# 第10章　線形符号

生成行列（G）　：符号生成に関連

検査行列（H）　：誤り検出・訂正に関連

シンドローム（s）：誤り検出・訂正に関連

# 10.1　組織符号

**組織符号**：
情報部分と検査部分が明確に分離できる符号

符号＝情報部分（情報ビット）＋検査部分（検査ビット）

$$(u_1, u_2, \cdots, u_n) = (x_1, x_2, \cdots, x_k, p_1, p_2, \cdots, p_{n-k})$$

**$(n, k)$符号**：　符号長が$n$で情報部分が$k$[bit]の組織符号

# 10.2　2元$(n, k)$線形符号

全ての変数やパラメータは0，1で表現

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

$$\boldsymbol{u} = (u_1, \cdots, u_n)$$

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_k \end{pmatrix}, \quad \boldsymbol{p} = \begin{pmatrix} p_1 \\ \cdot \\ \cdot \\ \cdot \\ p_{n-k} \end{pmatrix}$$

$$u_i \in \{0, 1\} \quad (i = 1, \cdots, n)$$

$$x_i \in \{0, 1\} \quad (i = 1, \cdots, k)$$

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

# 10.3　生成行列G

通信路符号化（誤り検出・訂正符号化）

（情報ビット）→（ルール）→（検査ビットを構成）

検査ビット＝情報ビットの線形変換（線形符号）

$\boldsymbol{p} = \boldsymbol{P}\boldsymbol{x}$　　$\boldsymbol{P}$ を情報・検査ビット関連行列

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

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

# 性質10.1

情報ビット $\boldsymbol{x}$ が与えられれば，次のように符号 $\boldsymbol{u}$ が求まる．

$$\boldsymbol{u} = \boldsymbol{x}^T \boldsymbol{G}$$

ここで，

$$\boldsymbol{G} = [\boldsymbol{I}_k, \boldsymbol{P}^T] = \begin{bmatrix} 1 & & & p_{11} & \cdots & p_{n-k1} \\ & \ddots & 0 & \vdots & & \vdots \\ & 0 & \ddots & \vdots & & \vdots \\ & & 1 & p_{1k} & \cdots & p_{n-kk} \end{bmatrix}$$

$\boldsymbol{I}_k$ は，$k \times k$ 単位行列である．

（証明）

式（10.3）に式（10.7）の両辺を転置して代入すると，

$$\boldsymbol{u} = (\boldsymbol{x}^T, \boldsymbol{p}^T) = (\boldsymbol{x}^T, \boldsymbol{x}^T \boldsymbol{P}^T) = \boldsymbol{x}^T \underbrace{[\boldsymbol{I}_k, \boldsymbol{P}^T]}_{\boldsymbol{G}} = \boldsymbol{x}^T \boldsymbol{G}$$

# 例10．1

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

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}}_{\boldsymbol{I}_4} \underbrace{\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}}_{\boldsymbol{P}^T}$$

# 10.4 検査行列H

【性質 10.2】

符号 $\boldsymbol{u}$ にかけると $\mathbf{0}$ となる次のような行列 $\boldsymbol{H}$ が存在する.

$$\boldsymbol{H}\boldsymbol{u}^T=\mathbf{0} \quad \text{または} \quad \boldsymbol{u}\boldsymbol{H}^T=\mathbf{0}$$

こで,

$$\boldsymbol{H}=[\boldsymbol{P},\boldsymbol{I}_{n-k}]=\begin{bmatrix} p_{11} & \cdots & p_{1k} & 1 & & \\ \vdots & \cdots & \vdots & & \ddots & \\ & & & & & 0 \\ \vdots & \cdots & \vdots & & \ddots & \\ & & & 0 & & \ddots \\ p_{n-k1} & \cdots & p_{n-kk} & & & 1 \end{bmatrix}$$

(証明)

式 (10.7) より,

$$\boldsymbol{P}\boldsymbol{x}+\boldsymbol{p}=\mathbf{0}$$

$$\begin{bmatrix} p_{11} & \cdot & \cdot & \cdot & p_{1k} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{n-k1} & \cdot & \cdot & \cdot & p_{n-kk} \end{bmatrix} \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_k \end{pmatrix} + \begin{pmatrix} p_1 \\ \cdot \\ \cdot \\ \cdot \\ p_{n-k} \end{pmatrix} = \begin{pmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

$$\begin{aligned} &p_{11}x_1 + \cdots + p_{1k}x_k + p_1 = 0 \\ &\qquad \vdots \qquad\qquad\quad \ddots \\ &p_{n-k1}x_1 + \cdots + p_{n-kk}x_k + p_{n-k} = 0 \end{aligned}$$

$$\underbrace{\begin{bmatrix} p_{11} & \cdot & \cdot & \cdot & p_{1k} & 1 & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \\ p_{n-k1} & \cdot & \cdot & \cdot & p_{n-kk} & & & 1 \end{bmatrix}}_{\boldsymbol{H}} \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_k \\ p_1 \\ \vdots \\ p_{n-k} \end{pmatrix}}_{\boldsymbol{u}^T} = \underbrace{\begin{pmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}}_{\mathbf{0}}$$

