

2010年度 情報数理 期末試験 (その1)

学籍番号：

氏名：

問題 1 「情報量」について、次の (1)～(2) の問いに答えなさい。

(1) 情報量の定義として正しい数式を以下の選択肢から選び、解答欄にア～カの記号で答えなさい。ただし、情報源から発生する N 種類の通報の情報源記号を $s_1, s_2, \dots, s_N$ とし、各情報源記号の生起確率を $p(s_i)$ とする。(5 点)

解答欄：

イ

選択肢：

ア. $\sum_{i=1}^N p(s_i) \log_2 p(s_i)$

イ. $\sum_{i=1}^N p(s_i) \log_2 \frac{1}{p(s_i)}$

ウ. $\sum_{i=1}^N \frac{1}{p(s_i)} \log_2 p(s_i)$

エ. $\sum_{i=1}^N \frac{1}{p(s_i)} \log_2 \frac{1}{p(s_i)}$

オ. $-\sum_{i=1}^N p(s_i) \log_2 \frac{1}{p(s_i)}$

カ. $-\sum_{i=1}^N \frac{1}{p(s_i)} \log_2 p(s_i)$

(2) ある情報源

$$S = \left\{ \begin{array}{cccc} s_1, & s_2, & s_3, & s_4 \\ \frac{4}{10}, & \frac{4}{10}, & \frac{1}{10}, & \frac{1}{10} \end{array} \right\}$$

がある。この情報源 S の情報量を四捨五入により小数点以下第 2 位まで求め、その値を解答欄に記入しなさい。なお、必要があれば $\log_2 10 = 3.32192 \dots$ を利用しなさい。(5 点)

解答例

$$\begin{aligned} H(S) &= \sum_{i=1}^4 p(s_i) \log_2 \frac{1}{p(s_i)} \\ &= \frac{4}{10} \log_2 \frac{10}{4} + \frac{4}{10} \log_2 \frac{10}{4} + \frac{1}{10} \log_2 \frac{10}{1} + \frac{1}{10} \log_2 \frac{10}{1} \\ &= 2 \frac{4}{10} (\log_2 10 - 2) + 2 \frac{1}{10} \log_2 10 \\ &= \log_2 10 - \frac{16}{10} \\ &\doteq 3.321 - 1.600 = 1.721 \end{aligned}$$

解答欄：

1.72

/10

2010 年度 情報数理 期末試験 (その 2)

学籍番号：

氏名：

問題 2 α をガロア拡大体 $\text{GF}(2^4)$ の原始多項式 $x^4 + x + 1 (= 0)$ の 1 つの根 (原始元) とするとき、次の (1)～(5) の問いに答え、 $\text{GF}(2)$ 上の 3 個の誤りが訂正可能な $[15, 5]$ BCH 符号の受信語

$$\mathbf{y} = (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$$

の誤りの検出および訂正を行ない、推定情報 $\hat{\mathbf{i}}$ を求めなさい ($m = 4, t = 3$)。

(1) $[15, 5]$ BCH 符号の生成多項式 $G(x)$ を求めなさい (展開しなくてもよい)。(10 点)

解答例 3 個の誤りが訂正可能であるから、生成多項式 $G(x)$ は $\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根に持つ。さらに、 $\text{GF}(2)$ 上の多項式の性質 (α^i を根に持てば α^{2i} も根となること) より、根 α^i ($i = 1, 3, 5$) に対する根が、それぞれ

$$\begin{aligned} \alpha^{1 \cdot 2^0} &= \alpha, & \alpha^{1 \cdot 2^1} &= \alpha^2, & \alpha^{1 \cdot 2^2} &= \alpha^4, & \alpha^{1 \cdot 2^3} &= \alpha^8 & (\alpha^1 \text{ に対して}), \\ \alpha^{3 \cdot 2^0} &= \alpha^3, & \alpha^{3 \cdot 2^1} &= \alpha^6, & \alpha^{3 \cdot 2^2} &= \alpha^{12}, & \alpha^{3 \cdot 2^3} &= \alpha^9 & (\alpha^3 \text{ に対して}), \\ \alpha^{5 \cdot 2^0} &= \alpha^5, & \alpha^{5 \cdot 2^1} &= \alpha^{10} & & & & & (\alpha^5 \text{ に対して}) \end{aligned}$$

