代数系と符号理論　第10回板書プリント

植松友彦 2007.6.5

1　Vandermonde行列

補題 5.3.1 $\beta \in F_q$ を位数 n の元とし、$j = 1, 2, \cdots, n$ に対して $x_j = \beta^{j-1}$ とおく。また、$s + a + 1 \leq n$ として、行列

$$A = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^a & x_2^a & \cdots & x_n^a \end{bmatrix}, \quad B = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^s & x_2^s & \cdots & x_n^s \end{bmatrix}$$

を考える。このとき、

$$BA^T = 0, \quad AB^T = 0$$

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ことに注意する。

$a = n - 1$ のとき、行列 A を Vandermonde 行列といい、その行列式について次の定理が成り立つ。

定理 5.3.1

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

これまでの結果に基づき、β を F_q において位数 n の元として、$x_j = \beta^{j-1}$ $(j = 1, 2, \cdots, n)$ である特別な場合に、RS 符号のパリティ検査行列を得ることができる。この (n, k)RS 符号の生成行列は、

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \vdots & x_n^{k-1} \end{bmatrix}$$

であるので、従って、補題5.3.1 において $A = G$ とすれば、この符号のパリティ検査行列（$GH^T = 0$ となる行列 H）は、$x_j = \beta^{j-1}$ を用いて、

$$H = B = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-k} & x_2^{n-k} & \cdots & x_n^{n-k} \end{bmatrix} = \begin{bmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \cdots & (\beta^2)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{n-k} & \cdots & (\beta^{n-k})^{n-1} \end{bmatrix} \tag{1}$$

となる。これから、$c = (c_1, c_2, \cdots, c_n)$ を RS 符号の符号語とすると、

$$Hc^T = \begin{bmatrix} \sum_{i=1}^n c_i \beta^{i-1} \\ \sum_{i=1}^n c_i \beta^{2(i-1)} \\ \vdots \\ \sum_{i=1}^n c_i \beta^{(n-k)(i-1)} \end{bmatrix} = 0$$

が成り立つ。従って、符号語 $c \in F_q^n$ に対応する多項式 $c(x) \in F_q[x]$ を

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

によって定めると。

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

が成り立つことが分かる。

2　その他の復号アルゴリズム (Peterson のアルゴリズム)

以下では、F_q の位数 n の元 β を用い、$x_j = \beta^{j-1}$ $(j = 1, 2, \cdots, n)$ と選んで定まる (n, k)RS 符号を取り上げる。ここで述べる復号法は、次の 2 段階によって行われる。

1. 誤り位置多項式 $Q_1(x)$ を求め、誤り位置を求める。
2. 誤りベクトル（誤り値）を決定する。

まず、(n, k)RS 符号の符号語、誤りベクトル、受信語を

$$\begin{aligned} c &= (c_1, c_2, \cdots, c_n) \in F_q \quad : \text{符号語} \\ e &= (e_1, e_2, \cdots, e_n) \in F_q \quad : \text{誤りベクトル、但し } w(e) < d/2 = (n-k+1)/2 \\ r &= (r_1, r_2, \cdots, r_n) = c + e \quad : \text{受信語} \end{aligned}$$

によって定める。このとき、受信語のシンドローム $S = (S_1, \cdots, S_{n-k})$ を

$$S = Hr^T$$

によって定める。ただし、H は式 (1) で定まるパリティ検査行列である。

さて、符号語 c、誤りベクトル e、受信語 r に対応する多項式をそれぞれ

$$\begin{aligned} c(x) &= c_1 + c_2 x + \cdots + c_n x^{n-1} \\ e(x) &= e_1 + e_2 x + \cdots + e_n x^{n-1} \\ r(x) &= r_1 + r_2 x + \cdots + r_n x^{n-1} \end{aligned}$$

とすると、

$$S_i = r(\beta^i) = c(\beta^i) + e(\beta^i) = e(\beta^i), \quad i = 1, 2, \cdots, n-k$$

