない場合もある。

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \xrightarrow{\text{2 行目を 1 行目に加える}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

G_2 の場合、符号化規則により、情報ベクトル (u_1, u_2) は

$$(u_1, u_2)G_2 = (u_1, u_2)\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} = (u_1, u_1, u_2, u_2)$$

と符号化されるので、1 番目と 2 番目の記号の片方、および 3 番目と 4 番目の記号の片方が情報記号になっている。式 (1) の形の生成行列を得るには、2 番目と 3 番目の列を入れ換える操作が更に必要である。

3　双対符号とパリティ検査行列

定義 2.2 (内積)

体 F 上の n 次元ベクトル空間 F^n の 2 つのベクトル

$$\boldsymbol{x} = (x_1, x_2, \ldots, x_n),\ \boldsymbol{y} = (y_1, y_2, \ldots, y_n)$$

の内積 $\boldsymbol{x} \cdot \boldsymbol{y}$ を

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$$

によって定義する。但し、右辺の積和演算は体 F 上の積と和によって行う。また、$\boldsymbol{x} \cdot \boldsymbol{y} = 0$ であるとき、「$\boldsymbol{x}$ と $\boldsymbol{y}$ は直交する」という。

定義 2.3 (双対符号)

体 F 上の線形符号 C の全ての符号語と直交する F^n の全てのベクトルからなる集合を C の「双対符号 (dual code)」と言い、$C^\perp$ によって表す。すなわち、

$$C^\perp = \{\boldsymbol{v} \in F^n : \boldsymbol{v} \cdot \boldsymbol{c} = 0,\ \forall \boldsymbol{c} \in C\}$$

である。

$\boldsymbol{v}$ が双対符号 $C^\perp$ の符号語である為の必要十分条件は、

$$\boldsymbol{v} G^T = 0$$

である。但し、$\cdot^T$ は転置を表す。これから直ちに双対符号は線形符号であることが分る。

尚、符号 C が双対符号 $C^\perp$ と一致する場合もあり、そのような符号 C を「自己双対符号」と呼ぶ。例えば、生成行列が

$$G_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

によって定まる符号が自己双対符号の例である (各自確かめよ)。

定義 2.4 (パリティ検査行列)

体 F 上の (n, k) 線形符号 C のパリティ検査行列 H とは、双対符号 $C^\perp$ の基底を行ベクトルとして並べた $(n-k) \times n$ 行列である。パリティ検査行列の定義から

$$G H^T = O \tag{2}$$

が成り立つこと、ならびに H の行ベクトルは線形独立であることに注意する。

特に符号 C が組織符号であり、生成行列 G が単位行列 I_k を用いて、

$$G = [I_k\ P] \tag{3}$$

と書ける場合、

$$H = [-P^T\ I_{n-k}] \tag{4}$$

は、式 (3) の生成行列 G に対応するパリティ検査行列である。

符号語とパリティ検査行列との直交性

任意の符号語 $\boldsymbol{c} \in C$ について、

$$\boldsymbol{c}H^T = \boldsymbol{0} \tag{5}$$

が成り立つ。

線形符号の表現法

- 生成行列 G を用いた表現法

$$C = \{\boldsymbol{u}G : \forall \boldsymbol{u} \in F^k\}$$

- パリティ検査行列 H を用いた表現法

$$C = \{\boldsymbol{c} \in F^n : \boldsymbol{c}H^T = \boldsymbol{0}\}$$

表 2.1 符号 C とその双対符号 $C^\perp$ の生成行列とパリティ検査行列の関係

符号	生成行列	パリティ検査行列
C	G	H
$C^\perp$	H	G

表 2.1 と同じことだが、行ベクトルが線形独立の $\ell \times n$ 行列 A を用いた次の 2 つの符号 C_1 と C_2 は互いに他の双対符号になっている。

符号	定義	符号長	情報記号数
C_1	A を生成行列 $(G = A)$ とする符号	n	ℓ
C_2	A をパリティ検査行列 $(H = A)$ とする符号	n	$n - \ell$

4 符号の最小距離

定義 2.5 (ハミング距離)

F^n の 2 つのベクトル $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ と $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ のハミング距離 $d_H(\boldsymbol{x}, \boldsymbol{y})$ は

$$d_H(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\triangle}{=} \sum_{i=1}^{n} d(x_i, y_i)$$

によって定義される。但し,

$$d(x_i, y_i) \stackrel{\triangle}{=} \begin{cases} 0 & x_i = y_i \\ 1 & x_i \neq y_i \end{cases}$$

である。

定義 2.6 (ハミング重み)

F^n のベクトル $\boldsymbol{x}$ のハミング重み $w_H(\boldsymbol{x})$ を

$$w_H(\boldsymbol{x}) \stackrel{\triangle}{=} d_H(\boldsymbol{x}, 0)$$

によって定義する。

定義 2.7 (ブロック符号の最小距離)

ブロック符号 C の最小距離 $d_{min}(C)$ は、異なる符号語間のハミング距離の最小値によって定義される。すなわち、

$$d_{min}(C) \stackrel{\triangle}{=} \min_{\substack{\boldsymbol{x},\boldsymbol{y}\in C \\ \boldsymbol{x}\neq\boldsymbol{y}}} d_H(\boldsymbol{x},\boldsymbol{y})$$

である。

定理 2.1

線形符号 C の最小距離 $d_{min}(C)$ は、非零の符号語の最小重み

$$w_{min}(C) \stackrel{\triangle}{=} \min_{\substack{\boldsymbol{x}\in C \\ \boldsymbol{x}\neq\boldsymbol{0}}} w_H(\boldsymbol{x})$$

に等しい。すなわち、$d_{min}(C) = w_{min}(C)$ が成り立つ。

線形符号の最小距離の計算法

2 元線形符号 C の生成行列 G が

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

で与えられたとする。このとき、この符号 C の全ての符号語は、基底

$$\{(100011), (010110), (001011)\}$$

の線形結合によって作られるので、

$$\begin{aligned} C \quad = \quad & \{(000000), (100011), (010110), (001011), \\ & (110101), (101000), (011101), (111110)\} \end{aligned}$$

となり、非零の符号語の最小重みは 2 である。従って、定理 2.1 から線形符号 C の最小距離は 2 である。

連絡事項：16 日 (水) は演習を行う。