9.5　次の2元対称通信路 T に対して，以下の問いに答えなさい．

$$\boldsymbol{T}=\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

（1）　p を何と呼ぶか，答えなさい．

（2）　通報 $\boldsymbol{x}_1=101010$ を送信し，$\boldsymbol{y}_1=100110$ を受信した場合，$\boldsymbol{x}_1$ と $\boldsymbol{y}_1$ のハミング距離 $h(\boldsymbol{x}_1,\boldsymbol{y}_1)$ を求めなさい．

（3）　（2）の場合の $P(\boldsymbol{y}_1|\boldsymbol{x}_1)$ を求めなさい．

（4）　一般に長さ n の通報 $\boldsymbol{x}$ を送信し，$\boldsymbol{y}$ が受信されるとき，その間のハミング距離が $h(\boldsymbol{x},\boldsymbol{y})=\alpha$ の場合，$P(\boldsymbol{y}|\boldsymbol{x})$ はどのように表されるかを答えなさい．

（1）pは送信における誤り確率（p.84参照）

（2）ハミング距離＝異なるビットの数

$$\boldsymbol{x}_1 = 101010, \boldsymbol{y}_1 = 100110, h(\boldsymbol{x}_1, \boldsymbol{y}_1) = 2$$

（3）＜送信誤り無し＞$x_1(i) = 1 \rightarrow y_1(i) = 1, x_1(i) = 0 \rightarrow y_1(i) = 0$となる確率は$1 - p$,

＜送信誤り有り＞$x_1(i) = 1 \rightarrow y_1(i) = 0, x_1(i) = 0 \rightarrow y_1(i) = 1$となる確率は$p$である.

送信誤り無しが4ビット，送信誤り有りが2ビット

$\boldsymbol{x}_1$を送信したとき，$\boldsymbol{y}_1$が受信される確率$P(\boldsymbol{y}_1|\boldsymbol{x}_1)$:

$$P(\boldsymbol{y}_1|\boldsymbol{x}_1) = (1-p)^4 p^2$$

（4）ハミング距離（$h(\boldsymbol{x}, \boldsymbol{y}) = \alpha$）＝送信誤りのビット数

通報$\boldsymbol{x}$の長さn－ハミング距離（α）＝送信誤りのないビット数

$$P(\boldsymbol{y}|\boldsymbol{x}) = (1-p)^{n-\alpha} p^{\alpha}$$

10.5　情報ビットと検査ビットの線形関係を規定する次のような情報・検査ビット関連行列 $\boldsymbol{P}$ に対して，以下の問いに答えなさい．

$$\boldsymbol{P}=\begin{bmatrix}1 & 0\\ 0 & 1\\ 1 & 1\end{bmatrix}$$

（1）　これは，(n,k) 線形符号である．n と k を答えなさい．

（2）　生成行列 $\boldsymbol{G}$ を求めなさい．

（3）　情報ビット 00,01,10,11 に対する符号語 $\boldsymbol{u}_1,\boldsymbol{u}_2,\boldsymbol{u}_3,\boldsymbol{u}_4$ を求めなさい．

（4） 線形符号の符号語の線形結合（符号語を加え合わせたもの）によりできた符号語は，また線形符号の符号語となるが，（3）で求めた符号語 $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4$ を用いて，それを示しなさい．

（5） 検査行列 $\boldsymbol{H}$ を求めなさい．

（6） 1箇所のみ誤りがある場合のシンドローム $\boldsymbol{s}$ をすべて求めなさい．また，誤り箇所とシンドローム $\boldsymbol{s}$ の間には，どのような関係があるかを示しなさい．

（7） （6）で求めたシンドローム $\boldsymbol{s}$ を0,1の記号列として見た場合，可能性として現れてもよい他の記号列が存在する．それを示しなさい．また，そのシンドローム $\boldsymbol{s}$ は，何を意味するかを答えなさい．

