RS 符号における誤り検出と誤り訂正の具体例　例として、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

$$\boldsymbol{y} = (\alpha^5, \alpha^3, \alpha^2, 1, 1, \alpha, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

の誤りの検出と訂正を行ない、推定情報 $\hat{\boldsymbol{i}}$ を求めてみましょう ($q = 2^4$, $m = 1$, $t = 3$)。

【注意】この RS 符号は 3 個の誤りが訂正可能であることから、生成多項式 $G(x)$ は、$\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ を根に持ち、

$$\begin{aligned} G(x) &= (x-\alpha^0)(x-\alpha^1)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5) \\ &= 1 + \alpha^4 x + \alpha^2 x^2 + \alpha x^3 + \alpha^{12} x^4 + \alpha^9 x^5 + x^6 \end{aligned}$$

となります。ただし、α は GF(2^4) の原始多項式 $x^4 + x + 1$ $(= 0)$ の 1 つの根とします。このとき、多項式表現された情報

$$\begin{aligned} &I(x) = i_0 + i_1 x + i_2 x^2 + i_3 x^3 + i_4 x^4 + i_5 x^5 + i_6 x^6 + i_7 x^7 + i_8 x^8 \\ &\left(\Longleftrightarrow \ \boldsymbol{i} = (i_0, i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8) \right) \end{aligned}$$

に対する多項式表現された符号語

$$\begin{aligned} X(x) = {} & x_0 + x_1 x + x_2 x^2 + x_3 x^3 + x_4 x^4 + x_5 x^5 + x_6 x^6 + x_7 x^7 \\ & + x_8 x^8 + x_9 x^9 + x_{10} x^{10} + x_{11} x^{11} + x_{12} x^{12} + x_{13} x^{13} + x_{14} x^{14} \end{aligned}$$

$$\left(\Longleftrightarrow \ \boldsymbol{x} = (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}) \right)$$

は、多項式 $I(x)\, x^6$ を生成多項式 $G(x)$ で割った剰余多項式

$$\begin{aligned} R(x) &= [I(x)\, x^6] \bmod G(x) \\ &= r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 + r_5 x^5 \end{aligned}$$

を用いて、

$$\begin{aligned} X(x) &= I(x)\, x^6 - R(x) = I(x)\, x^6 + R(x) \\ &= r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 + r_5 x^5 \\ &\quad + (i_0 + i_1 x + i_2 x^2 + i_3 x^3 + i_4 x^4 + i_5 x^5 + i_6 x^6 + i_7 x^7 + i_8 x^8)\, x^6 \\ &= r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 + r_5 x^5 \\ &\quad + i_0 x^6 + i_1 x^7 + i_2 x^8 + i_3 x^9 + i_4 x^{10} + i_5 x^{11} + i_6 x^{12} + i_7 x^{13} + i_8 x^{14} \end{aligned}$$

で与えられます。すなわち、符号語 $\boldsymbol{x}$ は

$$\boldsymbol{x} = (r_0, r_1, r_2, r_3, r_4, r_5, i_0, i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8)$$

という構造を持ちます。

まず、受信語 $\boldsymbol{y} = (y_0, y_1, y_2, \cdots, y_{14})$ に誤りが含まれていないかを調べるために、シンドロームを計算しましょう。 $[15, 9]$RS 符号の多項式表現された受信語

$$\begin{aligned} Y(x) &= y_0 + y_1 x + y_2 x^2 + \cdots + y_{14} x^{14} \\ &= \alpha^5 + \alpha^3 x + \alpha^2 x^2 + x^3 + x^4 + \alpha x^5 \end{aligned}$$

より、シンドローム S_i は

$$S_i = Y(\alpha^i) \qquad (i = 0, 1, 2, 3, 4, 5)$$

となります。シンドロームを具体的に計算すると

$$\begin{cases} S_0 = Y(\alpha^0) = \alpha^5 + \alpha^3(\alpha^0) + \alpha^2(\alpha^0)^2 + (\alpha^0)^3 + (\alpha^0)^4 + \alpha(\alpha^0)^5 = \alpha^3 \\ S_1 = Y(\alpha^1) = \alpha^5 + \alpha^3(\alpha^1) + \alpha^2(\alpha^1)^2 + (\alpha^1)^3 + (\alpha^1)^4 + \alpha(\alpha^1)^5 = 1 \\ S_2 = Y(\alpha^2) = \alpha^5 + \alpha^3(\alpha^2) + \alpha^2(\alpha^2)^2 + (\alpha^2)^3 + (\alpha^2)^4 + \alpha(\alpha^2)^5 = \alpha^7 \\ S_3 = Y(\alpha^3) = \alpha^5 + \alpha^3(\alpha^3) + \alpha^2(\alpha^3)^2 + (\alpha^3)^3 + (\alpha^3)^4 + \alpha(\alpha^3)^5 = \alpha^3 \\ S_4 = Y(\alpha^4) = \alpha^5 + \alpha^3(\alpha^4) + \alpha^2(\alpha^4)^2 + (\alpha^4)^3 + (\alpha^4)^4 + \alpha(\alpha^4)^5 = \alpha^7 \\ S_5 = Y(\alpha^5) = \alpha^5 + \alpha^3(\alpha^5) + \alpha^2(\alpha^5)^2 + (\alpha^5)^3 + (\alpha^5)^4 + \alpha(\alpha^5)^5 = \alpha^8 \end{cases}$$

