2011年後期
通信伝送工学

第6回　誤り訂正符号

阪口 啓 <sakaguchi@mobile.ee.titech.ac.jp>

2011年11月22日

講義スケジュール前半

	日付	教科書	内容
第1回	10月4日	1	通信伝送のモデルと具体例
第2回	10月11日	10.1 – 10.3	情報理論1：情報源符号化
第3回	10月25日	10.4 – 10.5	情報理論2：データ圧縮
	11月1日		休講
第4回	11月8日	10.6 – 10.7	情報理論3：通信路容量
第5回	11月15日	10.8	情報理論4：通信路符号化
第6回	11月22日	10.10 – 10.11	情報理論5：誤り訂正符号
	11月29日		中間試験

前回の復習

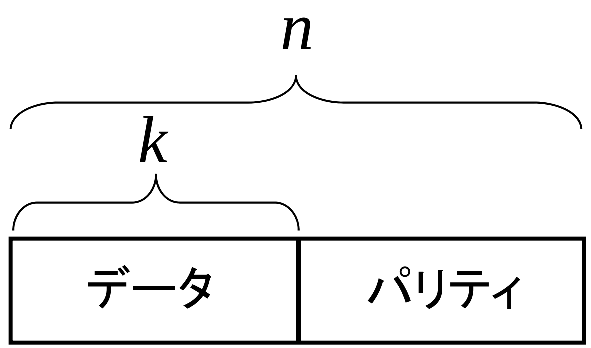
- 通信路容量

$$C = \max_{p(x_j)} I(X;Y) = \max_{p(x_j)} \left[H(X) - H(X \mid Y) \right]$$

- 通信路符号化

k ビットのデータを *n* ビットの符号にマッピング

符号化率:　$r = \dfrac{k}{n}$



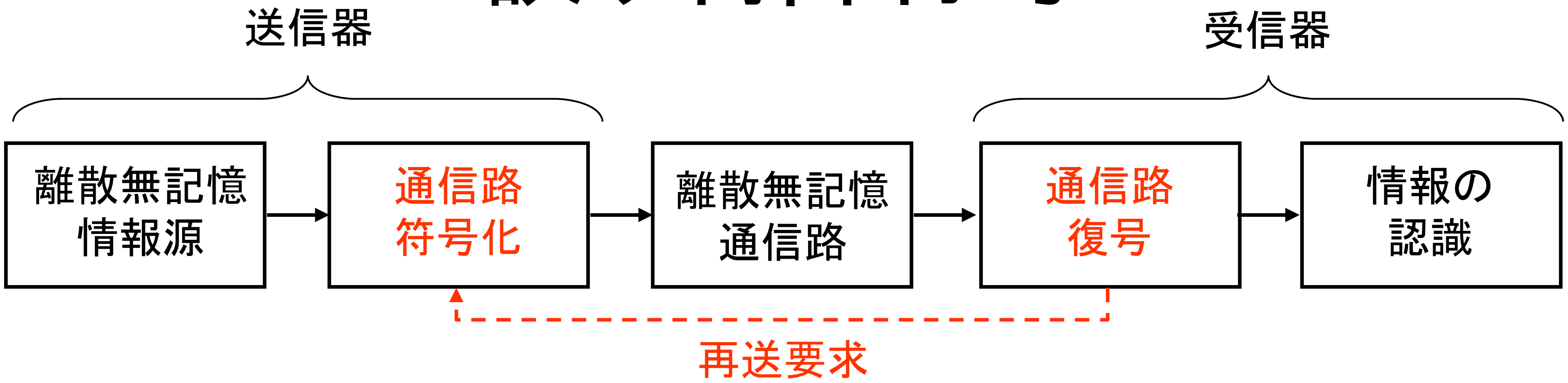
- 通信路符号化定理

$$H(\zeta)/T_{\mathrm{s}} \le C/T_{\mathrm{c}} \longrightarrow$$ 誤り率を任意に小さくできる符号が存在

- 二元対称通信路

$$\frac{H(\zeta)}{T_{\mathrm{s}}} = \frac{H(\zeta)}{nT_{\mathrm{c}}} = \frac{k}{nT_{\mathrm{c}}} \le \frac{C}{T_{\mathrm{c}}} \longrightarrow r \le C$$

