1. 行列の演算

$N \times M$ 行列 $A = (a_{ij})$ と $M \times L$ 行列 $B = (b_{jk})$ の積 $C = AB$ は、

$$C = (c_{ik}), c_{ik} = \sum_{j=1}^{M} a_{ij} b_{jk}$$

で与えられる。

$A = (a_{ij})$ の転置行列 A^T は、

$$A^T = (c_{ij}), c_{ij} = a_{ji}$$

で与えられる。

2. ２元体　$\mathbb{F}_2$

$\mathbb{F}_2 = \{0, 1\}$ の演算は、整数として計算した後、計算結果が偶数なら 0 奇数なら 1 と置き換えればよい。特に、任意の $x \in \mathbb{F}_2$ に対し $x + x = 0$ が成立する。

3. 通信のベクトル表記

$\mathbb{F}_2 = \{0, 1\}$ を 2 元体とし、$\mathbb{F}_2$ 上の n 次元ベクトル空間を $\mathbb{F}_2^n$ と表すことにする。この時、n ビットのデータ $v_1 v_2 ... v_n$ は $v = (v_1, v_2, ..., v_n) \in \mathbb{F}_2^n$ とベクトル表記される。また、通信路で発生するエラーもベクトル $e = (e_1, e_2, ..., e_n)$ を使って表される。e_i の値は、その位置でエラーが発生している場合 1 を、エラーが発生していない場合は 0 をとる。データ v を送信しエラー e が発生した場合、受信されるデータは $r = v + e$ で表される。このとき、$v = r + e$、$e = v + r$ という関係も成立している ($\mathbb{F}_2$ 上のベクトル空間の特殊性！)。

4. 符号化

写像

$$\varphi : \mathbb{F}_2^k \ni u = (u_1, .., u_k) \to v = (v_1, ..., v_n) \in \mathbb{F}_2^n$$

を**符号化**と呼ぶ。ただし、$k \leq n$ とする。符号化によって得られる $\mathbb{F}_2^n$ の部分集合

$$C = \{\varphi(u); u \in \mathbb{F}_2^k\}$$

を**符号**と呼び、C の要素を**符号語**と呼ぶ。また、この章では、符号の例をいくつか紹介する。

4.1. 単一パリティ検査符号

符号化

$$u = (u_1, ..., u_k) \to v = (u_1, ..., u_k, \sum_{i=1}^{k} u_i) \tag{1}$$

を考える。ここで、v は行列

$$G = \begin{bmatrix} 1 & & & 1 \\ & \ddots & & \vdots \\ & & 1 & 1 \end{bmatrix} \tag{2}$$

を使って、$v = uG$ と表すことができる（行列 G は**生成行列**と呼ばれる）。従って、符号化 (1) に対応する符号 C は、以下のように書くことができる。

$$C = \{(u_1, ..., u_k, \sum_{i=1}^{k} u_i); u_1 \in \mathbb{F}_2, ..., u_k \in \mathbb{F}_2\} = \{uG; u \in \mathbb{F}_2^k\} \tag{3}$$

このようにして得られた符号 C は、**パリティ検査符号**と呼ばれる。

次に受信側の処理について説明する。送信されたパリティ検査符号 v に対し、受信語 $r = v + e = (r_1, ..., r_n)$ を得た時、受信者は $r_1 + \cdots + r_n = 1$ ならば誤りが発生したと判定し、$r_1 + \cdots + r_n = 0$ ならば誤りが発生していないと判定する。誤りが発生したと判定された場合、受信者は送信者にデータの再送を要求する。誤りが発生していないと判定された場合、受信者はデータ r の最初の $k = n - 1$ ビット $(r_1, ..., r_k)$ を受信ベクトルとして取り出す。

上記の誤り判定では、ベクトル $r = (r_1, ..., r_n)$ に対して

$$r_1 + \cdots + r_n \tag{4}$$

の値が 0 または 1 かによって判定を行った。ここで、行列

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix} \tag{5}$$

を用いて、式 (4) を、rH^T と書くことができる。行列 H を**パリティ検査行列**と呼ぶ。

パリティ検査符号 C は、パリティ検査行列 H を使って以下のように表すことができる。

$$C = \{v \in \mathbb{F}_2^n; vH^T = 0\} \tag{6}$$

証明：$C' = \{v \in \mathbb{F}_2^n; vH^T = 0\}$ と置き、これが (3) で与えられる C と等しいことをいえば良い。まず、$v = uG \in C$ とする。$GH^T = 0$ より $vH^T = uGH^T = 0$ が成立するので、$v \in C'$ であり、$C \subset C'$ がいえる。逆に、$v \in C'$ とするとき、$vH^T = 0$ であるが、これは $v_1 + \cdots + v_n = 0$ を意味している。さらに $v_i = -v_i, i = 1, 2, .., n-1$ に注意すると、$v_n = \sum_{i=1}^{n-1} v_i$ であり、$v \in C$ であることがわかる。よって $C \supset C'$ もいえた。

