

9 第9回

体 F 上の線形符号 C の次元を k とすれば、 C の基底を適切に選ぶことで、(G に行基本変形と列の入れ換えを施すことで) 生成行列 G を

$$G = \begin{bmatrix} I_k & P \end{bmatrix}$$

の形で書くことができる。但し、

$$\begin{array}{l} I_k \quad k \times k \text{ の単位行列} \\ P \quad F \text{ 上の } k \times (n-k) \text{ 行列} \end{array}$$

このような G によって定まる線形符号を組織符号という。組織符号では、最初の k 記号に情報系列がそのまま現れていることに注意する。

$$iG = i \begin{bmatrix} I_k & P \end{bmatrix} = \left(\underbrace{i}_{k} \quad \underbrace{iP}_{n-k} \right)$$

i : 情報記号, iP : 検査記号

[例]

$$G_0 = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

2 行目を 1 行目に加える

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

1 行目と 2 行目を 4 行目に加える

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

3 行目と 4 行目を入れ換えることで

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

が得られる。

9.1 パリティ検査行列

線形符号 C の生成行列 G が

$$G = \begin{bmatrix} I_k & P \end{bmatrix}$$

と書けるとき

$$H = \begin{bmatrix} -P^T & I_{n-k} \end{bmatrix} \quad P^T : (n-k) \times k \text{ 行列}, I_{n-k} : (n-k) \times (n-k) \text{ 行列}$$

をパリティ検査行列という。このとき

$$\begin{aligned} GH^T &= \begin{bmatrix} I_k & P \end{bmatrix} \begin{bmatrix} -P^T & I_{n-k} \end{bmatrix}^T \\ &= \begin{bmatrix} I_k & P \end{bmatrix} \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} \\ &= -P + P \\ &= 0 \end{aligned}$$

が成り立つ。従って、線形符号 C の符号語はパリティ検査行列に直交する。すなわち、符号語を $v = iG$ とすれば

$$vH^T = iGH^T = i0 = 0$$

である。

定理 20 パリティ検査行列 H を有する F 上の線形符号 C において v が符号語である為の必要十分条件は

$$vH^T = 0$$

である。

(証明) $v \in C$ ならば $vH^T = 0$ は明らか。そこで、 $vH^T = 0$ のとき、 $v \in C$ であることを示す。 $v = (v_1, v_2, \dots, v_n) \in F^n$ とすると、 $vH^T = 0$ から

$$\begin{aligned} (v_1, v_2, \dots, v_n) \begin{bmatrix} -P^T & I_{n-k} \end{bmatrix}^T &= 0 \\ (v_1, v_2, \dots, v_n) \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} &= 0 \\ -(v_1, \dots, v_k)P + (v_{k+1}, \dots, v_n) &= 0 \\ (v_{k+1}, \dots, v_n) &= (v_1, \dots, v_k)P \end{aligned}$$

となる。従って、 $i = (v_1, \dots, v_k)$ とすれば、

$$v = (v_1, v_2, \dots, v_n) \begin{bmatrix} I & P \end{bmatrix} = iG$$

が得られ、 $v \in C$ であることが分る。

9.2 パリティ検査行列と最小距離

パリティ検査行列 H を有する F 上の符号 C が、 $v = (v_1, v_2, \dots, v_n) \in F^n$ を符号語とする為の必要十分条件は $vH^T = 0$ である。ここで、

$$H = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix} \quad h_i \in F^{n-k} \quad (i = 1, 2, \dots, n)$$

とすれば、 $vH^T = 0$ は

$$v_1 h_1 + v_2 h_2 + \cdots + v_n h_n = 0$$

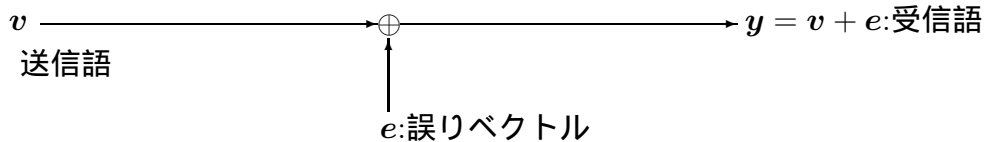
となる。ここで、 v のハミング重みは $v_1, v_2, \dots, v_n$ のうち非零のものの個数であり、線形符号 C では最小距離と最小重みが一致することから次の定理を得る。