が成立する。

以下では、簡単のため最小距離 $d(= n-k+1)$ を奇数と仮定する。d が偶数の場合は $d-1$ に対して、同様の考察を行えば良い。

定理 5.4.1 誤り位置多項式 $Q_1(x)$ の係数は、次の連立方程式の解である。

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_{l_1+1} \\ S_2 & S_3 & \cdots & S_{l_1+2} \\ \vdots & \vdots & & \vdots \\ S_{l_1} & S_{l_1+1} & \cdots & S_{2l_1} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = 0$$

(証明)　$Q(x, y)$ を決定する連立方程式は次のように書ける。

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{l_0} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{l_0} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{l_0} \end{bmatrix} \begin{bmatrix} Q_{0,0} \\ Q_{0,1} \\ \vdots \\ Q_{0,l_0} \end{bmatrix} + \begin{bmatrix} r_1 & r_1x_1 & r_1x_1^2 & \cdots & r_1x_1^{l_1} \\ r_2 & r_2x_2 & r_2x_2^2 & \cdots & r_2x_2^{l_1} \\ \vdots & \vdots & \vdots & & \vdots \\ r_n & r_nx_n & r_nx_n^2 & \cdots & r_nx_n^{l_1} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = 0 \quad (2)$$

両辺に、

$$H = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{l_1} & x_2^{l_1} & \vdots & x_n^{l_1} \end{bmatrix}$$

を乗じることで、第一項を消去すると、

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{l_1} & x_2^{l_1} & \vdots & x_n^{l_1} \end{bmatrix} \begin{bmatrix} r_1 & r_1x_1 & r_1x_1^2 & \cdots & r_1x_1^{l_1} \\ r_2 & r_2x_2 & r_2x_2^2 & \cdots & r_2x_2^{l_1} \\ \vdots & \vdots & \vdots & & \vdots \\ r_n & r_nx_n & r_nx_n^2 & \cdots & r_nx_n^{l_1} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = 0$$

が得られる。ここで、

$$D(r) \quad = \quad \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{l_1} & x_2^{l_1} & \vdots & x_n^{l_1} \end{bmatrix} \begin{bmatrix} r_1 & r_1x_1 & r_1x_1^2 & \cdots & r_1x_1^{l_1} \\ r_2 & r_2x_2 & r_2x_2^2 & \cdots & r_2x_2^{l_1} \\ \vdots & \vdots & \vdots & & \vdots \\ r_n & r_nx_n & r_nx_n^2 & \cdots & r_nx_n^{l_1} \end{bmatrix}$$

とすれば、$D(r)$ の ij 要素 d_{ij} は、

$$d_{ij}(r) = \sum_{k=1}^{n} x_k^i r_k x_k^{j-1} = \sum_{k=1}^{n} r_k x_k^{i+j-1} = S_{i+j-1} \quad i = 1, 2, \cdots, l_1, j = 1, 2, l_1 + 1$$

を満足する。従って、$Q_1(x)$ は次の連立方程式の解である。

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_{l_1+1} \\ S_2 & S_3 & \cdots & S_{l_1+2} \\ \vdots & \vdots & & \vdots \\ S_{l_1} & S_{l_1+1} & \cdots & S_{2l_1} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = 0$$

他方、$Q_1(x)$ がこの方程式の解であるならば、

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{l_1} & x_2^{l_1} & \vdots & x_n^{l_1} \end{bmatrix} \begin{bmatrix} r_1 & r_1x_1 & r_1x_1^2 & \cdots & r_1x_1^{l_1} \\ r_2 & r_2x_2 & r_2x_2^2 & \cdots & r_2x_2^{l_1} \\ \vdots & \vdots & \vdots & & \vdots \\ r_n & r_nx_n & r_nx_n^2 & \cdots & r_nx_n^{l_1} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = 0$$

