2008 年度 情報数理　レポート 6　学生用

学籍番号：　　氏名：

下記の注意事項を守り、次ページ以降の問いに答え、レポートを完成させなさい。

提出期限：2009 年 1 月 9 日 (金) 13:00 まで
提出場所：理学部棟 正面玄関内に設置のレポートボックス

注意事項：

(1) このページを印刷し、必要事項を記入の上 (学籍番号欄と氏名欄は 2 箇所あるので忘れずに記入すること)、レポートの表紙として提出すること。

(2) ~~文章処理ソフトウェアや図形処理ソフトウェア等を駆使してレポートを作成し~~ (問→解答→問→解答→ ··· の順になるように記述すること)、A4 サイズの用紙 ~~に印刷して提出すること (手書きは不可)。~~

(3) クラスメイトのレポートを参考にしたり、クラスメイトと協力してレポートを作成した場合は、教員控の協力者氏名欄にクラスメイトの氏名を記入すること。これらの場合も、自分の言葉で表現し直すこと。**コピー禁止**。

(4) 情報数理について、あなたの声を聞かせてください (教員控の意見・質問欄に記入のこと)。気軽にどうぞ (成績には一切影響しません)。

出題者：幸山 直人
出題日：2008 年 12 月 11 日 (木)

得点：　/6

- 切り取り線 -

2008 年度 情報数理　レポート 6　教員控

学籍番号：　　氏名：

協力者氏名：　　,　　,

レポート作成に要した時間：　　.　　時間

得点：　/6

意見・質問：

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

$$\boldsymbol{y} = (\alpha^3, \alpha^7, \alpha^5, \alpha^4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

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

$$Y(x) = y_0 + y_1 x + y_2 x^2 + \cdots + y_{14} x^{14}$$

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。(1 点)

解答例　多項式表現された受信語 $Y(x)$ は

$$Y(x) = \alpha^3 + \alpha^7 x + \alpha^5 x^2 + \alpha^4 x^3$$

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

$$\begin{cases} S_0 = Y(\alpha^0) = \alpha^3 + \alpha^7(\alpha^0) + \alpha^5(\alpha^0)^2 + \alpha^4(\alpha^0)^3 = \alpha^5 \\ S_1 = Y(\alpha^1) = \alpha^3 + \alpha^7(\alpha^1) + \alpha^5(\alpha^1)^2 + \alpha^4(\alpha^1)^3 = \alpha^{13} \\ S_2 = Y(\alpha^2) = \alpha^3 + \alpha^7(\alpha^2) + \alpha^5(\alpha^2)^2 + \alpha^4(\alpha^2)^3 = \alpha^{12} \\ S_3 = Y(\alpha^3) = \alpha^3 + \alpha^7(\alpha^3) + \alpha^5(\alpha^3)^2 + \alpha^4(\alpha^3)^3 = \alpha^6 \\ S_4 = Y(\alpha^4) = \alpha^3 + \alpha^7(\alpha^4) + \alpha^5(\alpha^4)^2 + \alpha^4(\alpha^4)^3 = \alpha^{14} \\ S_5 = Y(\alpha^5) = \alpha^3 + \alpha^7(\alpha^5) + \alpha^5(\alpha^5)^2 + \alpha^4(\alpha^5)^3 = \alpha^8 \end{cases}$$

となる。

評価基準　解答例に準じた解答であれば 1 点。

(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。(1 点)

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

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

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

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

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

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

となる。

評価基準　解答例に準じた解答であれば 1 点。

(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。(2 点)

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) で求めたシンドローム S_i ($i = 0, 1, 2, 3, 4, 5$) を代入すると、σ_1, σ_2, σ_3 を変数とする連立 1 次方程式

$$\begin{cases} \alpha^{12}\sigma_1 = \alpha^6 + \alpha^{13}\sigma_2 + \alpha^5\sigma_3 & \cdots ④ \\ \alpha^6\sigma_1 = \alpha^{14} + \alpha^{12}\sigma_2 + \alpha^{13}\sigma_3 & \cdots ⑤ \\ \alpha^{14}\sigma_1 = \alpha^8 + \alpha^6\sigma_2 + \alpha^{12}\sigma_3 & \cdots ⑥ \end{cases}$$

を得る。σ_1 を消すと σ_2, σ_3 を変数とする連立 1 次方程式

$$\begin{cases} 0 = \alpha^9 + \alpha^8\sigma_2 + \alpha^8\sigma_3 & \cdots ⑦ \quad (\because ④ - \alpha^6 \times ⑤) \\ 0 = \alpha^{11} + \alpha^9\sigma_2 + \alpha^4\sigma_3 & \cdots ⑧ \quad (\because ⑥ - \alpha^8 \times ⑤) \end{cases}$$