となり、受信語 $\boldsymbol{y}$ に誤りが含まれていることを知ることができます。もちろん、全ての S_i が 0 であれば、誤りが含まれていないと判断し、誤りの訂正を行なう必要はありません。

次に、誤り位置を求めましょう。多項式表現された誤りパターン $E(x)$ を

$$E(x) = e_0 + e_1 x + e_2 x^2 + \cdots + e_{14} x^{14}$$

とし、多項式表現された受信語 $Y(x)$ が

$$Y(\alpha^i) = X(\alpha^i) + E(\alpha^i) = 0 + E(\alpha^i) = E(\alpha^i) \qquad (i = 0, 1, 2, 3, 4, 5)$$

を満たすことに注意すれば、シンドローム S_i は

$$S_i = Y(\alpha^i) = e_0 + e_1 \alpha^i + e_2 (\alpha^i)^2 + \cdots + e_{14} (\alpha^i)^{14} \qquad (i = 0, 1, 2, 3, 4, 5)$$

という構造をしていることになります。ここで、$[15, 9]$BCH 符号は 3 つの誤りが訂正可能であることから、誤り位置を k_1, k_2, k_3 とし、その誤りの値 (大きさ) を $a_{k_1}, a_{k_2}, a_{k_3}$ ($a_{k_t} = e_{k_t}$, 他は 0) と仮定すると、シンドローム S_i は改めて

$$\begin{aligned} S_i = Y(\alpha^i) &= a_{k_1} \cdot (\alpha^i)^{k_1} + a_{k_2} \cdot (\alpha^i)^{k_2} + a_{k_3} \cdot (\alpha^i)^{k_3} \\ &= a_{k_1} (\alpha^i)^{k_1} + a_{k_2} (\alpha^i)^{k_2} + a_{k_3} (\alpha^i)^{k_3} \\ &= a_{k_1} (\alpha^{k_1})^i + a_{k_2} (\alpha^{k_2})^i + a_{k_3} (\alpha^{k_3})^i \qquad \cdots ① \end{aligned}$$

と書き直すことができます。さらに、誤り位置多項式 $\sigma(x)$ を

$$\begin{aligned} \sigma(x) &= (x - \alpha^{k_1})(x - \alpha^{k_2})(x - \alpha^{k_3}) \\ &= x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 \qquad \cdots ② \end{aligned}$$

とすると、シンドローム S_i (式①) は

$$\begin{cases} S_3 = S_2 \sigma_1 - S_1 \sigma_2 + S_0 \sigma_3 \\ S_4 = S_3 \sigma_1 - S_2 \sigma_2 + S_1 \sigma_3 \qquad \cdots ③ \\ S_5 = S_4 \sigma_1 - S_3 \sigma_2 + S_2 \sigma_3 \end{cases}$$

という関係を満たします (2 を法として計算する)。したがって、式③の連立 1 次方程式を解くことで誤り位置多項式 $\sigma(x)$ の係数 $\sigma_1, \sigma_2, \sigma_3$ を求めることができます。具体的に数値を代入して連立 1 次方程式

$$\begin{cases} \alpha^3 = \alpha^7\sigma_1 + \sigma_2 + \alpha^3\sigma_3 \\ \alpha^7 = \alpha^3\sigma_1 + \alpha^7\sigma_2 + \sigma_3 \\ \alpha^8 = \alpha^7\sigma_1 + \alpha^3\sigma_2 + \alpha^7\sigma_3 \end{cases}$$

を解くと、それぞれ

$$\begin{cases} \sigma_1 = \alpha \\ \sigma_2 = \alpha^{10} \\ \sigma_3 = \alpha^6 \end{cases}$$

となります。ゆえに、誤り位置多項式 $\sigma(x)$ は

$$\sigma(x) = x^3 + \alpha x^2 + \alpha^{10}x + \alpha^6 \qquad \leftarrow \text{誤りが 3 個であることがわかる}$$