# 例10.2

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

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \underbrace{\begin{matrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{matrix}}_{\boldsymbol{P}} & \underbrace{\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}}_{\boldsymbol{I}_4} \end{bmatrix}$$

# 性質10.3

$\boldsymbol{u}$が線形符号$C$の符号語である必要十分条件

$$\boldsymbol{H}\boldsymbol{u}^T=\boldsymbol{0} \quad (\text{または } \boldsymbol{u}\boldsymbol{H}^T=\boldsymbol{0})$$

$\boldsymbol{H}$ は検査行列である.

# 10.5 シンドロームs

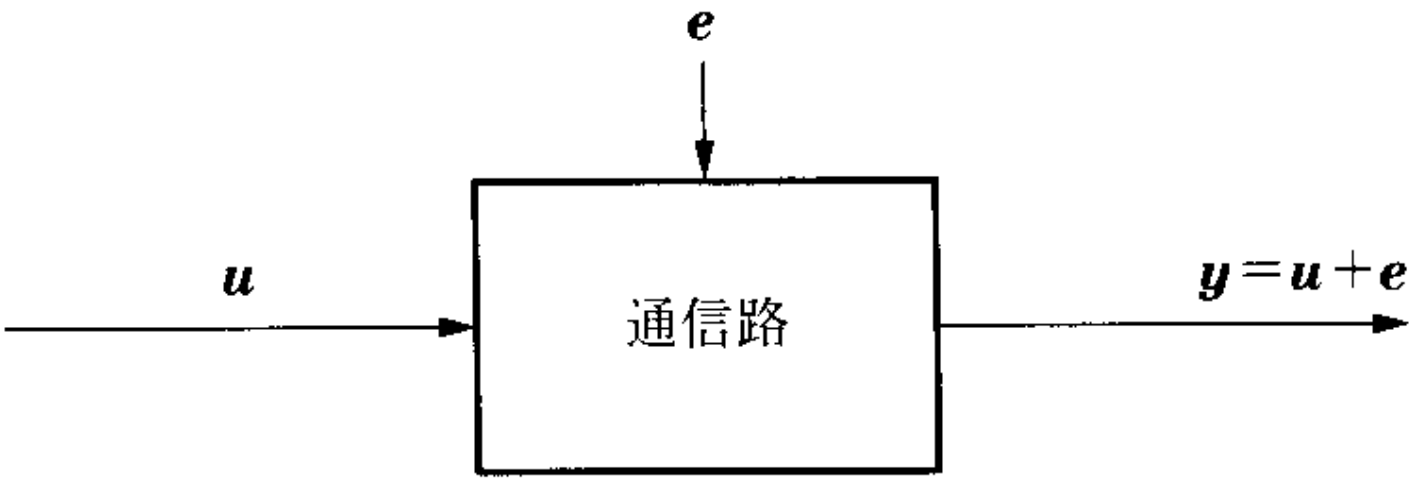



図 10.1　誤りベクトル

$$\boldsymbol{y}=\boldsymbol{u}+\boldsymbol{e}$$

$$\boldsymbol{s}=\boldsymbol{y}\boldsymbol{H}^{T}$$

$$\boldsymbol{s}=\boldsymbol{y}\boldsymbol{H}^{T}=(\boldsymbol{u}+\boldsymbol{e})\boldsymbol{H}^{T}=\underbrace{\boldsymbol{u}\boldsymbol{H}^{T}}_{\mathbf{0}}+\boldsymbol{e}\boldsymbol{H}^{T}=\boldsymbol{e}\boldsymbol{H}^{T}$$

# シンドロームの性質

【性質 10.4】

シンドローム $\boldsymbol{s}$ と誤りの存在には，次の関係が成り立つ．

$$\left.\begin{array}{ll} \boldsymbol{s}=\boldsymbol{0} & \Leftrightarrow \quad \text{誤りなし} \\ \boldsymbol{s}\neq\boldsymbol{0} & \Leftrightarrow \quad \text{誤りあり} \end{array}\right\}$$

