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、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

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

の誤りの検出と訂正を行い、推定情報 \( i \) を求めなさい (\( q = 2^4, m = 1, t = 3 \)。ただし、\( \alpha \) を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 \( y = (y_0, y_1, y_2, \cdots, y_{14}) \)の多項式表現された受信語 \( Y(x) \) を

\[ Y(x) = y_0 + y_1x + y_2x^2 + \cdots + y_{14}x^{14} \]

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

解答例 多項式表現された受信語 \( Y(x) \) は

\[ Y(x) = \alpha^4 + \alpha^7x + x^2 + \alpha^{11}x^5 + \alpha^6x^9 + \alpha^{12}x^7 \]

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

\[
\begin{align*}
S_0 &= Y(\alpha^0) = \alpha^4 + \alpha^7(\alpha^0) + (\alpha^0)^2 + \alpha^{11}(\alpha^0)^5 + \alpha(\alpha^0)^6 + \alpha^{12}(\alpha^0)^7 = \alpha^9 \\
S_1 &= Y(\alpha^1) = \alpha^4 + \alpha^7(\alpha^1) + (\alpha^1)^2 + \alpha^{11}(\alpha^1)^5 + \alpha(\alpha^1)^6 + \alpha^{12}(\alpha^1)^7 = \alpha^3 \\
S_2 &= Y(\alpha^2) = \alpha^4 + \alpha^7(\alpha^2) + (\alpha^2)^2 + \alpha^{11}(\alpha^2)^5 + \alpha(\alpha^2)^6 + \alpha^{12}(\alpha^2)^7 = \alpha^8 \\
S_3 &= Y(\alpha^3) = \alpha^4 + \alpha^7(\alpha^3) + (\alpha^3)^2 + \alpha^{11}(\alpha^3)^5 + \alpha(\alpha^3)^6 + \alpha^{12}(\alpha^3)^7 = \alpha^{13} \\
S_4 &= Y(\alpha^4) = \alpha^4 + \alpha^7(\alpha^4) + (\alpha^4)^2 + \alpha^{11}(\alpha^4)^5 + \alpha(\alpha^4)^6 + \alpha^{12}(\alpha^4)^7 = \alpha^9 \\
S_5 &= Y(\alpha^5) = \alpha^4 + \alpha^7(\alpha^5) + (\alpha^5)^2 + \alpha^{11}(\alpha^5)^5 + \alpha(\alpha^5)^6 + \alpha^{12}(\alpha^5)^7 = \alpha^0 = 1
\end{align*}
\]

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、シンドローム \( S_i \) \( (i = 0, 1, 2, 3, 4, 5) \) 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、

\[
\begin{align*}
\sigma_1 &= -(a_{k_1} + a_{k_2} + a_{k_3}) = \alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3} \\
\sigma_2 &= a_{k_1}\alpha^{k_2} + a_{k_2}\alpha^{k_3} + a_{k_3}\alpha^{k_1} \\
\sigma_3 &= -a_{k_1}\alpha^{k_2}\alpha^{k_3} = \alpha^{k_1}\alpha^{k_2}\alpha^{k_3}
\end{align*}
\]

となる。また、

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

に注意すれば、シンドローム \( S_i \) \( (i = 0, 1, 2, 3, 4, 5) \) は

\[
\begin{align*}
S_0 &= a_{k_1}(\alpha^0)^{k_1} + a_{k_2}(\alpha^0)^{k_2} + a_{k_3}(\alpha^0)^{k_3} = a_{k_1} + a_{k_2} + a_{k_3} \cdots (1) \\
S_1 &= a_{k_1}(\alpha^1)^{k_1} + a_{k_2}(\alpha^1)^{k_2} + a_{k_3}(\alpha^1)^{k_3} \cdots (2) \\
S_2 &= a_{k_1}(\alpha^2)^{k_1} + a_{k_2}(\alpha^2)^{k_2} + a_{k_3}(\alpha^2)^{k_3} \cdots (3) \\
S_3 &= a_{k_1}(\alpha^3)^{k_1} + a_{k_2}(\alpha^3)^{k_2} + a_{k_3}(\alpha^3)^{k_3} \\
S_4 &= a_{k_1}(\alpha^4)^{k_1} + a_{k_2}(\alpha^4)^{k_2} + a_{k_3}(\alpha^4)^{k_3} \\
S_5 &= a_{k_1}(\alpha^5)^{k_1} + a_{k_2}(\alpha^5)^{k_2} + a_{k_3}(\alpha^5)^{k_3}
\end{align*}
\]

