4.3. 生成行列の変形

線形符号 $C \subset \mathbb{F}_2^n$ の次元が k であるとき、C を (n,k) 線形符号と呼ぶことにする。(n,k) 線形符号の生成行列は、基底 $g_1, ..., g_k$ を用いて、以下のように与えられた。

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_k \end{bmatrix} \tag{1}$$

ここで、基底の取り方は一意ではないので、生成行列 G も線形符号 C に対して一意に決まるわけではないことに注意する。たとえば、線形符号 C の任意の生成行列に対し、次の行基本操作を施したものもまた同じ線形符号 C の生成行列になっている。

(i) 任意の 2 つの行を交換する。

(ii) 任意の行を他の任意の行に加える。

実際、これらの基本操作を行って得られた行列を、

$$G' = \begin{bmatrix} g'_1 \\ \vdots \\ g'_k \end{bmatrix} \tag{2}$$

とするとき、$g'_1, ..., g'_k$ が C の基底となっているのは明らかである。従って、G' は C の生成行列になっている。

次に生成行列の列の入れ替えが符号に与える影響について見てみよう。符号 C の生成行列を G とするとき、C の符号語は、$v = uG, u \in \mathbb{F}_2^k$ で与えられる。この時、生成行列 G の第 i 列と第 j 列を入れ替えて得られる行列 G' を生成行列として持つ符号 C' の符号語 $v' = uG'$ は、符号 C の符号語 v の第 i 成分と第 j 成分を入れ替えたものである。すなわち、生成行列 G の列の入れ替えを行っても本質的な符号の性質は変わらないことがわかる。

生成行列 G に対して、上記の行基本変形 (i),(ii) と列の入れ替えを適宜行い、生成行列を以下の形に変形することができる。

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

ここで、I_k は、$k \times k$ の単位行列であり、P は、$k \times (n-k)$ 行列である。生成行列 G' を持つ符号の符号語は、

$$v = (u_1, ..., u_k)[I_k \; P] = (u_1, ..., u_k, v_{k+1}, ..., v_n)$$

で与えられる。ここで符号語の最初の k ビットの部分は、情報を表しており、**情報ビット**と呼ばれ、残りの $n-k$ ビットは冗長性を与えており、**パリティ検査ビット**と呼ばれる。

生成行列$G = [I_k\, P]$に対応するパリティ検査行列は、$H = [P^T\, I_{n-k}]$で与えられる。

証明:

$$GH^T = [I_k\ P] \begin{bmatrix} P \\ I_{n-k} \end{bmatrix} = [I_k P + P I_{n-k}] = [P + P] = 0 \tag{4}$$

ここで、

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_k \end{bmatrix}, H = \begin{bmatrix} h_1 \\ \vdots \\ h_{n-k} \end{bmatrix} \tag{5}$$

と表記すると、
$GH^T = 0$は、$g_i \cdot h_j = 0, i = 1, ..., k, j = 1, 2, .., n-k$を意味しており、$h_1, .., h_{n-k}$が、$C^{\perp}$の基底となっていることがわかる。すなわち、$H$は符号$C$のパリティ検査行列となっている。