【性質 10.5】

シンドローム $\boldsymbol{s}\neq\boldsymbol{0}$ になる場合，誤りが1つと仮定すると，その値によって誤りの箇所が，以下のように検出でき，訂正が可能となる．

$$\boldsymbol{s}=(\boldsymbol{H}\ \text{の}\ i\ \text{列}) \quad \Leftrightarrow \quad i\ \text{番目の受信記号が誤り} \tag{10.28}$$

$$\boldsymbol{e}=\left(0,\cdots,0,\underset{i}{1},0,\cdots,0\right)$$

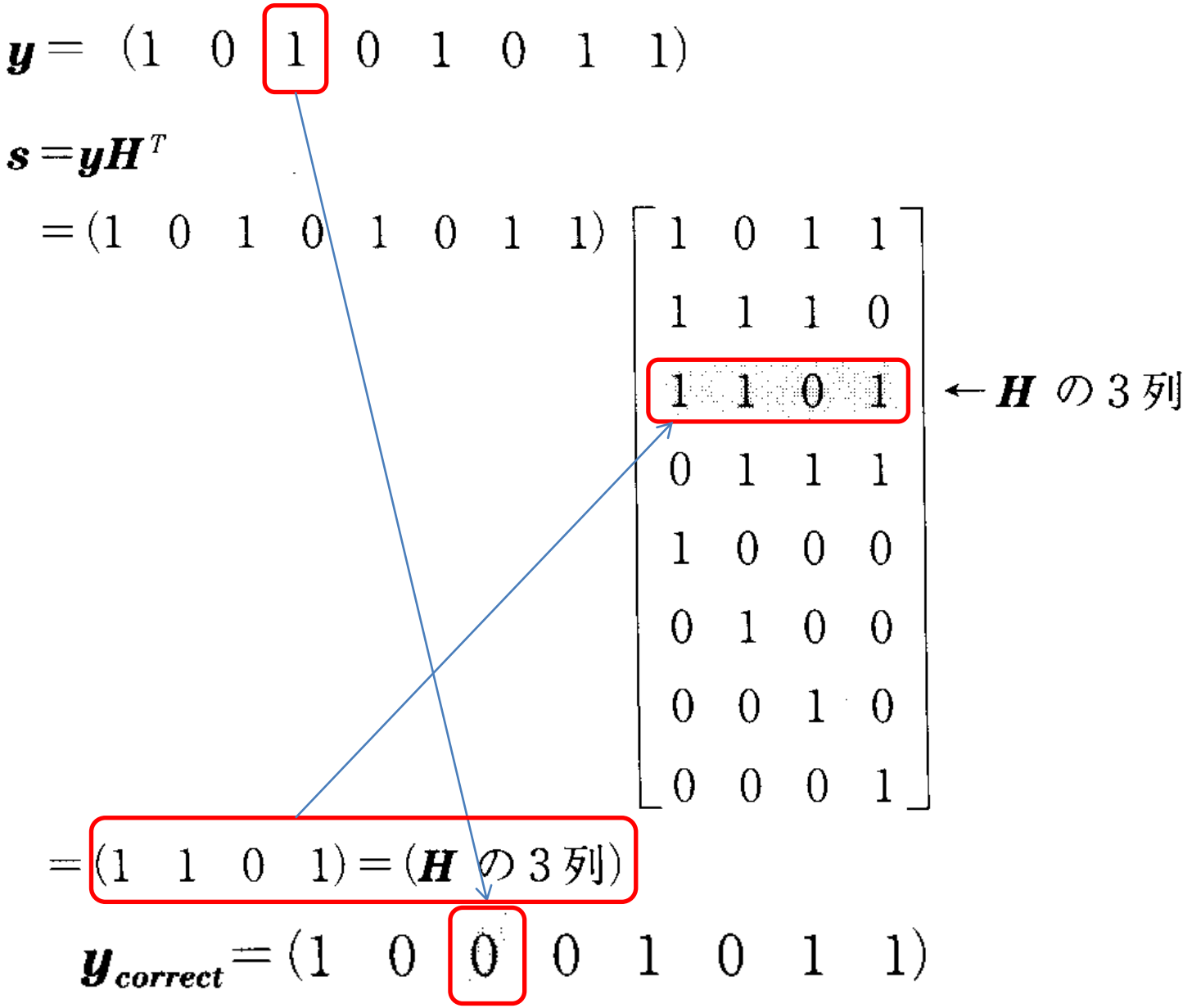
$$\boldsymbol{s} = \underbrace{(0, \cdots, 0, 1, 0, \cdots, 0)}_{i}$$

$$\begin{bmatrix} p_{11} & \cdot & \cdot & \cdot & p_{n-k1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{1i} & \cdot & \cdot & \cdot & p_{n-ki} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{1k} & \cdot & \cdot & \cdot & p_{n-kk} \\ 1 & & & & \\ & \cdot & & 0 & \\ & & \cdot & & \\ & 0 & & \cdot & \\ & & & & 1 \end{bmatrix} \leftarrow \boldsymbol{H} \text{ の } i \text{ 列}$$

$$= (p_{1i}, \cdots, p_{n-ki}) = (\boldsymbol{H} \text{ の } i \text{ 列}) \qquad (10.30)$$

$$\therefore \boldsymbol{s} = (\boldsymbol{H} \text{ の } i \text{ 列}) \quad \Leftrightarrow \quad i \text{ 番目の受信記号が誤り}$$

