

2019 年度 情報数理特論 B 練習問題 5

学籍番号 : _____

氏名 : _____

問題の質問や不明な点は、授業終了後またはオフィスアワーを利用して、質問してください。

出題者 : 幸山 直人
出題日 : 2019 年 7 月 2 日 (火)

問 1 次の (1)～(5) の問いに答え、 $\text{GF}(2^4)$ 上の 3 個の誤りが訂正可能な $[15, 9]$ RS 符号の受信語

$$\mathbf{y} = (\alpha^4, \alpha^7, 1, 0, 0, \alpha^{11}, \alpha, \alpha^{12}, 0, 0, 0, 0, 0, 0, 0)$$

の誤りの検出と訂正を行い、推定情報 $\hat{\mathbf{i}}$ を求めなさい ($q = 2^4, m = 1, t = 3$)。ただし、 α を $\text{GF}(2^4)$ の原始多項式 $x^4 + x + 1 (= 0)$ の 1 つの根とし、生成多項式 $G(x)$ を

$$G(x) = (x - \alpha^0)(x - \alpha^1)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)(x - \alpha^5)$$

とする。

(1) 受信語 $\mathbf{y} = (y_0, y_1, y_2, \dots, y_{14})$ の多項式表現された受信語 $Y(x)$ を

$$Y(x) = y_0 + y_1x + y_2x^2 + \dots + y_{14}x^{14}$$

で表すとき、シンδροーム $S_i = Y(\alpha^i)$ ($i = 0, 1, 2, 3, 4, 5$) を求めなさい。

解答例 多項式表現された受信語 $Y(x)$ は

$$Y(x) = \alpha^4 + \alpha^7x + x^2 + \alpha^{11}x^5 + \alpha x^6 + \alpha^{12}x^7$$

であるから、シンδροーム $S_i = Y(\alpha^i)$ ($i = 0, 1, 2, 3, 4, 5$) を計算すると

$$\left\{ \begin{array}{l} S_0 = Y(\alpha^0) = \alpha^4 + \alpha^7(\alpha^0) + (\alpha^0)^2 + \alpha^{11}(\alpha^0)^5 + \alpha(\alpha^0)^6 + \alpha^{12}(\alpha^0)^7 = \alpha^9 \\ S_1 = Y(\alpha^1) = \alpha^4 + \alpha^7(\alpha^1) + (\alpha^1)^2 + \alpha^{11}(\alpha^1)^5 + \alpha(\alpha^1)^6 + \alpha^{12}(\alpha^1)^7 = \alpha^3 \\ S_2 = Y(\alpha^2) = \alpha^4 + \alpha^7(\alpha^2) + (\alpha^2)^2 + \alpha^{11}(\alpha^2)^5 + \alpha(\alpha^2)^6 + \alpha^{12}(\alpha^2)^7 = \alpha^8 \\ S_3 = Y(\alpha^3) = \alpha^4 + \alpha^7(\alpha^3) + (\alpha^3)^2 + \alpha^{11}(\alpha^3)^5 + \alpha(\alpha^3)^6 + \alpha^{12}(\alpha^3)^7 = \alpha^{13} \\ S_4 = Y(\alpha^4) = \alpha^4 + \alpha^7(\alpha^4) + (\alpha^4)^2 + \alpha^{11}(\alpha^4)^5 + \alpha(\alpha^4)^6 + \alpha^{12}(\alpha^4)^7 = \alpha^9 \\ S_5 = Y(\alpha^5) = \alpha^4 + \alpha^7(\alpha^5) + (\alpha^5)^2 + \alpha^{11}(\alpha^5)^5 + \alpha(\alpha^5)^6 + \alpha^{12}(\alpha^5)^7 = \alpha^0 = 1 \end{array} \right.$$

となる。

(2) 3 個の誤り位置を k_1, k_2, k_3 とし、それぞれの誤りの値 (大きさ) を $a_{k_1}, a_{k_2}, a_{k_3}$ とするとき、シンδροーム S_i ($i = 0, 1, 2, 3, 4, 5$) は

$$S_i = a_{k_1}(\alpha^i)^{k_1} + a_{k_2}(\alpha^i)^{k_2} + a_{k_3}(\alpha^i)^{k_3}$$