定理 21 F 上の線形符号 C のパリティ検査行列 H の任意の $d-1$ 個の列が F 上で一次独立であるが、 d 個の列には一次従属のものがあるとすれば、 C の最小距離は d である。

[例] $GF(2)$ 上の符号長 $n = 2^m - 1$ ($m = 2, 3, \dots$) のハミング符号は $GF(2)^m$ の非零の全ての列ベクトルを並べたものをパリティ検査行列として有する。従って、最小距離は 3 である。

9.3 線形符号の復号

F 上の符号長 n 、次元 k の線形符号 C の符号語 v を加法的通信路を通して送る。通信路では誤りベクトル e が加わって、受信語 $y = v + e$



を受信したとする。線形符号 C のパリティ検査行列を H とするとき、

$$yH^T = s = (s_1, s_2, \dots, s_{n-k}) \in F^{n-k}$$

によって定まるベクトル s をシンδροームと呼ぶ。ここで、 $vH^T = 0$ に注意すれば、

$$s = yH^T = (v + e)H^T = vH^T + eH^T = eH^T$$

となり、シンδροームは送信語 $v \in C$ には依存せず、誤りベクトル e にのみによって定まる。

9.4 線形符号のシンδροームによる復号

1. 受信語 y からシンδροーム s を計算する。
2. s から誤りベクトル $\tilde{e}$ を推定する。推定できない場合は誤りを検出したとして復号を終わる。
3. 推定した誤りベクトル $\tilde{e}$ により、受信語 y を訂正し、訂正した受信語 $y - \tilde{e}$ から情報記号を取り出す。

以下ではステップ 2 について説明する。線形符号 C のパリティ検査行列を H 、誤りベクトルの集合を $E = \{e_0 = 0, e_1, e_2, \dots, e_M\}$ とする。このとき、シンδροーム $s_i = e_i H^T$ が全て異なるとすれば、シンδροーム s から E に含まれる誤りベクトルを一意的に定めることができる。そのような E の選び方として、次の定理が成り立つ。

定理 22 線形符号 C の最小距離を d とすると、集合

$$E = \left\{ e \in F^n : W_H(e) \leq \left\lfloor \frac{d-1}{2} \right\rfloor \right\}$$

に属するベクトルのシンδροームは全て異なる。すなわち、シンδροームを用いた復号法により $\left\lfloor \frac{d-1}{2} \right\rfloor$ 個までの誤りを訂正できる。

(証明) $e_1, e_2 \in E$ ($e_1 \neq e_2$) のシンδροームが等しかったとすると

$$e_1 H^T = e_2 H^T \quad \therefore (e_1 - e_2) H^T = 0$$

となり、 $e_1 - e_2$ は非零の符号語である。一方

$$W_H(e_1 - e_2) \leq W_H(e_1) + W_H(e_2) \leq 2 \cdot \left\lfloor \frac{d-1}{2} \right\rfloor \leq d-1$$

となり、符号 C の最小距離が d であることに矛盾する。

[例] パリティ検査行列

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

によって定まる $GF(2)$ 上の線形符号 C を考える。ここで、重み 1 以下の誤りベクトルの集合 E を考えると、誤りベクトルとシンδροームの関係は

誤りベクトル	シンδροーム
000000	000
000001	001
000010	010
000100	011
001000	100
010000	101
100000	111

となる。従って、受信語が (111101) であるとすればシンδροームは

$$s = (111101)H^T = (100)$$

となり、表から誤りベクトルは (001000) と推定される。従って、送信符号語は

$$(111101) - (001000) = (110101)$$

と推定される。他方、受信語が (111111) であるとすれば、シンδροームは (110) となる。しかし、この (110) は表にないので誤り検出となる。(訂正はできない)

特に、各シンδροーム s に対して、

$$eH^T = s$$

をみたす $e \in F^n$ の中で e の生起確率 $\Pr(e)$ が最大のものを選ぶことによって定まる復号法を最尤復号法という。