11　第11回

11.1　巡回符号のパリティ検査行列

$GF(p)$ 上の符号長 $n = p^m - 1$ の巡回符号 C の生成多項式 $g(x)$ は $x^n - 1 = x^{p^m-1} - 1$ の因数なので、$x(x^{p^m-1} - 1)$ の因数である。従って、$g(x)$ の次数を r とし、$g(x)$ の根を $\beta_1, \beta_2, \cdots, \beta_r$ とし $m_i(x)$ を β_i の $GF(p)$ 上の最小多項式とすれば

$$g(x) = \mathrm{LCM}\{m_1(x), m_2(x), \cdots, m_r(x)\}$$

と書ける。なぜなら、右辺の多項式は根として $\beta_1 \sim \beta_r$ を含むので $g(x)$ は右辺を割り切る。逆に、β_i を根としてもてば、$g(x)$ は $m_i(x)$ で割り切れねばならないので、$g(x)$ が右辺で割り切れる。

次の定理は、上の巡回行列 C のパリティ検査行列を与える。

定理 24

$$H = \begin{bmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \beta_r & \beta_r^2 & \cdots & \beta_r^{n-1} \end{bmatrix}$$

で与えられる。

(証明)　$F = GF(p)$ とし

$$\begin{aligned} C_1 &= \{\boldsymbol{v} \in F^n : \boldsymbol{v}H^T = \boldsymbol{0}\} \\ C_2 &= \{v(x) = i(x)g(x) : i(x) \in F[x], \deg i(x) < n - r\} \end{aligned}$$

として、$C_1 = C_2$ を示す。

1. $\boldsymbol{v} \in C_1 \to v(x) \in C_2$
   $\boldsymbol{v}H^T = \boldsymbol{0}$ をみたす符号語の多項式表現を $v(x)$ とすれば、

$$\boldsymbol{v}H^T = \begin{pmatrix} \sum_{i=1}^{n-1} v_i \beta_1^i \\ \vdots \\ \sum_{i=1}^{n-1} v_i \beta_r^i \end{pmatrix} = \begin{pmatrix} v(\beta_1) \\ \vdots \\ v(\beta_r) \end{pmatrix} = \boldsymbol{0}$$

2. $v(x) \in C_2 \to \boldsymbol{v} \in C_1$
   $v(x) = i(x)g(x)$ ならば、$v(\beta_j) = i(\beta_j)g(\beta_j) = 0 \quad (j = 1 \sim r)$ なので、$\boldsymbol{v}H^T = \boldsymbol{0}$ が得られる。

[**例**]　$GF(2)$ 上の符号長 $2^3-1=7$ の巡回符号を考えよう。$GF(2)$ 上では、

$$x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1)$$

であり、$g(x)=x^3+x+1$ とする。ここで、x^3+x+1 の根 α によって定まる $GF(2^3)$ を考えると、$g(x)$ の根は α,α^2,α^4 である。なぜならば

$$\begin{aligned} g(\alpha) &= \alpha^3+\alpha+1=0 \\ g(\alpha^2) &= \alpha^6+\alpha^2+1=(\alpha^3+\alpha+1)^2=0 \\ g(\alpha^4) &= \alpha^12+\alpha^4+1=(\alpha^6+\alpha^2+1)^2=0 \end{aligned}$$

が成り立つからである。従って、この巡回符号のパリティ検査行列 H は、$\alpha^7=1$ に注意して

$$\begin{aligned} H &= \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^10 & \alpha^12 \\ 1 & \alpha^4 & \alpha^8 & \alpha^12 & \alpha^16 & \alpha^20 & \alpha^24 \end{bmatrix} \\ &= \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{bmatrix} \end{aligned}$$

となる。次に、パリティ検査行列 H から不要な行を取り除く為に、定理を 1 つ用意する。

定理 25 $GF(p)$ 上のある多項式 $m(x)$ が β を根として持てば、β^p もまた $m(x)$ の根である。

(証明)　$p=2$ について証明する。($p\neq 2$ の場合は各自考えよ)$m(x)=\sum_i m_i x^i$ とすれば

$$\begin{aligned} (m(x))^2 &= \sum_i m_i^2 x^{2i} + \sum_i \sum_{j\neq i} m_i m_j x^{i+j} \\ &= \sum_i m_i^2 x^{2i} + \underbrace{\sum_i \sum_{j>i} m_i m_j x^{i+j}}_{=} + \underbrace{\sum_i \sum_{j<i} m_i m_j x^{i+j}}_{} \\ &= \sum_i m_i^2 x^{2i} \\ &= \sum_i m_i x^{2i} \quad (\because GF(2)\text{ の全ての元は } x^2=x \text{ をみたす}) \\ &= m(x^2) \end{aligned}$$