と表すことができる。また、誤り位置多項式 $\sigma(x)$ を

$$\sigma(x) = (x - \alpha^{k_1})(x - \alpha^{k_2})(x - \alpha^{k_3}) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3$$

と定義する。このとき、 $S_2\sigma_1, S_3\sigma_1, S_4\sigma_1$ それぞれを $S_0, S_1, S_2, S_3, S_4, S_5$ および $\sigma_1, \sigma_2, \sigma_3$ で表しなさい。

解答例 誤り位置多項式 $\sigma(x)$ の解と係数の関係より、

$$\begin{cases} \sigma_1 = -(\alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3}) = \alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3} \\ \sigma_2 = \alpha^{k_1}\alpha^{k_2} + \alpha^{k_2}\alpha^{k_3} + \alpha^{k_3}\alpha^{k_1} \\ \sigma_3 = -\alpha^{k_1}\alpha^{k_2}\alpha^{k_3} = \alpha^{k_1}\alpha^{k_2}\alpha^{k_3} \end{cases}$$

となる。また、

$$S_i = a_{k_1}(\alpha^i)^{k_1} + a_{k_2}(\alpha^i)^{k_2} + a_{k_3}(\alpha^i)^{k_3} = a_{k_1}(\alpha^{k_1})^i + a_{k_2}(\alpha^{k_2})^i + a_{k_3}(\alpha^{k_3})^i$$

に注意すれば、シンδροーム S_i ($i = 0, 1, 2, 3, 4, 5$) は

$$\begin{cases} S_0 = a_{k_1}(\alpha^{k_1})^0 + a_{k_2}(\alpha^{k_2})^0 + a_{k_3}(\alpha^{k_3})^0 = a_{k_1} + a_{k_2} + a_{k_3} \quad \cdots \textcircled{1} \\ S_1 = a_{k_1}(\alpha^{k_1})^1 + a_{k_2}(\alpha^{k_2})^1 + a_{k_3}(\alpha^{k_3})^1 \quad \cdots \textcircled{2} \\ S_2 = a_{k_1}(\alpha^{k_1})^2 + a_{k_2}(\alpha^{k_2})^2 + a_{k_3}(\alpha^{k_3})^2 \quad \cdots \textcircled{3} \\ S_3 = a_{k_1}(\alpha^{k_1})^3 + a_{k_2}(\alpha^{k_2})^3 + a_{k_3}(\alpha^{k_3})^3 \\ S_4 = a_{k_1}(\alpha^{k_1})^4 + a_{k_2}(\alpha^{k_2})^4 + a_{k_3}(\alpha^{k_3})^4 \\ S_5 = a_{k_1}(\alpha^{k_1})^5 + a_{k_2}(\alpha^{k_2})^5 + a_{k_3}(\alpha^{k_3})^5 \end{cases}$$