# 例題10.3


$\boldsymbol{y} = (1\ 0\ 1\ 0\ 1\ 0\ 1\ 1)$
$\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^T$
$= (1\ 0\ 1\ 0\ 1\ 0\ 1\ 1)$
$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
← $\boldsymbol{H}$ の 3 列
$= (1\ 1\ 0\ 1) = (\boldsymbol{H}$ の 3 列$)$
$\boldsymbol{y}_{correct} = (1\ 0\ 0\ 0\ 1\ 0\ 1\ 1)$

# 10.6　生成行列Gと検査行列Hの関係

【性質 10.6】

$$\boldsymbol{G}\boldsymbol{H}^T=\boldsymbol{0}$$

（証明）

$$\boldsymbol{G}\boldsymbol{H}^T=[\boldsymbol{I}_k,\boldsymbol{P}^T]\begin{bmatrix}\boldsymbol{P}^T\\ \\ \boldsymbol{I}_{n-k}\end{bmatrix}=\boldsymbol{P}^T+\boldsymbol{P}^T=\boldsymbol{0}$$

$$\because\quad \forall k,\ \ell\quad p_{i\ell}+p_{i\ell}=0$$

# 10.7 線形符号Cの最小ハミング距離

符号 $C=\{\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_n\}$ の最小ハミング距離

$$d_{\min}(C)=\min_{\substack{\forall(\boldsymbol{c}_k,\boldsymbol{c}_\ell)\\ k\neq\ell}} h(\boldsymbol{c}_k,\boldsymbol{c}_\ell)$$

$$h(\boldsymbol{x},\boldsymbol{y})=w(\boldsymbol{x}-\boldsymbol{y})=w(\boldsymbol{x}+\boldsymbol{y})$$

$$d_{\min}(C)=\min_{\substack{\forall(\boldsymbol{c}_k,\boldsymbol{c}_\ell)\\ k\neq\ell}} w(\boldsymbol{c}_k+\boldsymbol{c}_\ell)$$

$$d_{\min}(C)=\min_{\forall\boldsymbol{c}_i(\neq\boldsymbol{0})} w(\boldsymbol{c}_i) \qquad \boldsymbol{c}_i=\boldsymbol{c}_k+\boldsymbol{c}_l$$

# 線形符号の1次結合

$$\forall \boldsymbol{c}_k, \boldsymbol{c}_\ell \in C \quad \text{（線形符号）}$$

$$(\boldsymbol{c}_k + \boldsymbol{c}_\ell)\boldsymbol{H}^T = \underbrace{\boldsymbol{c}_k \boldsymbol{H}^T}_{0} + \underbrace{\boldsymbol{c}_\ell \boldsymbol{H}^T}_{0} = \boldsymbol{0}$$

$$\boldsymbol{c}_k + \boldsymbol{c}_\ell \in C \quad \text{（線形符号）}$$

線形符号の1次結合（線形結合）もまた線形符号である.

【性質 10.7】

$$d_{\min}(C)=d$$

ここで，$d$ は **0** 以外の全符号語のハミング重みの最小値である．

【性質 10.8】

**0** 以外の全符号語のハミング重みの最小値 $d$ を用いて，線形符号の誤り検出・訂正の原理が，次のように成り立つ．

（1） $s$ 個以下の誤りの検出が可能

$\Leftrightarrow \quad d \geq s+1$ ・・・(9.23)と同じ

（2） $t$ 個以下の誤りの訂正が可能

$\Leftrightarrow \quad d \geq 2t+1$ ・・・(9.24)と同じ

# 演　習

（1）記号列$x = 101100101$を偶数パリティ，及び，奇数パリティで送信するときの検査ビット$p$を求めよ.

# 演　習

（2）次の符号$C$について，以下の問いに答えよ.

$$C = \{c_1, c_2, c_3\}$$
$$c_1 = 100101, c_2 = 101011, c_3 = 011011$$

（i） ハミング距離$h(c_1, c_2)$を求めよ.
（ii）ハミング重み$w(c_3)$を求めよ.
（iii） $h(c_1, c_3) = w(c_1 - c_3) = w(c_1 + c_3)$を確かめよ.
（iv）最小ハミング距離$d_{min}(C)$を求めよ.
（v） $d_{min}(C) = \min h(c_k, c_l) = \min w(c_k + c_l)$を確かめよ.

# 演　習

（３）以下の問いに答えよ.

（i） 検査行列$\boldsymbol{H}$が次式で与えられるとき，受信記号ベクトル $y = (1010011)$ が正しいか否か判定せよ.

（ii） もし，誤っているとき，誤りが１個であると仮定して，訂正した受信記号ベクトルを求めよ.

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$