従って、$m(\beta)=0$ ならば、$m(\beta^2)=(m(\beta))^2=0$ である。

[**例**]　先の例において、符号多項式 $v(x)$ が根 α をもてば、α^2, α^4 も根となる。すなわち、$v(\alpha)=0$ ならば自動的に $v(\alpha^2)=0,\ \ v(\alpha^4)=0$ である。そこで、パリティ検査行列を

$$H=\left[\begin{array}{ccccc} 1 & \alpha & \alpha^2 & \cdots & \alpha^6 \end{array}\right]$$

としても良い。この H の各要素を列ベクトルで表示することで、ハミング符号のパリティ検査行列 H(長さ 3 の非零のベクトル全体) が得られる。従って、ハミング符号は巡回符号である。

11.2　BCH 符号

定理 26　β を $GF(p^m)$ の元とするとき、β の最小多項式は

$$m(x)=(x-\beta)(x-\beta^p)(x-\beta^{p^2})\cdots(x-\beta^{p^{l-1}})$$

で与えられる。但し、l は $\beta^{p^l}=\beta$ をみたす最小の正整数である。特に、$\beta\in GF(p^m)$ から $\beta^{p^m}=\beta$ が成り立つので、$l\le m$ である。

(証明)　$p=2$ について証明する。

$$\begin{aligned}\{m(x)\}^2 &= (x-\beta)^2(x-\beta^2)^2(x-\beta^4)^2\cdots(x-\beta^{2^{l-1}})^2\\ &= (x^2-\beta^2)(x^2-\beta^4)(x^2-\beta^8)\cdots(x^2-\beta^{2^{l-1}})(x^2-\beta^{2^l})\\ &= (x^2-\beta^2)(x^2-\beta^4)\cdots(x^2-\beta^{2^{l-1}})(x^2-\beta)\\ &= m(x^2)\end{aligned}$$

従って、$m(x)=\sum_{i=0}^{l} m_i x^i$ とすると

$$\begin{array}{rcl}\{m(x)\}^2 & = & \sum_{i=0}^{l} m_i^2 x^{2i}\\ \| & & \\ m(x^2) & = & \sum_{i=0}^{l} m_i x^{2i}\end{array}$$

から、$m_i^2=m_i\quad(i=0,1,\cdots,l)$ が成り立つ。ここで、m_i は $x^2=x$ の根なので $m_i\in GF(2)$ であることが分る。

α を $GF(p^m)$ の原始元とする。このとき

$$\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{2t}$$

の全てを根とする次数最小の多項式 $g(x)$ を生成多項式とする。$GF(p)$ 上の符号長 $n=p^m-1$ の巡回符号を BCH 符号という。従って、α^i の $GF(p)$ 上の最小多項式を $m_i(x)$ とすれば

$$g(x)=\mathrm{LCM}\{m_1(x),m_2(x),\cdots,m_{2t}(x)\}$$

となる。一般に定理 26 から $\deg m_i(x) \leq m$ なので

$$\deg g(x) \leq 2tm$$

が成り立つ。特に $p = 2$ のときは、α^i と α^{2i} の最小多項式は一致するので

$$g(x) = \mathrm{LCM}\{m_1(x), m_3(x), \cdots, m_{2t-1}(x)\}$$

としても良い。この場合

$$\deg g(x) \leq tm$$

が成り立つ。

BCH のパラメータ

	$p = 2$	$p \neq 0$
符号長 n	$n = 2^m - 1$	$n = P^m - 1$
情報記号数 k	$k \geq n - mt$	$k \geq n - 2mt$
検査記号数 $n - k$	$n - k \leq mt$	$n - k \leq 2mt$
最小距離 d	$d \geq 2t + 1$	$d \geq 2t + 1$