となるから、最小多項式 $M_i(x)$ は、それぞれ

$$\begin{aligned} M_1(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8), \\ M_3(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}), \\ M_5(x) &= (x - \alpha^5)(x - \alpha^{10}) \end{aligned}$$

となる。よって、最小多項式 $M_i(x)$ の最小公倍多項式によって得られる生成多項式 $G(x)$ は

$$\begin{aligned} G(x) &= \text{LCM}[M_1(x), M_3(x), M_5(x)] \\ &= (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)(x - \alpha^5)(x - \alpha^6)(x - \alpha^8)(x - \alpha^9)(x - \alpha^{10})(x - \alpha^{12}) \\ &= (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4)(x + \alpha^5)(x + \alpha^6)(x + \alpha^8)(x + \alpha^9)(x + \alpha^{10})(x + \alpha^{12}) \end{aligned}$$

となる (係数は 2 を法とするのでプラスで表してもマイナスで表しても、どちらでもよい)。

【参考】 上記の生成多項式 $G(x)$ は 10 次の多項式であり、関係式 $\alpha^4 + \alpha + 1 = 0$ と $\alpha^{15} = 1$ 用いて展開すると、

$$G(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$$

となる (テキストの p.61 参照)。言い換えれば、検査記号数は 10 である。したがって、符号長 15 ($= 2^m - 1$) の内、検査記号数は 10 で、情報記号数は 5 ($= 15 - 10$) となる (i.e. $[15, 5]$ BCH 符号)。

2010年度 情報数理 期末試験 (その3)

学籍番号：

氏名：

(2) 3個の誤り位置を k_1, k_2, k_3 と仮定すると、シンδροーム S_i ($i = 1, 2, 3, 4, 5, 6$) は

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

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、変数 $\sigma_1, \sigma_2, \sigma_3$ を求めるために必要な連立1次方程式を導きなさい。(10点)

解答例 仮定より、 $(\alpha^i)^k = (\alpha^k)^i$ が成り立つことに注意すれば、シンδροーム S_i は

$$\begin{cases} S_1 = (\alpha^{k_1})^1 + (\alpha^{k_2})^1 + (\alpha^{k_3})^1 \\ S_2 = (\alpha^{k_1})^2 + (\alpha^{k_2})^2 + (\alpha^{k_3})^2 = S_1^2 \\ S_3 = (\alpha^{k_1})^3 + (\alpha^{k_2})^3 + (\alpha^{k_3})^3 \\ S_4 = (\alpha^{k_1})^4 + (\alpha^{k_2})^4 + (\alpha^{k_3})^4 = S_2^2 \\ S_5 = (\alpha^{k_1})^5 + (\alpha^{k_2})^5 + (\alpha^{k_3})^5 \\ S_6 = (\alpha^{k_1})^6 + (\alpha^{k_2})^6 + (\alpha^{k_3})^6 = S_3^2 \end{cases}$$

となる。また、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。以上の関係式を用いると、

$$S_1 = \alpha^{k_1} + \alpha^{k_2} + \alpha^{k_3} = \sigma_1,$$

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

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

が成り立つ。したがって、変数 $\sigma_1, \sigma_2, \sigma_3$ を求めるために必要な連立1次方程式は

$$\begin{cases} S_1 + \sigma_1 = 0 \\ S_3 + S_2\sigma_1 + S_1\sigma_2 + \sigma_3 = 0 \\ S_5 + S_4\sigma_1 + S_3\sigma_2 + S_2\sigma_3 = 0 \end{cases}$$

となる。【注意】上記の計算は、全て2を法として計算したものである。

2010年度 情報数理 期末試験 (その4)

学籍番号：

氏名：

(3) 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 $S_i = Y(\alpha^i)$ ($i = 1, 2, 3, 4, 5, 6$) を求めなさい。ヒント：シンδροーム S_i は $0, \alpha^5, \alpha^{10}$ のいずれかである。(5点)

