2007 年度 情報数理 期末試験 (その 1)

学籍番号：＿＿＿＿＿＿＿＿＿＿　　氏名：＿＿＿＿＿＿＿＿＿＿

問題 1 以下の文章は「情報」に関して述べたものである。空欄に当てはまる適切な語句を選択肢から選び、ア〜シの記号で答えなさい。(各 2 点)

(1) 1948 年、クロード E. シャノンによって発表された画期的な論文「A Mathematical Theory of Communication (通信に関する 1 つの数学的理論)」では、情報を確率的概念として捉え、情報を定量化するために [サ] の定義を導いた。

(2) 役立つ符号とは、「一意に復号が可能であること」と「瞬時に復号が可能であること」が必要かつ十分な条件となる。役立つ符号に対する符号の木を描くと、各符号語は [カ] に位置する。

(3) ある情報源において、情報源記号とその生起確率が与えられたとき、平均符号長が最小となる符号をその情報源に対する [イ] と呼ぶ。この符号は、Huffman の符号化法によって構成することができる。

(4) ある情報源に対して、繰り返し Huffman の符号化法を適用すると、平均符号長はある値に収束する。これをシャノンの [オ] と呼ぶ。

(5) 情報量は、平均符号長の [ケ] によって定義される。情報量の単位はビットである。

選択肢：

ア. 中間節点	イ. コンパクト符号	ウ. 上限	エ. Kraft の不等式
オ. 情報源符号化定理	カ. 終端節点	キ. 冗長度	ク. 等長符号
ケ. 下限	コ. 特異な符号	サ. 情報量	シ. プレフィックス

/10

2007 年度 情報数理 期末試験 (その 2)

学籍番号：＿＿＿＿＿＿＿＿＿＿＿＿　　氏名：＿＿＿＿＿＿＿＿＿＿＿＿

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

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

の誤りの検出および訂正を行ない、推定情報 $\hat{\boldsymbol{i}}$ 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、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

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

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

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

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)。

/10

2007 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、シンドローム 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、シンドローム 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。

/10

2007年度 情報数理 期末試験 (その4)

学籍番号：

氏名：

(3)　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 $S_i = Y(\alpha^i)$ $(i = 1, 2, 3, 4, 5, 6)$ を求めなさい。ヒント：シンドローム S_i は $1, \alpha^7, \alpha^{11}, \alpha^{14}$ 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

$$Y(x) = x^2 + x^3 + x^5 + x^7 + x^8 + x^9$$

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

$$\begin{cases} S_1 = Y(\alpha^1) = (\alpha^1)^2 + (\alpha^1)^3 + (\alpha^1)^5 + (\alpha^1)^7 + (\alpha^1)^8 + (\alpha^1)^9 = \alpha^{11} \\ S_2 = Y(\alpha^2) = S_1^2 = \alpha^7 \\ S_3 = Y(\alpha^3) = (\alpha^3)^2 + (\alpha^3)^3 + (\alpha^3)^5 + (\alpha^3)^7 + (\alpha^3)^8 + (\alpha^3)^9 = \alpha^{11} \\ S_4 = Y(\alpha^4) = S_2^2 = \alpha^{14} \\ S_5 = Y(\alpha^5) = (\alpha^5)^2 + (\alpha^5)^3 + (\alpha^5)^5 + (\alpha^5)^7 + (\alpha^5)^8 + (\alpha^5)^9 = 1 \\ S_6 = Y(\alpha^6) = S_3^2 = \alpha^7 \end{cases}$$

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 $0, \alpha^9, \alpha^{11}$ のいずれかである。(5点)

解答例　まず、直ちに $\sigma_1 = S_1 = \alpha^{11}$ が求まる。次に、$\sigma_1 = \alpha^{11}$ を残りの2式に代入すると

$$\begin{cases} \alpha^5 + \alpha^{11}\sigma_2 + \sigma_3 = 0 \\ \alpha^5 + \alpha^{11}\sigma_2 + \alpha^7\sigma_3 = 0 \end{cases}$$

となる。続いて、2式の両辺をそれぞれ加えると $(1 + \alpha^7)\sigma_3 = 0$ となり、$\sigma_3 = 0$ が求まる。最後に、$\sigma_3 = 0$ を上記の2式の上の式に代入すると $\alpha^5 + \alpha^{11}\sigma_2 + 0 = 0$ となるので、これを解くと $\sigma_2 = \alpha^5\alpha^{-11} = \alpha^{-6} = 1 \cdot \alpha^{-6} = \alpha^{15}\alpha^{-6} = \alpha^9$ が求まる。以上より、求める誤り位置多項式 $\sigma(x)$ は

$$\sigma(x) = x^3 + \alpha^{11}x^2 + \alpha^9 x$$

である。

/10

2007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 $\boldsymbol{y}$ の誤りを訂正し、推定情報 $\hat{\boldsymbol{i}} = (i_0, i_1, i_2, i_3, i_4)$ 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 $\mathrm{GF}(2^4)$ の元 α^i $(i = 0, 1, 2, \cdots, 14)$ を誤り位置多項式 $\sigma(x)$ を代入すると

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

となるから、解は α^{10} と α^{14} となる。すなわち、誤り位置は 10 と 14 である。したがって、誤りパターン $\boldsymbol{e}$ は

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

となるから、受信語 $\boldsymbol{y}$ の誤りを訂正すると

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

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 $\hat{\boldsymbol{i}}$ は

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

となる。

【参考】BCH 符号に用いられる記号は、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。

/10