(1) (n,k)線形符号：符号（n bit）＝情報（k bit）＋検査（$n-k$ bit）

$$\boldsymbol{u}=(\boldsymbol{x}^T,\boldsymbol{p}^T)=(\underbrace{x_1,\cdots,x_k}_{\text{情報ビット}},\ \underbrace{p_1,\cdots,p_{n-k}}_{\text{検査ビット}})$$

$$\boldsymbol{p}=\boldsymbol{P}\boldsymbol{x}$$

$$\boldsymbol{P}=\begin{bmatrix} p_{11} & \cdot & \cdot & \cdot & p_{1k} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{n-k1} & \cdot & \cdot & \cdot & p_{n-kk} \end{bmatrix}$$

$$\forall i,\ \ell \quad p_{i\ell}\in\{0,1\}$$

$P=3\times 2$行列であるから，$n-k=3, k=2 \rightarrow n=5, k=2$

（2）GとPの関係

$$G=[I_k, P^T] \qquad G=[I_2, P^T]=\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

（3） $p=Px$ $u=(x^T, p^T)=(\underbrace{x_1, \cdots, x_k}_{\text{情報ビット}}, \underbrace{p_1, \cdots, p_{n-k}}_{\text{検査ビット}})$

または $u=x^TG$

x^T として，00, 01, 10, 11 を代入

$u_1=(0\ 0\ 0\ 0\ 0)$ $u_3=(1\ 0\ 1\ 0\ 1)$

$u_2=(0\ 1\ 0\ 1\ 1)$ $u_4=(1\ 1\ 1\ 1\ 0)$

（4）u_k+u_lがu_1～u_4のいずれかになることを示す．
または，$u_k+u_l=x_k^TG+x_l^TG=(x_k+x_l)^TG$
であるから，x_k+x_lがx_1～x_4のいずれかになることを示す．
（参考）10．6の問題

（5）

$$\boldsymbol{H}=[\boldsymbol{P},\boldsymbol{I}_{n-k}] \qquad \boldsymbol{H}=[\boldsymbol{P},\boldsymbol{I}_3]=\begin{bmatrix}1&0&1&0&0\\0&1&0&1&0\\1&1&0&0&1\end{bmatrix}$$

（6）

i 番目に誤りがある誤りベクトル $\boldsymbol{e}_i(i=1,\cdots,5)$ と，誤りがない場合 $\boldsymbol{e}_0=(0\ 0\ 0\ 0\ 0)$ に対するシンドローム $\boldsymbol{s}_i(i=0,\cdots,5)$ を求める．

$$\begin{bmatrix}\boldsymbol{s}_0\\\boldsymbol{s}_1\\\boldsymbol{s}_2\\\boldsymbol{s}_3\\\boldsymbol{s}_4\\\boldsymbol{s}_5\end{bmatrix}=\begin{bmatrix}\boldsymbol{e}_0\\\boldsymbol{e}_1\\\boldsymbol{e}_2\\\boldsymbol{e}_3\\\boldsymbol{e}_4\\\boldsymbol{e}_5\end{bmatrix}\boldsymbol{H}^T=\begin{bmatrix}0&0&0&0&0\\1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}1&0&1\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}=\begin{bmatrix}0&0&0\\1&0&1\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

以上より，誤りが i 番目の場合は，シンドローム $\boldsymbol{s}_i$ は，検査行列 $\boldsymbol{H}$ の i 列となる．

（7）

・シンドローム$\boldsymbol{s}$は検査ビット$\boldsymbol{p}$と同じ3ビット$(n-k)=3$

・シンドローム$\boldsymbol{s}$は000～111の８通りを表現できる.

・符号語の長さは5ビット$(n=5)$

・誤差ベクトル：（誤り無し），（１箇所の誤り：５通り）＝６通り

　　→６通りのシンドロームが（６）で計算された.

・８－６＝２通りのパターンが残っている

　　→$\boldsymbol{s}_6=110, \boldsymbol{s}_7=111$→何を意味するか？

・$\boldsymbol{s}_6=\boldsymbol{s}_1+\boldsymbol{s}_2, \boldsymbol{s}_7=\boldsymbol{s}_2+\boldsymbol{s}_3$であるから，

　$\boldsymbol{e}_1+\boldsymbol{e}_2=(11000), \boldsymbol{e}_2+\boldsymbol{e}_3=(01100)$に対応する

　しかし，$\boldsymbol{s}_6=\boldsymbol{s}_3+\boldsymbol{s}_4, \boldsymbol{s}_7=\boldsymbol{s}_1+\boldsymbol{s}_4$とも表せるので，２個の誤りを検出・訂正できない.