解答例 多項式表現された受信語 $Y(x)$ は

$$Y(x) = x^2 + x^4 + x^6 + x^7 + x^{10}$$

であるから、シンδροーム $S_i = Y(\alpha^i)$ ($i = 1, 2, 3, 4, 5, 6$) を計算すると

$$\begin{cases} S_1 = Y(\alpha^1) = (\alpha^1)^2 + (\alpha^1)^4 + (\alpha^1)^6 + (\alpha^1)^7 + (\alpha^1)^{10} = \alpha^{10} \\ S_2 = Y(\alpha^2) = S_1^2 = \alpha^5 \\ S_3 = Y(\alpha^3) = (\alpha^3)^2 + (\alpha^3)^4 + (\alpha^3)^6 + (\alpha^3)^7 + (\alpha^3)^{10} = \alpha^5 \\ S_4 = Y(\alpha^4) = S_2^2 = \alpha^{10} \\ S_5 = Y(\alpha^5) = (\alpha^5)^2 + (\alpha^5)^4 + (\alpha^5)^6 + (\alpha^5)^7 + (\alpha^5)^{10} = 0 \\ S_6 = Y(\alpha^6) = S_3^2 = \alpha^{10} \end{cases}$$

となる。

(4) (2), (3) を利用して、誤り位置多項式 $\sigma(x)$ を求めなさい。ヒント：係数 $\sigma_1, \sigma_2, \sigma_3$ は $0, 1, \alpha^{10}$ のいずれかである。(5点)

解答例 まず、直ちに $\sigma_1 = S_1 = \alpha^{10}$ が求まる。次に、 $\sigma_1 = \alpha^{10}$ を残りの2式に代入すると

$$\begin{cases} \alpha^{10} + \alpha^{10}\sigma_2 + \sigma_3 = 0 & \dots \textcircled{1} \\ \alpha^5 + \alpha^5\sigma_2 + \alpha^5\sigma_3 = 0 & \dots \textcircled{2} \end{cases}$$

となる。続いて、 $\textcircled{1} \times \alpha^5 - \textcircled{2}$ を計算すると $(\alpha^5 + 1)\sigma_2 = \alpha^5 + 1$ となり、 $\sigma_2 = 1$ が求まる。最後に、 $\sigma_2 = 1$ を $\textcircled{1}$ 式に代入すると $\alpha^{10} + \alpha^{10} + \sigma_3 = 0$ となるので、これを解くと $\sigma_3 = 0$ が求まる。以上より、求める誤り位置多項式 $\sigma(x)$ は

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

である(2ヶ所に誤りがあることがわかる)。

2010 年度 情報数理 期末試験 (その 5)

学籍番号：

氏名：

(5) (4) を利用して誤り位置を特定し、受信語 $\mathbf{y}$ の誤りを訂正し、推定情報 $\hat{\mathbf{i}} = (i_0, i_1, i_2, i_3, i_4)$ を求めなさい。(10 点)

解答例 まず、誤り位置を特定するために誤り位置多項式 $\sigma(x)$ の解を求める。0 以外の $\text{GF}(2^4)$ の元 α^i ($i = 0, 1, 2, \dots, 14$) を誤り位置多項式 $\sigma(x)$ に代入すると

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

となるから、解は α^3 および α^{12} となる。すなわち、誤り位置は 0 から数えて 3 番目および 12 番目である。したがって、誤りパターン $\mathbf{e}$ は

$$\mathbf{e} = (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$$

となるから、受信語 $\mathbf{y}$ の誤りを訂正すると

$$\begin{aligned}\mathbf{y} - \mathbf{e} = \mathbf{y} + \mathbf{e} &= (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \\ &\quad + (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \\ &= (0, 0, 1, \underline{1}, 1, 0, 1, 1, 0, 0, 1, 0, \underline{1}, 0)\end{aligned}$$

となる。以上より、符号語の生成方法を考慮すると、推定情報 $\hat{\mathbf{i}}$ は

$$\hat{\mathbf{i}} = (1, 0, 1, 0, 0)$$

となる。

【参考】 BCH 符号に用いられる記号は、 $\text{GF}(2)$ の元 (0 または 1) なので誤りの大きさは常に 1 である。したがって、RS 符号のように誤りの大きさを求める必要はない。

べき表現	展開	ベクトル表現
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001