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

\[
S_2\sigma_1 = (a_{k_1}(\alpha^1)^{k_1} + a_{k_2}(\alpha^1)^{k_2} + a_{k_3}(\alpha^1)^{k_3})(\alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3})
\]

\[
= a_{k_1}(\alpha^1)^{k_1} + a_{k_2}(\alpha^1)^{k_2} + a_{k_3}(\alpha^1)^{k_3} + a_{k_4}(\alpha^2)^{k_4} + a_{k_5}(\alpha^3)^{k_5}
\]

\[
= S_3 + S_1\sigma_2 - S_0\sigma_3 = S_3 + S_1\sigma_2 - S_0\sigma_3,
\]

\[
S_3\sigma_1 = (a_{k_1}(\alpha^2)^{k_1} + a_{k_2}(\alpha^2)^{k_2} + a_{k_3}(\alpha^2)^{k_3})(\alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3})
\]

\[
= a_{k_1}(\alpha^2)^{k_1} + a_{k_2}(\alpha^2)^{k_2} + a_{k_3}(\alpha^2)^{k_3} + a_{k_4}(\alpha^3)^{k_4}
\]

\[
= S_4 + S_2\sigma_2 - S_1\sigma_3 = S_4 + S_2\sigma_2 - S_1\sigma_3,
\]

\[
S_4\sigma_1 = (a_{k_1}(\alpha^3)^{k_1} + a_{k_2}(\alpha^3)^{k_2} + a_{k_3}(\alpha^3)^{k_3})(\alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3})
\]

\[
= a_{k_1}(\alpha^3)^{k_1} + a_{k_2}(\alpha^3)^{k_2} + a_{k_3}(\alpha^3)^{k_3} + a_{k_4}(\alpha^4)^{k_4}
\]

\[
= S_5 + S_3\sigma_2 - S_2\sigma_3 = S_5 + S_3\sigma_2 - S_2\sigma_3.
\]

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 個以下の場合には、\(k\) 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

\[
\begin{align*}
S_2\sigma_1 &= S_3 + S_1\sigma_2 + S_0\sigma_3 \\
S_3\sigma_1 &= S_4 + S_2\sigma_2 + S_1\sigma_3 \\
S_4\sigma_1 &= S_5 + S_3\sigma_2 + S_2\sigma_3
\end{align*}
\]

に、(1) で求めたシンドローム \(S_i\) \((i = 0, 1, 2, 3, 4, 5)\) 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

\[
\begin{align*}
\alpha^8\sigma_1 &= \alpha^{13} + \alpha^3\sigma_2 + \alpha^9\sigma_3 \quad \cdots \text{(4)} \\
\alpha^{13}\sigma_1 &= \alpha^9 + \alpha^8\sigma_2 + \alpha^3\sigma_3 \quad \cdots \text{(5)} \\
\alpha^9\sigma_1 &= \alpha^0 + \alpha^{13}\sigma_2 + \alpha^8\sigma_3 \quad \cdots \text{(6)}
\end{align*}
\]

を得る。ここで、上記の連立 1 次方程式から \(\sigma_1\) を消すと、\(\sigma_2, \sigma_3\) を変数とする連立 1 次方程式

\[
\begin{align*}
0 &= \alpha + \sigma_3 \quad \cdots \text{(7)} \quad (\because \alpha^5 \times \text{(4)} - \text{(5)}) \\
0 &= \alpha^{14} + \sigma_2 + \alpha^8\sigma_3 \quad \cdots \text{(8)} \quad (\because \text{(5)} - \alpha^4 \times \text{(6)})
\end{align*}
\]

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

\[
\begin{align*}
\alpha^8\sigma_1 &= \alpha^{13} + \alpha^{13} + \alpha^{10} = \alpha^{10} \\
\iff \quad &\sigma_1 = \alpha^{10}\alpha^{-8} = \alpha^2
\end{align*}
\]