10.6

線形符号Cの符号語$\boldsymbol{u}$と$\boldsymbol{v}$の和もまた，線形符号Cの符号語となることを示せ．

$$\boldsymbol{u} \in C \quad \Leftrightarrow \quad \boldsymbol{u}\boldsymbol{H}^T = \boldsymbol{0}$$

$$\boldsymbol{v} \in C \quad \Leftrightarrow \quad \boldsymbol{v}\boldsymbol{H}^T = \boldsymbol{0}$$

ここで，符号語 $\boldsymbol{u}+\boldsymbol{v}$ を考える．

$$(\boldsymbol{u}+\boldsymbol{v})\boldsymbol{H}^T = \boldsymbol{u}\boldsymbol{H}^T + \boldsymbol{v}\boldsymbol{H}^T = \boldsymbol{0}$$

$$\therefore \quad \boldsymbol{u}+\boldsymbol{v} \in C$$

第11章　巡回符号

巡回符号:　線形符号の一種

符号語に対応する符号多項式を定義

線形符号の生成行列　　生成多項式
　　検査行列　　検査多項式

11.1 巡回符号とは

符号長が n の2元線形符号 C を考える.

$$\forall \boldsymbol{a} = (a_0, a_1, \cdots, a_{n-2}, a_{n-1}) \in C$$

$$a_k \in \{0, 1\} \quad (k = 0, \cdots, n-1)$$

$$\boldsymbol{a}^{(1)} = (a_{n-1}, a_0, \cdots, a_{n-3}, a_{n-2})$$

これをまた置換すると,

$$\boldsymbol{a}^{(2)} = (a_{n-2}, a_{n-1}, a_0, \cdots, a_{n-3})$$

$$\vdots$$

$\forall \boldsymbol{a} \in C$ に対して, $\forall k \ \boldsymbol{a}^{(k)} \in C \quad \Rightarrow \quad C$: 巡回符号

11.2 符号多項式

符号語 $\boldsymbol{a}=(a_0, a_1, \cdots, a_{n-2}, a_{n-1})$ に対する**符号多項式**を次のように定義する.

$$F(x)=a_0+a_1x+\cdots+a_{n-2}x^{n-2}+a_{n-1}x^{n-1}$$

$$(\deg F(x)\leq n-1)$$

$\deg F(x)$ は，$F(x)$ の**次数**

$a_{n-1}\neq 0$ ならば $\deg F(x)=n-1$

$x\in\{0,1\}$　　$\bmod 2$ の演算

$$
\begin{aligned}
\boldsymbol{a} &\Rightarrow F(x) = a_0 + a_1 x + \cdots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1} \\
\boldsymbol{a}^{(1)} &\Rightarrow F^{(1)}(x) = a_{n-1} + a_0 x + \cdots + a_{n-3} x^{n-2} + a_{n-2} x^{n-1} \\
\boldsymbol{a}^{(2)} &\Rightarrow F^{(2)}(x) = a_{n-2} + a_{n-1} x + \cdots + a_{n-4} x^{n-2} + a_{n-3} x^{n-1} \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots
\end{aligned}
$$

生成多項式$G(x)$

符号Cの全ての符号語に対する符号多項式$F^{(i)}(x)$の中で次数が最小な符号多項式

11.3 符号多項式の性質

$$F(x) = a_0 + a_1 x + \cdots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1}$$

$$\begin{aligned} xF(x) &= a_{n-1}(x^n - 1) + a_{n-1} + a_0 x + \cdots + a_{n-3} x^{n-2} + a_{n-2} x^{n-1} \\ &= a_{n-1}(x^n - 1) + F^{(1)}(x) \end{aligned}$$

$xF(x)$を$(x^n - 1)$で割ったならば，商がa_{n-1}で余り（剰余）が$F^{(1)}(x)$である.

