

代数系と符号理論 (O) 第10回板書プリント

制作：植松友彦

2014.6.24

第9回の復習

1. RS 符号の定義
2. RS 符号の最小距離
3. 補間多項式
4. 補間多項式を用いた誤り訂正

1 Vandermonde 行列とその性質

$x_1, x_2, \dots, x_n$ を体 F の要素とするとき

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{bmatrix}$$

の形式の行列を Vandermonde 行列という。

[定理 11.1]

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{i>j}^n (x_i - x_j)$$

次の定理は、RS 符号のパリティ検査行列を求める際に用いる。

[定理 11.2] $\beta \in \mathbb{F}_q$ を位数 (8.4 節参照) が n の元とし、 s と a を

$$s + a + 1 \leq n$$

を満足する任意の正の整数として、 $(a+1) \times n$ 行列 A と $s \times n$ 行列 B を

$$A = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \beta & \dots & \beta^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^a & \dots & \beta^{a(n-1)} \end{bmatrix}, \quad B = \begin{bmatrix} 1 & \beta & \dots & \beta^{n-1} \\ 1 & \beta^2 & \dots & \beta^{2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^s & \dots & \beta^{s(n-1)} \end{bmatrix}$$

によって定める。このとき、

$$BA^T = O, \quad AB^T = O$$

が成り立つ。特に、 $s + a + 1 = n$ の場合、行列 A の行ベクトルによって生成される部分空間と行列 B の行ベクトルによって生成される部分空間は、互いに他の直交補空間になっている。

2 RS 符号の生成行列とパリティ検査行列

$\mathbb{F}_q$ における位数 n の元を β ($n = q - 1$ ならば β は $\mathbb{F}_q$ の原始元) とし、 $x_j = \beta^{j-1}$ ($j = 1, 2, \dots, n$) によって定まる $RS(n, k)$ 符号のパリティ検査行列を求めよう¹。

$RS(n, k)$ 符号の場合、多項式 x^i ($i = 0, 1, \dots, k-1$) に対応する符号語が $(x_1^i, x_2^i, \dots, x_n^i)$ であるので、 $RS(n, k)$ 符号の生成行列は、これらを並べて得られる

$$G = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \dots & x_n^{k-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \beta & \dots & \beta^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{k-1} & \dots & \beta^{(n-1)(k-1)} \end{bmatrix}$$

である。従って、定理 11.2 において $a = k - 1$, $s = n - k$ とおくことで $A = G$ となり、 $RS(n, k)$ 符号のパリティ検査行列 H は

$$H = B = \begin{bmatrix} 1 & \beta & \dots & \beta^{n-1} \\ 1 & \beta^2 & \dots & (\beta^{n-1})^2 \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{n-k} & \dots & (\beta^{n-1})^{n-k} \end{bmatrix}$$

となる。

他方、 $\mathbf{c} = (c_1, c_2, \dots, c_n) \in \mathbb{F}_q^n$ を $RS(n, k)$ 符号の符号語とすると、

$$\mathbf{0} = \mathbf{c}H^T = \left[\sum_{i=1}^n c_i \beta^{i-1}, \quad \dots, \quad \sum_{i=1}^n c_i \beta^{(n-k)(i-1)} \right] \quad (1)$$

が成り立つ。そこで、符号語 $\mathbf{c} \in \mathbb{F}_q^n$ に対応する多項式 $c(x) \in \mathbb{F}_q[x]$ を

$$c(x) = c_1 + c_2 x + \dots + c_n x^{n-1}$$

によって定め、「符号多項式」と呼べば、式 (1) から、符号多項式 $c(x)$ について

$$c(\beta^i) = 0, \quad i = 1, 2, \dots, n - k \quad (2)$$

が成り立ち、符号多項式 $c(x)$ は常に $\beta, \beta^2, \dots, \beta^{n-k}$ を根として有する。

¹RS 符号の定義 (定義 10.1) においては、符号長 n と $x_1, x_2, \dots, x_n$ は任意であった。他方、本節では符号長 n と $x_1, \dots, x_n$ とが位数 n の元 β によって密接に関係付けられている。従って、このような特別な RS 符号について本節の議論が成り立つことに注意する。

[Peterson による RS(n, k) 符号の復号アルゴリズム]

初期設定: $t = \lfloor (n - k)/2 \rfloor$ とする。

入力: 受信語 $\mathbf{r} = (r_1, r_2, \dots, r_n)$

1. 受信多項式 $r(x) = r_1 + r_2x + \dots + r_nx^{n-1}$ に対し、シンドローム

$$S_i = r(\beta^i) \quad i = 1, 2, \dots, n - k$$

を計算する。

2. 連立方程式

$$\begin{bmatrix} S_1 & S_2 & \dots & S_{t+1} \\ S_2 & S_3 & \dots & S_{t+2} \\ \vdots & \vdots & & \vdots \\ S_{t+1} & S_{t+2} & \dots & S_{2t} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,t} \end{bmatrix} = \mathbf{0}$$

を解くことで、最小次数の非零の多項式

$$Q_1(x) = Q_{1,t}x^t + Q_{1,t-1}x^{t-1} + \dots + Q_{1,0}$$

を求める。実際には、 $Q_{1,t}$ から $Q_{1,0}$ に向けて可能な限り続けて零の値を取る非自明な解を探す。

3. $Q_1(x) = 0$ の根 $\beta^{i_1}, \dots, \beta^{i_t}$ を求め、誤りの位置 $i_1, \dots, i_t$ を決定する。
4. 連立方程式

$$\begin{bmatrix} \beta^{i_1} & \beta^{i_2} & \dots & \beta^{i_t} \\ \beta^{2i_1} & \beta^{2i_2} & \dots & \beta^{2i_t} \\ \vdots & \vdots & & \vdots \\ \beta^{ti_1} & \beta^{ti_2} & \dots & \beta^{ti_t} \end{bmatrix} \begin{bmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_t} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_t \end{bmatrix}$$

を解くことで、誤り値 $e_{i_1}, \dots, e_{i_t}$ を求め、誤り多項式

$$e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + \dots + e_{i_t}x^{i_t}$$

を定める。

5. $c(x) = r(x) - e(x)$ を送信符号語として出力する。

今後の授業日程

- 7月2日 演習6回
- 7月8日 休講
- 7月9日 講義11回
- 7月16日 講義12回
- 7月22日 演習7回
- 7月23日 演習(過去問)
- 7月30日 期末試験