を得る。同様に、σ_2 を消すと

$$\begin{aligned} & 0 = \alpha^{14} + \alpha^{14}\sigma_3 \quad (\because ⑧ - \alpha \times ⑦) \\ \iff & \alpha^{14} = \alpha^{14}\sigma_3 \\ \iff & \sigma_3 = \alpha^{14}\alpha^{-14} = 1 \end{aligned}$$

を得る。さらに連立方程式の解法に従えば、式⑦に $\sigma_3 = 1$ を代入すると $\sigma_2 = \alpha^4$ を得て、式④に $\sigma_3 = 1$ および $\sigma_2 = \alpha^4$ を代入すると $\sigma_1 = \alpha^{14}$ を得る。以上より、誤り位置多項式 $\sigma(x)$ は

$$\sigma(x) = x^3 + \alpha^{14}x^2 + \alpha^4 x + 1$$

となる。したがって、誤り位置多項式 $\sigma(x)$ の解は、

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

より、$\alpha^4, \alpha^5, \alpha^6$ となる。ゆえに、誤り位置 k_1, k_2, k_3 は、それぞれ $k_1 = 4$, $k_2 = 5$, $k_3 = 6$ である。

評価基準　誤り位置多項式が正しく求められていれば 1 点、さらに誤り位置が正しく求められていれば 1 点。

(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 $1, \alpha^3, \alpha^{12}$ のいずれかである。(1 点)

解答例　(2) の式①, 式②, 式③に、(1) で求めたシンドローム $S_0 = \alpha^5, S_1 = \alpha^{13}, S_2 = \alpha^{12}$ と (3) で求めた $k_1 = 4, k_2 = 5, k_3 = 6$ 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

$$\begin{cases} \alpha^5 = a_4(\alpha^4)^0 + a_5(\alpha^5)^0 + a_6(\alpha^6)^0 = a_4 + a_5 + a_6 & \cdots ⑨ \\ \alpha^{13} = a_4(\alpha^4)^1 + a_5(\alpha^5)^1 + a_6(\alpha^6)^1 = a_4\alpha^4 + a_5\alpha^5 + a_6\alpha^6 & \cdots ⑩ \\ \alpha^{12} = a_4(\alpha^4)^2 + a_5(\alpha^5)^2 + a_6(\alpha^6)^2 = a_4\alpha^8 + a_5\alpha^{10} + a_6\alpha^{12} & \cdots ⑪ \end{cases}$$

が求まる。

$\vdots$

$\vdots$

$\vdots$

計算省略　((3) の前半部分と同様に連立 1 次方程式を解く)

$\vdots$

$\vdots$

$\vdots$

したがって、誤り位置 $k_1 = 4$, $k_2 = 5$, $k_3 = 6$ における誤りの値 a_{k_1}, a_{k_2}, a_{k_3} は、それぞれ $a_4 = 1$, $a_5 = \alpha^{12}$, $a_6 = \alpha^3$ である。

評価基準　解答例に準じた解答であれば 1 点。

(5) (3), (4) の結果を用いて、誤りパターン $\boldsymbol{e} = (e_0, e_1, e_2, \cdots, e_{14})$ を求め、受信語 $\boldsymbol{y}$ の誤りを訂正し、推定情報 $\hat{\boldsymbol{i}}$ を求めなさい。(1 点)

解答例　(3), (4) より、誤りパターン $\boldsymbol{e}$ は

$$\boldsymbol{e} = (0, 0, 0, 0, 1, \alpha^{12}, \alpha^3, 0, 0, 0, 0, 0, 0, 0, 0)$$

である。したがって、受信語 $\boldsymbol{y}$ の誤りを訂正すると

$$\begin{aligned} \boldsymbol{y} - \boldsymbol{e} = \boldsymbol{y} + \boldsymbol{e} = \quad & (\alpha^3, \alpha^7, \alpha^5, \alpha^4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \\ & + (0, 0, 0, 0, 1, \alpha^{12}, \alpha^3, 0, 0, 0, 0, 0, 0, 0, 0) \\ = \quad & (\alpha^3, \alpha^7, \alpha^5, \alpha^4, 0+1, 0+\alpha^{12}, 0+\alpha^3, 0, 0, 0, 0, 0, 0, 0, 0) \\ = \quad & (\alpha^3, \alpha^7, \alpha^5, \alpha^4, 1, \alpha^{12}, \alpha^3, 0, 0, 0, 0, 0, 0, 0, 0) \end{aligned}$$

となり、推定情報 $\hat{\boldsymbol{i}}$ は

$$\hat{\boldsymbol{i}} = (\alpha^3, 0, 0, 0, 0, 0, 0, 0, 0)$$

となる。

評価基準　解答例に準じた解答であれば 1 点。