$$xF(x) \bmod (x^n - 1) = F^{(1)}(x)$$

$$A(x) \bmod B(x) = \{A(x) \text{を} B(x) \text{で割った剰余多項式}\}$$

式（11.10）にもう一度xをかけると，

$$x^2F(x)=(a_{n-1}x+a_{n-2})(x^n-1)+F^{(2)}(x)$$

$$\therefore x^2F(x)\bmod(x^n-1)=F^{(2)}(x)$$

これを繰り返すと，

$$x^iF(x)\bmod(x^n-1)=F^{(i)}(x)$$

これは，

$$\forall i \quad x^iF(x)\bmod(x^n-1)=F^{(i)}(x)=\{\text{符号多項式}\}$$

が成り立つことを示している．

$i = 1, 2, \cdots, N$までの1次結合を考え，かつ，線形符号語の1次結合はまた線形符号であることから，

$$\sum_{i=1}^{N} c_i [x^i F(x)] \bmod (x^n - 1) = \sum_{i=1}^{N} c_i F^{(i)}(x)$$

$$\left[\left\{ \sum_{i=1}^{N} c_i x^i \right\} F(x) \right] \bmod (x^n - 1) = \sum_{i=1}^{N} c_i F^{(i)}(x)$$

$$= \{\text{符号多項式}\}$$

$$\sum_{i=1}^{N} c_i x^i = C(x)$$

とおくと，任意の多項式 $C(x)$ に対して，

$$C(x) F(x) \bmod (x^n - 1) = \{\text{符号多項式}\}$$

【性質 11.1】

符号多項式 $F(x)$ $(\deg F(x) \leq n-1)$ に対して，

$$\forall C(x) \quad C(x)F(x) \bmod (x^n-1) = \{\text{符号多項式}\} \tag{11.23}$$

が成り立つ．ここで，$\deg C(x)F(x) \leq n-1$ のときは，$C(x)F(x)$ 自身が剰余多項式となり，符号多項式である．

【性質 11.2】

任意の符号多項式 $F(x)$ $(\deg F(x) \leq n-1)$ に対して，

$$F(x) \bmod G(x) = 0$$

すなわち，すべての符号多項式は，生成多項式 $G(x)$ で割り切れる．

【性質 11.3】

多項式 $F(x)(\deg F(x) \leq n-1)$ がある.

$F(x)$ が符号多項式であることの必要十分条件は，以下のように表されることである.

$$F(x) = C(x)G(x) \tag{11.30}$$

ここで

$$\begin{aligned} &C(x)：多項式 \\ &G(x)：生成多項式 \end{aligned} \tag{11.31}$$

演習問題（1）

次の2元対称通信路に対して以下の問いに答えよ.

$$\boldsymbol{T} = \begin{bmatrix} 0.8 & 0.2 \\ 0.2 & 0.8 \end{bmatrix}$$

（1）$\boldsymbol{x} = (10101011)$を送信して，$\boldsymbol{y} = (10011010)$を受信したとする．ハミング距離$h(\boldsymbol{x}, \boldsymbol{y})$を求めよ.

（2）$P(y|x)$を求めよ．但し，解答はべき乗のままでよい.

演習問題(2)

情報・検査ビット関連行列が次のように与えられている.
以下の問いに答えよ.

$$\boldsymbol{P} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

(1)生成行列$\boldsymbol{G}$を求めよ.

(2)情報ビット00, 01, 10, 11に対する符号語$\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{u}_4$
を求めよ.

(3)検査行列$\boldsymbol{H}$を求めよ.

(4)次の関係が成り立つことを示せ.

$$\boldsymbol{H}\boldsymbol{u}_k^T = \boldsymbol{0}, k = 1 \sim 4$$

(5)受信記号$y = (10101)$が正しいか否か判定せよ.
誤っている場合は, 誤りが1箇所であるとして訂正せよ.

演習問題(3)

巡回符号に関して，以下の問いに答えよ.

(1) 2元線形符号Cの1つの符号語が$\boldsymbol{a} = (1001)$であるとき，その巡回置換してできる符号語$\boldsymbol{a}^{(k)}, k = 1\sim3$を求めよ.

(2) 上記の$\boldsymbol{a}$と$\boldsymbol{a}^{(k)}$に対する符号多項式$F(x)$を求めよ.

(3) 生成多項式を求めよ.
$F(x)$の中で次数が最小の多項式