4.4. ハミング符号

ここでは、線形符号の例として**ハミング符号**を取り上げる。4.1 章で説明した単一パリティ検査符号は符号語の成分に生じた 1 個の誤りを検出することができる線形符号であった。これに対し、ハミング符号は符号語の成分に生じた 1 個の誤りを訂正することができる線形符号である。

ハミング符号のパリティ検査行列 H は、零ベクトル以外のすべての $\mathbb{F}_2^m$ の列ベクトルを並べて得られる。すなわち、H は $m \times (2^m - 1)$ 行列であり、ハミング符号の符号長は $n = 2^m - 1$ となる。たとえば、$m = 3$ の場合のハミング符号のパリティ検査行列は、

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

となりその符号長は、$n = 2^3 - 1 = 7$ となる。次に、No.2 のプリントの p.2 の定理を適用して式 (1) で与えられるパリティ検査行列 H に対応する生成行列 G を求める。そのために行列 (1) に対し以下のように行基本操作を施す。

(i) 1 行目を 3 行目に足し込む

(ii) 2 行目を 3 行目に足し込む

(iii) 3 行目を 1 行目と 2 行目にそれぞれ足し込む

その結果以下の行列 $\hat{H}$ を得ることができる。

$$\hat{H} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{2}$$

基本変形を行って得られた行列 $\hat{H}$ も元の行列 H と同じ線形符号を与えるパリティ検査行列であるので、この $\hat{H}$ に対して定理を適用すればよい。すなわち、

$$P^T = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \tag{3}$$

として、生成行列 G は以下で与えられる。

$$G = [I_4\, P] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{4}$$

従って、情報ビット $u = (u_1, u_2, u_3, u_4)$ に対する符号語 v は、

$$v = uG = (u_1, u_2, u_3, u_4, u_2 + u_3 + u_4, u_1 + u_3 + u_4, u_1 + u_2 + u_4)$$

で与えられる。この時、パリティ検査行列の性質により、任意の符号語 v に対し

$$vH^T = (0, 0, 0)$$

が成立している。送信者が情報ビット u に対し符号語 $v = uG$ を送信し、通信路でエラー e が発生した場合、受信者の受け取る受信語 r は

$$r = v + e$$

となる。このとき受信者は、

$$s = rH^T$$

を計算する。s は受信語 r の**シンドローム**と呼ばれる。受信語のシンドロームが $s = (0, 0, 0)$ となる場合、受信者は「通信エラーなし」と判断し、r の最初の 4 ビットを情報ビットとして受け取る。それ以外の場合は誤り訂正を行う必要がある。受信者の誤り訂正の方法について説明するために、行列 H^T の第 i 行のベクトルを h'_i とし、

$$H^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} h'_1 \\ h'_2 \\ h'_3 \\ h'_4 \\ h'_5 \\ h'_6 \\ h'_7 \end{bmatrix} \tag{5}$$

と書いておく。ハミング符号 $(m = 3)$ の場合、$h'_1, ..., h'_7$ は、零ベクトル以外の $\mathbb{F}_2^3$ のベクトルをすべて並べたものとなっている。また、第 i 成分

のみが 1 でそれ以外の成分はすべて 0 の 7 次元ベクトルを e_i と書くことにする (例えば、$e_2 = (0, 1, 0, 0, 0, 0, 0)$)。$e_i$ は第 i ビットにのみ誤りが生じる場合の誤りベクトルを表している。受信者は、受信データ r のシンドローム $s = rH^T$ を計算し $s \neq 0$ の場合は、$s = h'_j$ となる j の値を $j = 1, 2, .., 7$ の中から見つける。その値を $j = j_0$ とするとき、受信者は、$r' = r + e_{j_0}$ と受信語の誤りを訂正した後、r' の最初の 4 ビットを情報ビットとして受け取る。このような誤り訂正を行うことにより、1 個の誤りが生じた場合でも正しい情報を受け取ることが可能になる。実際、符号語 $v = uG$ を送信し誤り e_j が発生した場合、受信語は

$$r = v + e_j$$

となるが、この場合のシンドローム s は

$$s = rH^T = vH^T + e_jH^T = e_jH^T = h'_j$$

となり、

$$r' = r + e_j = v + e_j + e_j = v$$

と誤り訂正することにより符号語 v が正しく復元されている。

以上、$m = 3$ の場合に受信者の処理を説明したが、一般の m の場合も全く同様に考えることができる。

5 演習問題

問 1． 実ベクトル空間 ($\mathbb{R}$ 上のベクトル空間) において以下を計算しなさい。

(i)

$$\begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} =$$

(ii)

$$\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \\ 1 & 2 \end{bmatrix} =$$

(iii)

$$\begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 3 & 1 & 1 \end{bmatrix} =$$

(iv)

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 2 & 5 \end{bmatrix}$$

のとき、A^T を求めよ。

(v)

$$a = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, b = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$$

の時 $a^T b$ を求めよ。

問２． $\mathbb{F}_2$(２元体) 上のベクトル空間において以下を計算しなさい。

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

問3. 以下の表の A, B, C を埋めなさい

送信ベクトル	$v = (A, 1, 0)$
誤りベクトル	$e = (1, B, 0)$
受信ベクトル	$r = (0, 1, C)$

問4. 以下は単一パリティ検査符号を使って送受信を行った時の送受信者の動作をまとめた表である。

1. v_1、v_2 を求めなさい
2. r_1、r_2 を求めなさい
3. 誤り判定の欄を埋めなさい
4. 受信者の動作の欄を埋めなさい

情報ビット	$u_1 = (0, 1, 1, 1)$	$u_2 = (0, 0, 1, 0)$
符号語	v_1	v_2
誤りベクトル	$e_1 = (1, 0, 0, 0, 0)$	$e_2 = (1, 1, 1, 0, 0)$
受信語	r_1	r_2
誤り判定		
受信者の動作		

問 5. $C = \langle (1,0,0,1),(0,1,1,0) \rangle_{\mathbb{F}_2}$ の生成行列 G とパリティ検査行列 H を求めなさい。