となります。さて、この誤り位置多項式 $\sigma(x)$ は $\alpha^{k_1}, \alpha^{k_2}, \alpha^{k_3}$ を解に持つことから、関係式

$$\sigma(\alpha^{k_1}) = \sigma(\alpha^{k_2}) = \sigma(\alpha^{k_3}) = 0$$

を満たします。言い換えれば、$\sigma(\alpha^i) = 0$ 満たす $\mathrm{GF}(2^4)$ の元 α^i を見つければ良いということです[1]。具体的に計算すると

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

となり、誤り位置多項式 $\sigma(x)$ の解が $\alpha^3, \alpha^4, \alpha^{14}$ であることがわかります。したがって、誤り位置が 0 から数えて 3 番目, 4 番目, 14 番目であることから、誤りパターン $\boldsymbol{e}$ は

$$\boldsymbol{e} = (0, 0, 0, a_3, a_4, 0, 0, 0, 0, 0, 0, 0, 0, 0, a_{14})$$

[1] 2 次や 3 次の多項式 (2 個や 3 個の誤りが訂正可能) であれば直接因数分解して解を求めることもできますが、誤り訂正できる個数が増えると因数分解で求めることは非常に困難です。

となります[2]。さらに、RS 符号の誤りの訂正には各誤り位置における誤りの値 (大きさ) を求める必要があります。そこで、先ほど求めた誤り位置 $(k_1 = 3, k_2 = 4, k_3 = 14)$ をシンドローム S_i (式①) に代入し、 $a_{k_1}, a_{k_2}, a_{k_3}$ を変数とする連立 1 次方程式

$$\begin{cases} S_0 = a_{k_1}(\alpha^{k_1})^0 + a_{k_2}(\alpha^{k_2})^0 + a_{k_3}(\alpha^{k_3})^0 \\ S_1 = a_{k_1}(\alpha^{k_1})^1 + a_{k_2}(\alpha^{k_2})^1 + a_{k_3}(\alpha^{k_3})^1 \\ S_2 = a_{k_1}(\alpha^{k_1})^2 + a_{k_2}(\alpha^{k_2})^2 + a_{k_3}(\alpha^{k_3})^2 \end{cases}$$

をつくります (3 変数なので 3 つの関係式だけでよい)。これを解けば誤りの値 (大きさ) $a_{k_1}, a_{k_2}, a_{k_3}$ を求めることができます。具体的に数値を代入して連立 1 次方程式

$$\begin{cases} \alpha^3 = a_3(\alpha^3)^0 + a_4(\alpha^4)^0 + a_{14}(\alpha^{14})^0 \\ 1 = a_3(\alpha^3)^1 + a_4(\alpha^4)^1 + a_{14}(\alpha^{14})^1 \\ \alpha^7 = a_3(\alpha^3)^2 + a_4(\alpha^4)^2 + a_{14}(\alpha^{14})^2 \end{cases}$$

を解くと、それぞれ

$$\begin{cases} a_3 = \alpha^6 \\ a_4 = \alpha^5 \\ a_{14} = \alpha \end{cases}$$

となります。したがって、最終的な誤りパターン $\boldsymbol{e}$ は

$$\boldsymbol{e} = (0, 0, 0, \alpha^6, \alpha^5, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha)$$

となります。

以上より、受信語 $\boldsymbol{y}$ の誤りを訂正すると

$$\begin{aligned} \boldsymbol{y} - \boldsymbol{e} = \boldsymbol{y} + \boldsymbol{e} = \quad & (\alpha^5, \alpha^3, \alpha^2, 1, 1, \alpha, 0, 0, 0, 0, 0, 0, 0, 0, 0) \\ & + (0, 0, 0, \alpha^6, \alpha^5, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha) \\ = \quad & (\alpha^5, \alpha^3, \alpha^2, 1 + \alpha^6, 1 + \alpha^5, \alpha, 0, 0, 0, 0, 0, 0, 0, 0, 0 + \alpha) \\ = \quad & (\alpha^5, \alpha^3, \alpha^2, \alpha^{13}, \alpha^{10}, \alpha, 0, 0, 0, 0, 0, 0, 0, 0, \alpha) \end{aligned}$$

となります。したがって、推定情報 $\hat{\boldsymbol{i}}$ は

$$\hat{\boldsymbol{i}} = (0, 0, 0, 0, 0, 0, 0, 0, \alpha)$$

となります (最初の注意を参照のこと)。

[2]BCH 符号の誤りの値 (大きさ) は 1 のみをとりますが、RS 符号の誤りの値 (大きさ) は GF(2^4) の元をとります。