が成り立ち、

$$l_0 + l_1 + 1 = 2n - 2t - k = 2n - (n-k) - k = n$$

であることに注意すれば、補題 5.3.1 からベクトル

$$\begin{bmatrix} r_1 & r_1x_1 & r_1x_1^2 & \cdots & r_1x_1^{l_1} \\ r_2 & r_2x_2 & r_2x_2^2 & \cdots & r_2x_2^{l_1} \\ \vdots & \vdots & \vdots & & \vdots \\ r_n & r_nx_n & r_nx_n^2 & \cdots & r_nx_n^{l_1} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix}$$

は B の行ベクトルで張られる部分空間の直交補空間に含まれるので、このベクトルは、

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{l_0} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{l_0} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{l_0} \end{bmatrix}$$

の列ベクトルで張られる部分空間に含まれるので、方程式 (2) は解 $Q_0(x)$ をもつ。 Q.E.D.

$Q_1(x)$ を決定したとき、その根 $\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_t}$ を求めるには、通常 β^j $(j = 1, 2, \cdots, n)$ を全て代入して根になっているかを調べれば良い。このとき、

$$e = \underbrace{(\cdots, e_{i_1}, \cdots, e_{i_2}, \cdots, e_{i_t}, \cdots)}_{e_{i_1}, \cdots, e_{i_t} \text{以外の要素は全て零}}$$

に注意すれば、

$$He^T = (S_1, S_2, \cdots, S_{n-k})$$

から、次の連立方程式を解くことで、誤りの値 $e_{i_1}, e_{i_2}, \cdots, e_{i_t}$ を求めることができる。

$$\begin{bmatrix} x_{i_1} & x_{i_2} & \cdots & x_{i_t} \\ x_{i_1}^2 & x_{i_2}^2 & \cdots & x_{i_t}^2 \\ \vdots & \vdots & & \vdots \\ x_{i_1}^t & x_{i_2}^t & \cdots & x_{i_t}^t \end{bmatrix} \begin{bmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_t} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_t \end{bmatrix}$$

すなわち、

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

以上をまとめて、次のアルゴリズムを得る。

アルゴリズム **5.2.1**
入力:受信語 $r = (r_1, r_2, \cdots, r_n)$

1. $r(x) = r_n x^{n-1} + \cdots + r_2 x + r_1$ に対し、シンドローム $S_i = r(\beta^i)$, $i = 1, 2, \cdots, n-k$ を計算する。

2. 次の連立方程式の最小次数の解 $Q_1(x) = \sum_{j=0}^{l_1} Q_{1,j} x^j$ を求める。

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_{l_1+1} \\ S_2 & S_3 & \cdots & S_{l_1+2} \\ \vdots & \vdots & & \vdots \\ S_{l_1} & S_{l_1+1} & \cdots & S_{2l_1} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = 0$$

3. $Q_1(x)$ の根 $\beta^{i_1}, \cdots, \beta^{i_t}$ を求め、誤りの位置 $i_1, \cdots, i_t$ を決定する。

4. 連立方程式

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

   を解くことで、誤り値 $e_{i_1}, \cdots, e_{i_t}$ を求め、誤りベクトル e を定める。

5. $c = r - e$ を推定符号語として出力する。

[例]　F_5 上の (4,2,3)RS 符号を考えよう。2 の位数は 4 なので、$x_j = 2^{j-1}$ $(j = 1, 2, 3, 4)$ とする。情報多項式を $i(x) = x + 1$ とすれば、対応する符号語は、

$$c = (i(1), i(2), i(2^2), i(2^3)) = (i(1), i(2), i(4), i(3)) = (2, 3, 0, 4)$$

となる。誤り $e = (3, 0, 0, 0)$ が生じたとし、受信語

$$r = c + e = (2, 3, 0, 4) + (3, 0, 0, 0) = (0, 3, 0, 4)$$

を得たとする。
　受信語に対応する受信語多項式は、

$$r(x) = 3x + 4x^3$$

であり、$l_1 = 4 - 1 - 1 - (2 - 1) = 1$ に注意して、S_1, S_2 を求める

$$\begin{aligned} S_1 &= r(2) = 3 \cdot 2 + 4 \cdot 2^3 = 3 \\ S_2 &= r(2^2) = 3 \cdot 2^2 + 4 \cdot 2^6 = 3 \end{aligned}$$

