代数系と符号理論 (O) 第 9 回板書プリント

制作：植松友彦

2014.6.11

第 8 回の復習

- 部分体と拡大体
- 標数の定義
- 最小多項式の定義
- 最小多項式の性質
- 多項式表現とべき表現

1　リード・ソロモン符号

[定義 **10.1**] **(RS 符号)** 有限体 $\mathbb{F}_q$ の相異なる n 個の元を $x_1, \ldots, x_n$ とする。$k \leq n$ であるような正の整数 k に対し、$\mathbb{F}_q$ 上の次数が k 次未満の多項式の集合

$$\mathcal{P}_k \stackrel{\triangle}{=} \{f(x) \in \mathbb{F}_q[x] : \deg f(x) < k\}$$

を考える。このとき、RS(n, k) 符号は、

$$RS(n,k) \stackrel{\triangle}{=} \{(f(x_1), f(x_2), \cdots, f(x_n)) \in \mathbb{F}_q^n : f(x) \in \mathcal{P}_k\}$$

として定義される。

RS 符号の性質

- 有限体 $\mathbb{F}_q$ 上の RS 符号の符号長は高々 q である。
- RS 符号は有限体 $\mathbb{F}_q$ 上の線形符号である。
- $\mathcal{P}_k$ に属する多項式 $f(x) \neq g(x)$ について対応する RS 符号語は異なる。すなわち

$$(f(x_1), f(x_2), \cdots, f(x_n)) \neq (g(x_1), g(x_2), \cdots, g(x_n))$$

- RS(n, k) 符号の最小距離 d は $n - k + 1$ である。

2　Sudan による RS(n,k) 符号の復号法

初期設定：$t=\left\lfloor\frac{n-k}{2}\right\rfloor$
入力: 受信語 $\boldsymbol{r}=(r_1,r_2,\ldots,r_n)$

1. 次の一次方程式の非零の解を求める。

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-t-1} & r_1 & r_1x_1 & \ldots & r_1x_1^t \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-t-1} & r_2 & r_2x_2 & \ldots & r_2x_2^t \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-t-1} & r_n & r_nx_n & \ldots & r_nx_n^t \end{bmatrix} \begin{bmatrix} Q_{0,0} \\ Q_{0,1} \\ \vdots \\ Q_{0,n-t-1} \\ Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,t} \end{bmatrix} = \mathbf{0}$$

2. 多項式 $Q_0(x)$ と $Q_1(x)$ を

$$Q_0(x)=\sum_{j=0}^{n-t-1}Q_{0,j}x^j,\quad Q_1(x)=\sum_{j=0}^{t}Q_{1,j}x^j$$

   によって定める。

3. $Q_0(x)$ が $Q_1(x)$ で割り切れるならば、

$$g(x)=-\frac{Q_0(x)}{Q_1(x)}$$

   とし、$(g(x_1),g(x_2),\ldots,g(x_n))$ を送信符号語とする。もし割り切れなければ、復号に失敗したとする。

復号の計算例 (教科書の例 **10.2** とは違う計算例)

例 10.1 の符号語 $\boldsymbol{c}=(0,\alpha^2,\alpha,1)$ に誤り $\boldsymbol{e}=(0,1,0,0)$ が生じて受信語 $\boldsymbol{r}=(0,\alpha,\alpha,1)$ が受信されたとする。$n=4,\ k=2,t=\lfloor(4-2)/2\rfloor=1$ に注意すれば、連立方程式の係数行列は、

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0\cdot1 \\ 1 & \alpha & \alpha^2 & \alpha & \alpha\cdot\alpha \\ 1 & \alpha^2 & (\alpha^2)^2 & \alpha & \alpha\cdot\alpha^2 \\ 1 & 0 & 0^2 & 1 & 1\cdot0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha & \alpha & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

となる。これを行基本変形すると、$\alpha^2+\alpha+1=0$ に注意して、

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha & \alpha & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \overset{1\text{ 行目を他の行に加える}}{\longrightarrow} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & \alpha^2 & \alpha & \alpha & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\overset{2\text{ 行目を}\alpha\text{倍する}}{\longrightarrow} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^2 & \alpha^2 & 1 \\ 0 & \alpha & \alpha^2 & \alpha & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \overset{\substack{2\text{ 行目を}\alpha\text{倍して }3\text{ 行目に加える} \\ 2\text{ 行目を }4\text{ 行目に加える}}}{\longrightarrow} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^2 & \alpha^2 & 1 \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 \\ 0 & 0 & \alpha & \alpha & 1 \end{bmatrix}$$

$$\overset{3\text{ 行目を}\alpha^2\text{倍する}}{\longrightarrow} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^2 & \alpha^2 & 1 \\ 0 & 0 & 1 & \alpha & \alpha \\ 0 & 0 & \alpha & \alpha & 1 \end{bmatrix} \overset{3\text{ 行目を}\alpha\text{倍して }4\text{ 行目に加える}}{\longrightarrow} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^2 & \alpha^2 & 1 \\ 0 & 0 & 1 & \alpha & \alpha \\ 0 & 0 & 0 & 1 & \alpha \end{bmatrix}$$

が得られる。従って、与えられた連立方程式は、

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^2 & \alpha^2 & 1 \\ 0 & 0 & 1 & \alpha & \alpha \\ 0 & 0 & 0 & 1 & \alpha \end{bmatrix} \begin{bmatrix} Q_{0,0} \\ Q_{0,1} \\ Q_{0,2} \\ Q_{1,0} \\ Q_{1,1} \end{bmatrix} = \mathbf{0}$$

と等価である。この方程式の非自明な解は、$Q_{1,1}=1$ と置いて、下側の式から順に代入することで、

$$\begin{aligned} Q_{1,0} &= -\alpha Q_{1,1} = \alpha \\ Q_{0,2} &= -\alpha Q_{1,0} - \alpha Q_{1,1} = -\alpha^2 - \alpha = 1 \\ Q_{0,1} &= -\alpha^2 Q_{0,2} - \alpha^2 Q_{1,0} - Q_{1,1} = -\alpha^2 - 1 - 1 = \alpha^2 \\ Q_{0,0} &= -Q_{0,1} - Q_{0,2} = -\alpha^2 - 1 = \alpha \end{aligned}$$

となる。従って,

$$Q_0(x) = x^2 + \alpha^2 x + \alpha, \quad Q_1(x) = x + \alpha$$

が得られる。これから、情報多項式として

$$g(x) = -\frac{Q_0(x)}{Q_1(x)} = \frac{x^2 + \alpha^2 x + \alpha}{x + \alpha} = x + 1$$

が得られ、

$$(g(1), g(\alpha), g(\alpha^2), g(0)) = (0, \alpha^2, \alpha, 1)$$

が送信符号語となる。