となる。上記の関係を用いて $S_2\sigma_1, S_3\sigma_1, S_4\sigma_1$ を計算すると、それぞれ

$$\begin{aligned} S_2\sigma_1 &= (a_{k_1}(\alpha^{k_1})^2 + a_{k_2}(\alpha^{k_2})^2 + a_{k_3}(\alpha^{k_3})^2)(\alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3}) \\ &= a_{k_1}(\alpha^{k_1})^3 + a_{k_2}(\alpha^{k_2})^3 + a_{k_3}(\alpha^{k_3})^3 \\ &\quad + (a_{k_1}\alpha^{k_1} + a_{k_2}\alpha^{k_2} + a_{k_3}\alpha^{k_3})(\alpha^{k_1}\alpha^{k_2} + \alpha^{k_2}\alpha^{k_3} + \alpha^{k_3}\alpha^{k_1}) \\ &\quad - (a_{k_1} + a_{k_2} + a_{k_3})(\alpha^{k_1}\alpha^{k_2}\alpha^{k_3}) \\ &= S_3 + S_1\sigma_2 - S_0\sigma_3 = \underline{S_3 + S_1\sigma_2 + S_0\sigma_3}, \\ S_3\sigma_1 &= (a_{k_1}(\alpha^{k_1})^3 + a_{k_2}(\alpha^{k_2})^3 + a_{k_3}(\alpha^{k_3})^3)(\alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3}) \\ &= a_{k_1}(\alpha^{k_1})^4 + a_{k_2}(\alpha^{k_2})^4 + a_{k_3}(\alpha^{k_3})^4 \\ &\quad + (a_{k_1}(\alpha^{k_1})^2 + a_{k_2}(\alpha^{k_2})^2 + a_{k_3}(\alpha^{k_3})^2)(\alpha^{k_1}\alpha^{k_2} + \alpha^{k_2}\alpha^{k_3} + \alpha^{k_3}\alpha^{k_1}) \\ &\quad - (a_{k_1}\alpha^{k_1} + a_{k_2}\alpha^{k_2} + a_{k_3}\alpha^{k_3})(\alpha^{k_1}\alpha^{k_2}\alpha^{k_3}) \\ &= S_4 + S_2\sigma_2 - S_1\sigma_3 = \underline{S_4 + S_2\sigma_2 + S_1\sigma_3}, \\ S_4\sigma_1 &= (a_{k_1}(\alpha^{k_1})^4 + a_{k_2}(\alpha^{k_2})^4 + a_{k_3}(\alpha^{k_3})^4)(\alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3}) \\ &= a_{k_1}(\alpha^{k_1})^5 + a_{k_2}(\alpha^{k_2})^5 + a_{k_3}(\alpha^{k_3})^5 \\ &\quad + (a_{k_1}(\alpha^{k_1})^3 + a_{k_2}(\alpha^{k_2})^3 + a_{k_3}(\alpha^{k_3})^3)(\alpha^{k_1}\alpha^{k_2} + \alpha^{k_2}\alpha^{k_3} + \alpha^{k_3}\alpha^{k_1}) \\ &\quad - (a_{k_1}(\alpha^{k_1})^2 + a_{k_2}(\alpha^{k_2})^2 + a_{k_3}(\alpha^{k_3})^2)(\alpha^{k_1}\alpha^{k_2}\alpha^{k_3}) \\ &= S_5 + S_3\sigma_2 - S_2\sigma_3 = \underline{S_5 + S_3\sigma_2 + S_2\sigma_3} \end{aligned}$$

となる。

(3) (1), (2) を利用して誤り位置 k_1, k_2, k_3 ($k_1 < k_2 < k_3$) を求めなさい。ただし、誤り位置の個数が 3 個以下の場合は、 k の添え字の小さい順に誤り位置を割り当てなさい。

解答例 (2) で求めた関係式

$$\begin{cases} S_2\sigma_1 = S_3 + S_1\sigma_2 + S_0\sigma_3 \\ S_3\sigma_1 = S_4 + S_2\sigma_2 + S_1\sigma_3 \\ S_4\sigma_1 = S_5 + S_3\sigma_2 + S_2\sigma_3 \end{cases}$$

に、(1) で求めたシンδροーム S_i ($i = 0, 1, 2, 3, 4, 5$) を代入すると、 $\sigma_1, \sigma_2, \sigma_3$ を変数とする連立 1 次方程式

$$\begin{cases} \alpha^8\sigma_1 = \alpha^{13} + \alpha^3\sigma_2 + \alpha^9\sigma_3 & \cdots \text{④} \\ \alpha^{13}\sigma_1 = \alpha^9 + \alpha^8\sigma_2 + \alpha^3\sigma_3 & \cdots \text{⑤} \\ \alpha^9\sigma_1 = \alpha^0 + \alpha^{13}\sigma_2 + \alpha^8\sigma_3 & \cdots \text{⑥} \end{cases}$$

を得る。ここで、上記の連立 1 次方程式から σ_1 を消すと、 σ_2, σ_3 を変数とする連立 1 次方程式

$$\begin{cases} 0 = \alpha + \sigma_3 & \cdots \text{⑦} & (\because \alpha^5 \times \text{④} - \text{⑤}) \\ 0 = \alpha^{14} + \sigma_2 + \alpha^{10}\sigma_3 & \cdots \text{⑧} & (\because \text{⑤} - \alpha^4 \times \text{⑥}) \end{cases}$$

