12 第12回

定理 27 生成多項式 $g(x)$ が $\alpha, \alpha^2, \dots, \alpha^{2t}$ を根としてもつ BCH 符号の最小距離は少なくとも $2t + 1$ である。特に、この t によって定まる距離 $2t + 1$ を設計距離という。

補題 3 (Vandermonde の行列式)

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_s \\ \vdots & \vdots & & \vdots \\ x_1^{s-1} & x_2^{s-1} & \cdots & x_s^{s-1} \end{vmatrix} = \prod_{i>j} (x_i - x_j)$$

が成り立つ。

(証明) もし $x_i = x_j$ ならば、左辺の行列式は 0 である。従って $(x_i - x_j)$ を因数としてもつ。一方、右辺と左辺の次数は共に

$$1 + 2 + \cdots + (s - 1) = \frac{s(s - 1)}{2}$$

であり一致する。最後に、左辺の対角要素の積 $1 \cdot x_2 \cdot x_3^2 \cdots x_s^{s-1}$ の係数 1 が右辺でも一致することから補題を得る。

(定理の証明) BCH 符号のパリティ検査行列は

$$H = \underbrace{\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^t & (\alpha^t)^2 & \cdots & (\alpha^t)^{n-1} \end{bmatrix}}_{2t} \left. \vphantom{\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^t & (\alpha^t)^2 & \cdots & (\alpha^t)^{n-1} \end{bmatrix}} \right\} 2t$$

となる。この行列の任意の $2t$ 列 $i_1, i_2, \dots, i_{2t}$ から成る正方行列を D とする。すなわち

$$D = \begin{bmatrix} \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{2t}} \\ (\alpha^2)^{i_1} & (\alpha^2)^{i_2} & \cdots & (\alpha^2)^{i_{2t}} \\ \vdots & \vdots & & \vdots \\ (\alpha^{2t})^{i_1} & (\alpha^{2t})^{i_2} & \cdots & (\alpha^{2t})^{i_{2t}} \end{bmatrix}$$

となる。このとき、線形代数の理論から、 $|D| \neq 0$ ならば D は正則、すなわち $2t$ 個の列ベクトルは一次独立である。さて、

$$|D| = \alpha^{i_1} \alpha^{i_2} \cdots \alpha^{i_{2t}} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{2t}} \\ \vdots & \vdots & & \vdots \\ (\alpha^{i_1})^{2t-1} & (\alpha^{i_2})^{2t-1} & \cdots & (\alpha^{i_{2t}})^{2t-1} \end{vmatrix}$$

であり、右辺は Vandermonde の行列式であり、 $\alpha^{i_1}, \alpha^{i_2}, \dots, \alpha^{i_{2t}}$ は全て異なるので、 $|D| \neq 0$ であることが分る。従って、 H の任意の $2t$ 列は一次独立であり、最小距離は少なくとも $2t - 1$ 以上である。

[例] $x^{15} - 1$ を $GF(2)$ 上で因数分解すると

$$x^{15} - 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

となる。ここで、 $x^4 + x + 1$ の根 α によって定まる $GF(2^4)$ を考えると

$x + 1$	α^0 の最小多項式
$x^4 + x + 1$	$\alpha, \alpha^2, \alpha^4, \alpha^8$ の最小多項式
$x^4 + x^3 + x^2 + x + 1$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ の最小多項式
$x^2 + x + 1$	α^5, α^{10} の最小多項式
$x^4 + x^3 + 1$	$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ の最小多項式

となる。従って、 $t = 1, 2, 3$ について BCH 符号の生成多項式は

$$\begin{aligned} t = 1 \quad g(x) &= x^4 + x + 1 \\ t = 2 \quad g(x) &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \\ t = 3 \quad g(x) &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) \end{aligned}$$

となる。また、これらの符号のパラメータは

	情報記号数	最小距離
$t = 1$	$15 - 4 = 11$	3
$t = 2$	$15 - 8 = 7$	5
$t = 3$	$15 - 10 = 5$	7
	符号長 - $g(x)$ の次数	

で与えられる。

12.1 Reed-Solomon 符号

$GF(p^m)$ の原始元を α とし、 d を任意の自然数とするとき、生成多項式

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{d-1})$$

を有する符号長 $n = p^m - 1$ の $GF(p^m)$ 上の巡回符号を Reed-Solomon 符号という。

Reed-Solomon 符号は、次のパラメータを有する。

$$\begin{array}{ll} \text{符号長} & n = p^m - 1 \\ \text{情報記号数} & k = n - d + 1 \\ \text{検査記号数} & n - k = d - 1 \\ \text{最小距離} & d \end{array}$$

12.2 BCH 符号の復号法

C を符号長 $n = 2^m - 1$ 、設計距離 $2t + 1$ の $GF(2)$ 上の BCH 符号とする。 α を $GF(2^m)$ の原始元、 $v(x) \in C$ とすれば、BCH 符号の定義から

$$v(\alpha^j) = 0 \quad j = 1, 2, \dots, 2t$$

が成り立つ。通信路で加わる誤りの個数を $s (\leq t)$ 個とし、誤り多項式を

$$e(x) = \sum_{i=1}^s x^{k_i}$$

とする。但し、 $0 \leq k_1 < k_2 < \dots < k_s \leq n - 1$ は誤りの位置に対応する。このとき、受信語 $r(x)$ は

$$r(x) = v(x) + e(x)$$

であり、 $r(x)$ に対して

$$S_j = r(\alpha^j) = v(\alpha^j) + e(\alpha^j) = e(\alpha^j) = \sum_{i=1}^s \alpha^{j k_i} \quad j = 1, 2, \dots, 2t$$

をシンドロームと呼ぶ。 S_j から誤り多項式 $e(x)$ を求めることができれば、誤りを訂正できることになる。

(1) 誤りの個数 s を求める。

定理 28

$$M_\mu = \begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_\mu \\ S_2 & S_3 & & & \vdots \\ S_3 & & & & \vdots \\ \vdots & & & & \vdots \\ S_\mu & \cdots & \cdots & \cdots & S_{2\mu-1} \end{bmatrix}$$

とすれば、 M_μ は $s \leq \mu \leq t$ ならば $|M_\mu| = 0$ 、 $\mu = s$ ならば $|M_\mu| \neq 0$ である。

(証明)

$$\sigma(X_l^{-1}) = 1 + \sum_{i=1}^s \sigma_i X_l^{-i} = 0 \quad l = 1, 2, \dots, s$$

両辺に X_l^{s+j} を乗じて l について和を取ると

$$\begin{aligned} \sum_{l=1}^s X_l^{s+j} + \sum_{l=1}^s \sum_{i=1}^s \sigma_i X_l^{s+j-i} &= 0 \\ S_{s+j} + \sum_{i=1}^l \sigma_i \left(\sum_{l=1}^s X_l^{s+j-i} \right) &= 0 \\ \therefore S_{s+j} + \sum_{i=1}^s \sigma_i S_{s+j-i} &= 0 \end{aligned}$$

ここで、 $j = 1, 2, \dots, s$ とすれば定理を得る。

$|M_s| \neq 0$ であるので、この連立方程式を解いて $\sigma_1, \sigma_2, \dots, \sigma_s$ を求めれば $\sigma(x)$ が定まる。続いて、 $\sigma(\alpha^{-j})$, $j = 0, 1, 2, \dots, n-1$ を計算し $\sigma(\alpha^{-k_i}) = 0$ から誤り位置 k_i ($i = 1, 2, \dots, s$) を決定できる。