4.2 線形符号

$\mathbb{F}_2^n$ の部分集合 C が以下の性質を満たしているとき、C を**線形符号**と呼ぶ。

(i) 任意の $v, w \in C$ に対して、$v + w \in C$

(ii) 任意の $v \in C$ と任意の $\lambda \in \mathbb{F}_2$ に対して、$\lambda v \in C$

【注】上記の条件 (ii) は、「(ii)' $C \ni (0, 0, ..., 0)$」と置き換えることができる。

C の元、$g_1, ..., g_k \in C$ が以下の条件を満たすとき、$g_1, ..., g_k \in C$ を C の**基底**と呼び、$C = \langle g_1, ..., g_k \rangle_{\mathbb{F}_2}$ と書くことにする。

(i) $\lambda_1 g_1 + \cdots + \lambda_k g_k = 0 \Longrightarrow \lambda_1 = \cdots = \lambda_k = 0$

(ii) 任意の元 $v \in C$ に対し、$\lambda_1, ..., \lambda_k \in \mathbb{C}$ が存在し、
$v = \lambda_1 g_1 + \cdots + \lambda_k g_k$ が成立する。

ここで、g_j はベクトルであることに気をつけること（記号が煩雑になるのを避けるため $\vec{g}_j$ の矢印を省略している）。基底 $g_1, ..., g_k$ の取り方は 1 つに定まらないが、基底を構成する元の数 k は一意に定まる。この数 k のことを線形符号 C の**次元**と呼び、$k = \dim C$ と書く。

$u = (\lambda_1, ..., \lambda_k) \in \mathbb{F}_2^k$ とし、$k \times n$ 行列 G を以下のように定める。

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_k \end{bmatrix} \tag{7}$$

この時、$uG = \lambda_1 g_1 + \cdots + \lambda_k g_k$ であり、

$$C = \{uG; u \in \mathbb{F}_2^k\} \tag{8}$$

が成立する (G は符号 C の生成行列となっている)。

ベクトル $v = (v_1, ..., v_n) \in \mathbb{F}_2^n, w = (w_1, ..., w_n) \in \mathbb{F}_2^n$ の内積を、

$$v \cdot w = v_1 w_1 + \cdots + v_n w_n$$

によって定める。内積は以下の性質を持つ。

(i) $v \cdot (w_1 + w_2) = v \cdot w_1 + v \cdot w_2$

(ii) $v \cdot (\lambda w) = (\lambda v) \cdot w = \lambda(v \cdot w)$

$v \cdot w = 0$ の時、v と w は**直交**しているという。

C を線形符号とする。このとき、

$$C^\perp := \{v \in \mathbb{F}_2^n; v \cdot w = 0, \forall w \in C\} \tag{9}$$

を C の**双対符号**と呼ぶ。$C = \langle g_1, ..., g_k \rangle_{\mathbb{F}_2}$ に対して、
$v \cdot g_i = 0$,$i = 1, ..., k$ が成立しているとする。線形符号の定義により、任意の元 $w \in C$ に対し、$\lambda_1, ..., \lambda_k \in \mathbb{C}$ が存在し、$w = \lambda_1 g_1 + \cdots + \lambda_k g_k$ が成立しているので、
$v \cdot w = v \cdot (\lambda_1 g_1 + \cdots + \lambda_k g_k) = \lambda_1 v \cdot g_1 + \cdots + \lambda_k v \cdot g_k = 0$ となる。よって式 (9) を以下のように書き換えることができる。

$$C^\perp = \{v \in \mathbb{F}_2^n; v \cdot g_1 = \cdots = v \cdot g_k = 0\} \tag{10}$$

また、$vG^T = (v \cdot g_1, ..., v \cdot g_k)$ であることより、

$$C^\perp = \{v \in \mathbb{F}_2^n; vG^T = 0\} \tag{11}$$

と書くこともできる（注：$0 = (0, ..., 0)$ と略記している）。$C^{\perp}$ の基底を $h_1, ..., h_l$ とし (i.e. $C^{\perp} = \langle h_1, ..., h_l \rangle_{\mathbb{F}_2}$)、$C^{\perp}$ の $l \times n$ 生成行列 H を

$$H = \begin{bmatrix} h_1 \\ \vdots \\ h_l \end{bmatrix} \tag{12}$$

と定める。このとき、

$$C^{\perp} = \{uH; u \in \mathbb{F}_2^l\} \tag{13}$$

が成立している。

線形符号の例としては、式 (2)、(3) によって定義される単一パリティ検査符号があげられる。単一パリティ検査符号の双対符号 $C^{\perp} = \{v \in \mathbb{F}_2^n; vG^T = 0\}$ の生成行列 H を求めよう。$v = (v_1, ..., v_n)$ が $vG^T = 0$ を満たすことと、$v_1 = v_2 = \cdots = v_n$ は同値なので、$C^{\perp} = \{(0, 0, ..., 0), (1, 1, ..., 1)\} = \langle (1, 1, ..., 1) \rangle_{\mathbb{F}_2}$ であり、生成行列は

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

で与えられる。これは、単一パリティ検査符号のパリティ検査行列 (5) と一致している。