令和６年度弁理士試験論文式筆記試験問題

［情報理論］

１　下記の検査行列$\boldsymbol{H}$で規定される(7,4)ハミング符号について、情報記号を$\boldsymbol{u} = (u_1, u_2, u_3, u_4)$、検査記号を$\boldsymbol{c} = (c_1, c_2, c_3)$とし、符号語を$\boldsymbol{w} = (u_1, u_2, u_3, u_4, c_1, c_2, c_3)$という組織符号の形で表すとする。以下の問いに答えよ。

$$\boldsymbol{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

【４０点】

(1) $\boldsymbol{w}\boldsymbol{H}^T = \boldsymbol{0}$を満たすことを利用して、検査記号$c_1, c_2, c_3$を情報記号$u_1, u_2, u_3, u_4$で表せ。なお、$\boldsymbol{H}^T$は$\boldsymbol{H}$の転置行列である。

(2) 情報記号$\boldsymbol{u}$から符号語$\boldsymbol{w}$を生成する生成行列$\boldsymbol{G}$を示せ。

(3) 受信語$\boldsymbol{y} = (1,0,1,1,1,0,1)$から元の情報記号を復号せよ。なお、受信語$\boldsymbol{y}$に含まれる誤りは高々１つとする。

(4) 誤り率$p = 0.1$の２元対称通信路を用いて符号語$\boldsymbol{w}$を送信したとき、受信語から元の情報記号$\boldsymbol{u}$を正しく復号できる確率を、有効桁数３桁で示せ。なお、計算過程も示すこと。

2　記号 a, b, c をそれぞれ確率 2/4, 1/4, 1/4 で発生する独立生起情報源がある。この独立生起情報源から、長さ K の記号系列を発生させた場合について、以下の問いに答えよ。

【４０点】

(1) 長さが K（任意の長さ）の場合に発生する記号系列の平均情報量を示せ。

(2) 長さが $K = 2$ の場合に発生する記号系列 aa, ab, ac, ba, bb, bc, ca, cb, cc それぞれの発生確率を示せ。

(3) 長さが $K = 2$ の場合に発生する記号系列を、４元符号{0, 1, 2, 3}により下記のように符号化した。

aa → 1
ab → 23
ac → 22
ba → 21
bb → 03
bc → 02
ca → 20
cb → 01
cc → 00

この符号化方法は、最短符号を生成するものとなっているかを理由とともに説明せよ。

(4) 長さが $K = 2$ の場合に発生する記号系列を４元符号により最短符号化した場合の平均符号長を示せ。導出の過程も示すこと。

3　情報理論に関する以下の用語について、その内容を説明せよ。

【２０点】

(1) RSA 暗号

(2) ナイキスト間隔

(3) HTTP Cookie

(4) ワンタイムパスワード

(5) エントロピー符号