となり、式⑦と式⑧から直ちに $\sigma_3 = \alpha$ および $\sigma_2 = \alpha^{14} + \alpha^{11} = \alpha^{10}$ を得る。さらに、式④に $\sigma_3 = \alpha$ および $\sigma_2 = \alpha^{10}$ を代入すると

$$\begin{aligned} \alpha^8\sigma_1 &= \alpha^{13} + \alpha^{13} + \alpha^{10} = \alpha^{10} \\ \iff \sigma_1 &= \alpha^{10}\alpha^{-8} = \alpha^2 \end{aligned}$$

を得る。以上より、誤り位置多項式 $\sigma(x)$ は

$$\sigma(x) = x^3 + \alpha^2x^2 + \alpha^{10}x + \alpha$$

となる。したがって、誤り位置多項式 $\sigma(x)$ の解は、

$$\begin{aligned} \sigma(\alpha^0) &= (\alpha^0)^3 + \alpha^2(\alpha^0)^2 + \alpha^{10}(\alpha^0) + \alpha = 0, & \leftarrow \\ \sigma(\alpha^1) &= (\alpha^1)^3 + \alpha^2(\alpha^1)^2 + \alpha^{10}(\alpha^1) + \alpha = \alpha^{10}, \\ \sigma(\alpha^2) &= (\alpha^2)^3 + \alpha^2(\alpha^2)^2 + \alpha^{10}(\alpha^2) + \alpha = \alpha^{13}, \\ \sigma(\alpha^3) &= (\alpha^3)^3 + \alpha^2(\alpha^3)^2 + \alpha^{10}(\alpha^3) + \alpha = 0, & \leftarrow \\ \sigma(\alpha^4) &= (\alpha^4)^3 + \alpha^2(\alpha^4)^2 + \alpha^{10}(\alpha^4) + \alpha = \alpha^4, \\ \sigma(\alpha^5) &= (\alpha^5)^3 + \alpha^2(\alpha^5)^2 + \alpha^{10}(\alpha^5) + \alpha = \alpha^{13}, \\ \sigma(\alpha^6) &= (\alpha^6)^3 + \alpha^2(\alpha^6)^2 + \alpha^{10}(\alpha^6) + \alpha = 1, \\ \sigma(\alpha^7) &= (\alpha^7)^3 + \alpha^2(\alpha^7)^2 + \alpha^{10}(\alpha^7) + \alpha = \alpha^3, \\ \sigma(\alpha^8) &= (\alpha^8)^3 + \alpha^2(\alpha^8)^2 + \alpha^{10}(\alpha^8) + \alpha = \alpha^3, \\ \sigma(\alpha^9) &= (\alpha^9)^3 + \alpha^2(\alpha^9)^2 + \alpha^{10}(\alpha^9) + \alpha = \alpha^3, \\ \sigma(\alpha^{10}) &= (\alpha^{10})^3 + \alpha^2(\alpha^{10})^2 + \alpha^{10}(\alpha^{10}) + \alpha = \alpha^{11}, \\ \sigma(\alpha^{11}) &= (\alpha^{11})^3 + \alpha^2(\alpha^{11})^2 + \alpha^{10}(\alpha^{11}) + \alpha = \alpha^6, \\ \sigma(\alpha^{12}) &= (\alpha^{12})^3 + \alpha^2(\alpha^{12})^2 + \alpha^{10}(\alpha^{12}) + \alpha = \alpha^7, \\ \sigma(\alpha^{13}) &= (\alpha^{13})^3 + \alpha^2(\alpha^{13})^2 + \alpha^{10}(\alpha^{13}) + \alpha = 0, & \leftarrow \\ \sigma(\alpha^{14}) &= (\alpha^{14})^3 + \alpha^2(\alpha^{14})^2 + \alpha^{10}(\alpha^{14}) + \alpha = \alpha^5 \end{aligned}$$

より、 $\alpha^0, \alpha^3, \alpha^{13}$ となる。ゆえに、誤り位置 k_1, k_2, k_3 は、それぞれ $k_1 = 0, k_2 = 3, k_3 = 13$ である。