となり、連立方程式

$$\left[\begin{array}{cc} 3 & 3 \end{array} \right] \left[\begin{array}{c} Q_{1,0} \\ Q_{1,1} \end{array} \right] = 0$$

を解くことで、$Q_{1,1} = 1, Q_{1,0} = 4$ が得られる。従って、誤り位置多項式は

$$Q_1(x) = x + 4$$

が得られ、$Q(2^0) = 0$ なので、誤り多項式は $e(x) = ax^0 = a$ となる。

$$e(2) = r(2) = S_1 = 3$$

から、$a = 3$ が得られ、$e(x) = 3$ となり、送信符号語は、

$$c(x) = r(x) - e(x) = -3 + 3x + 4x^3 = 2 + 3x + 4x^3 \leftrightarrow c = (2, 3, 0, 4)$$

となる。

例 **5.4.1** F_{11} 上の (10,5,6)RS 符号の復号。$x_j = 2^{j-1}$ $(i = 1, 2, \cdots, 10)$ とし、受信語 $r = (5, 9, 0, 9, 0, 1, 0, 7, 0, 5)$ に対応する受信語多項式を

$$r(x) = 5 + 9x + 9x^3 + x^5 + 7x^7 + 5x^9$$

とする。シンドロームを計算すると (d は偶数なので)$l_1 = 10 - 1 - 2 - (5 - 1)\underline{-1} = 2$

$$\begin{aligned} S_1 &= r(2^1) = 5 + 9 \cdot 2 + 9 \cdot 2^3 + 2^5 + 7 \cdot 2^7 + 5 \cdot 2^9 \\ &= 5 + 7 + 6 + 10 + 5 + 8 = 8 \\ S_2 &= r(2^2) = 8 \\ S_3 &= r(2^3) = 3 \\ S_4 &= r(2^4) = 10 \quad (S_{2l_1} \text{まで求める}) \end{aligned}$$

誤り位置多項式を定める連立方程式は、

$$\left[\begin{array}{ccc} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{array} \right] \left[\begin{array}{c} Q_{1,0} \\ Q_{1,1} \\ Q_{1,2} \end{array} \right] = \left[\begin{array}{ccc} 8 & 8 & 3 \\ 8 & 3 & 10 \end{array} \right] \left[\begin{array}{c} Q_{1,0} \\ Q_{1,1} \\ Q_{1,2} \end{array} \right] = \left[\begin{array}{c} 0 \\ 0 \end{array} \right]$$

基本変形をすると

$$\left[\begin{array}{ccc} 1 & 1 & 10 \\ 0 & 1 & 3 \end{array} \right] \left[\begin{array}{c} Q_{1,0} \\ Q_{1,1} \\ Q_{1,2} \end{array} \right] = \left[\begin{array}{c} 0 \\ 0 \end{array} \right]$$

が得られ、$Q_{1,2} = 1$ とおくと、$Q_{1,1} = 8, Q_{1,0} = 4$ が得られる。従って、誤り位置多項式は、

$$Q_1(x) = x^2 + 8x + 4$$

となり、$Q_1(2^3) = Q_1(2^9) = 0$ であるから、誤り多項式は、$e(x) = ax^3 + bx^9$ の形となる。ここで、

$$e(2) = r(2) = S_1 = 8, \quad e(2^2) = r(2^2) = S_2 = 8$$

に注意して連立方程式

$$\begin{bmatrix} 2^3 & 2^9 \\ 2^6 & 2^{18} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 8 \\ 8 \end{bmatrix}$$

すなわち、

$$\begin{bmatrix} 8 & 6 \\ 9 & 3 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 8 \\ 8 \end{bmatrix}$$

を解いて、$a = 3, b = 1$ を得る。従って、誤り多項式は、

$$e(x) = 3x^3 + x^9$$

であり、送信符号語は、

$$c(x) = r(x) - e(x) = 5 + 9x + 6x^3 + x^5 + 7x^7 + 4x^9$$

となる。