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、

\[
\begin{align*}
\sigma(a^0) &= (a^0)^3 + \alpha^2(a^0)^2 + \alpha^{10}(a^0) + \alpha = 0, \quad \leftarrow \\
\sigma(a^1) &= (a^1)^3 + \alpha^2(a^1)^2 + \alpha^{10}(a^1) + \alpha = \alpha^{10}, \\
\sigma(a^2) &= (a^2)^3 + \alpha^2(a^2)^2 + \alpha^{10}(a^2) + \alpha = \alpha^{13}, \\
\sigma(a^3) &= (a^3)^3 + \alpha^2(a^3)^2 + \alpha^{10}(a^3) + \alpha = 0, \quad \leftarrow \\
\sigma(a^4) &= (a^4)^3 + \alpha^2(a^4)^2 + \alpha^{10}(a^4) + \alpha = a^4, \\
\sigma(a^5) &= (a^5)^3 + \alpha^2(a^5)^2 + \alpha^{10}(a^5) + \alpha = a^{13}, \\
\sigma(a^6) &= (a^6)^3 + \alpha^2(a^6)^2 + \alpha^{10}(a^6) + \alpha = 1, \\
\sigma(a^7) &= (a^7)^3 + \alpha^2(a^7)^2 + \alpha^{10}(a^7) + \alpha = a^3, \\
\sigma(a^8) &= (a^8)^3 + \alpha^2(a^8)^2 + \alpha^{10}(a^8) + \alpha = a^3, \\
\sigma(a^9) &= (a^9)^3 + \alpha^2(a^9)^2 + \alpha^{10}(a^9) + \alpha = a^3, \\
\sigma(a^{10}) &= (a^{10})^3 + \alpha^2(a^{10})^2 + \alpha^{10}(a^{10}) + \alpha = a^{11}, \\
\sigma(a^{11}) &= (a^{11})^3 + \alpha^2(a^{11})^2 + \alpha^{10}(a^{11}) + \alpha = a^6, \\
\sigma(a^{12}) &= (a^{12})^3 + \alpha^2(a^{12})^2 + \alpha^{10}(a^{12}) + \alpha = a^7, \\
\sigma(a^{13}) &= (a^{13})^3 + \alpha^2(a^{13})^2 + \alpha^{10}(a^{13}) + \alpha = 0, \quad \leftarrow \\
\sigma(a^{14}) &= (a^{14})^3 + \alpha^2(a^{14})^2 + \alpha^{10}(a^{14}) + \alpha = a^5
\end{align*}
\]

より、\(a^0, a^3, a^{13}\) 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。
解答例 (2) 式①, 式②, 式③に、(1) で求めたシンドローム \( S_0 = \alpha^9, S_1 = \alpha^3, S_2 = \alpha^8 \) 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
\[
\begin{align*}
\alpha^9 &= a_0(\alpha^0)^9 + a_3(\alpha^3)^9 + a_{13}(\alpha^{13})^9 = a_1 + a_3 + a_{13} \\
\alpha^3 &= a_0(\alpha^0)^3 + a_3(\alpha^3)^3 + a_{13}(\alpha^{13})^3 = a_1 + a_3 + a_{13} \\
\alpha^8 &= a_0(\alpha^0)^8 + a_3(\alpha^3)^8 + a_{13}(\alpha^{13})^8 = a_1 + a_3 + a_{13}
\end{align*}
\]
が求まる (注意: \( \alpha^{26} = \alpha^{15} \alpha^{11} = 1 \alpha^{11} = \alpha^{11} \))。

\[
\begin{align*}
\vdots \\
\vdots \\
\vdots \\
\end{align*}
\]
計算省略 ((3) の前半部分と同様に上記の連立 1 次方程式を解く)
\[
\begin{align*}
\vdots \\
\vdots \\
\vdots \\
\end{align*}
\]

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 \( e = (e_1, e_2, \cdots, e_{14}) \) を求め、受信語 \( y \) の誤りを訂正し、推定情報 \( \hat{i} \) を求めなさい。

解答例 (3), (4) より、誤りパターン \( e \) は
\[
e = (\alpha, 0, 0, \alpha^{10}, 0, 0, 0, 0, 0, 0, 0, 0, \alpha^{12}, 0)
\]
である。したがって、受信語 \( y \) の誤りを訂正すると
\[
\begin{align*}
y - e &= y + e = (\alpha^4, \alpha^7, 1, 0, 0, 0, \alpha^{11}, \alpha, \alpha^{12}, 0, 0, 0, 0, 0, 0, 0, 0) \\
&= (\alpha^4 + \alpha^7, 1, 0, 0, 0, \alpha^{11}, \alpha, \alpha^{12}, 0, 0, 0, 0, 0, 0, 0, 0, 0)
\end{align*}
\]
となり、推定情報 \( \hat{i} \) は
\[
\hat{i} = (\alpha, \alpha^{12}, 0, 0, 0, 0, 0, \alpha^{12}, 0)
\]
となる。