(4) (1), (2), (3) の結果を用いて、誤り位置 k_1, k_2, k_3 における誤りの値 $a_{k_1}, a_{k_2}, a_{k_3}$ を求めるために必要な連立 1 次方程式を求めなさい。さらに、この連立 1 次方程式を解き、 $a_{k_1}, a_{k_2}, a_{k_3}$ を求めなさい。ヒント：誤りの値は $\alpha, \alpha^{10}, \alpha^{12}$ のいずれかである。

解答例 (2) の式①, 式②, 式③に、(1) で求めたシンジローム $S_0 = \alpha^9, S_1 = \alpha^3, S_2 = \alpha^8$ と (3) で求めた $k_1 = 0, k_2 = 3, k_3 = 13$ を代入すると、誤りの値 $a_{k_1}, a_{k_2}, a_{k_3}$ を求めるために必要な連立 1 次方程式

$$\begin{cases} \alpha^9 = a_0(\alpha^0)^0 + a_3(\alpha^3)^0 + a_{13}(\alpha^{13})^0 = a_1 + a_3 + a_{13} \\ \alpha^3 = a_0(\alpha^0)^1 + a_3(\alpha^3)^1 + a_{13}(\alpha^{13})^1 = a_1 + a_3\alpha^3 + a_{13}\alpha^{13} \\ \alpha^8 = a_0(\alpha^0)^2 + a_3(\alpha^3)^2 + a_{13}(\alpha^{13})^2 = a_1 + a_3\alpha^6 + a_{13}\alpha^{11} \end{cases}$$

が求まる (注意： $\alpha^{26} = \alpha^{15}\alpha^{11} = 1\alpha^{11} = \alpha^{11}$)。

$$\begin{array}{c} \vdots \\ \vdots \\ \vdots \\ \text{計算省略} \quad ((3) \text{ の前半部分と同様に上記の連立 1 次方程式を解く}) \\ \vdots \\ \vdots \\ \vdots \end{array}$$

したがって、誤り位置 $k_1 = 0, k_2 = 3, k_3 = 13$ における誤りの値 $a_{k_1}, a_{k_2}, a_{k_3}$ は、それぞれ $a_0 = \alpha, a_3 = \alpha^{10}, a_{13} = \alpha^{12}$ である。

(5) (3), (4) の結果を用いて、誤りパターン $\mathbf{e} = (e_0, e_1, e_2, \dots, e_{14})$ を求め、受信語 $\mathbf{y}$ の誤りを訂正し、推定情報 $\hat{\mathbf{i}}$ を求めなさい。

解答例 (3), (4) より、誤りパターン $\mathbf{e}$ は

$$\mathbf{e} = (\alpha, 0, 0, \alpha^{10}, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha^{12}, 0)$$

である。したがって、受信語 $\mathbf{y}$ の誤りを訂正すると

$$\begin{aligned} \mathbf{y} - \mathbf{e} = \mathbf{y} + \mathbf{e} &= (\alpha^4, \alpha^7, 1, 0, 0, \alpha^{11}, \alpha, \alpha^{12}, 0, 0, 0, 0, 0, 0, 0) \\ &\quad + (\alpha, 0, 0, \alpha^{10}, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha^{12}, 0) \\ &= (\alpha^4 + \alpha, \alpha^7, 1, 0 + \alpha^{10}, 0, \alpha^{11}, \alpha, \alpha^{12}, 0, 0, 0, 0, 0 + \alpha^{12}, 0) \\ &= (1, \alpha^7, 1, \alpha^{10}, 0, \alpha^{11}, \underline{\alpha}, \underline{\alpha^{12}}, \underline{0}, \underline{0}, \underline{0}, \underline{0}, \underline{0}, \underline{\alpha^{12}}, \underline{0}) \end{aligned}$$

となり、推定情報 $\hat{\mathbf{i}}$ は

$$\hat{\mathbf{i}} = (\alpha, \alpha^{12}, 0, 0, 0, 0, 0, \alpha^{12}, 0)$$

となる。