誤り制御符号



■ 誤り制御符号の種類

- 前方誤り訂正符号

通信路符号化による冗長性によりある範囲の誤りを訂正する通信方式

例: 繰返し符号、ハミング符号、畳込み符号、ターボ符号、LDPC符号

- 誤り検出符号＋再送

通信路符号化による冗長性によりある精度で誤りを検出し再送を行う通信方式

例: パリティ検査符号＋自動再送要求(ARQ) ⟶ 奇数パリティ = 1
if ビット1の数 = 奇数

誤り訂正符号(二元対称通信路)

■ 通信路容量

$$C = \max I(X;Y) = 1 - H(p)$$

■ (n, k) 符号

k ビットデータ $\longrightarrow$ n ビット符号

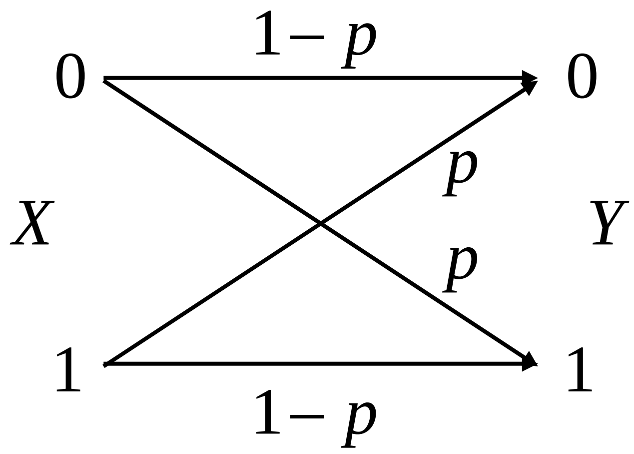
符号化率: $r = k/n < 1$

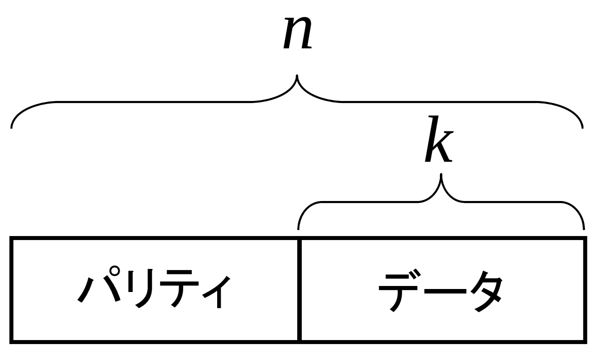
■ 通信路符号化定理

$r \le C$ $\longrightarrow$ 任意に誤り訂正可能

■ (3,1) 繰返し符号の例

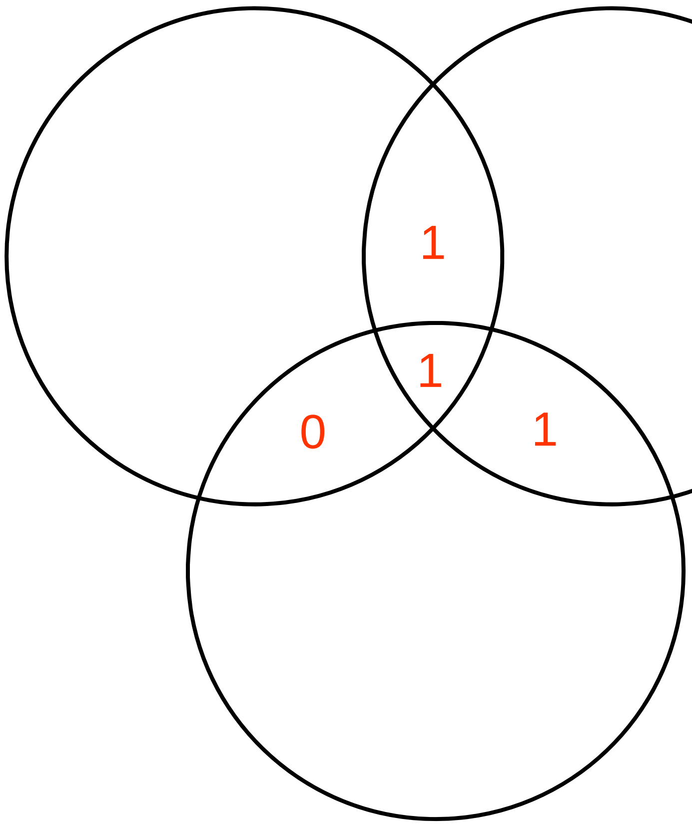
$r = 1/3$ $\longrightarrow$ より高いデータレートを実現するには?

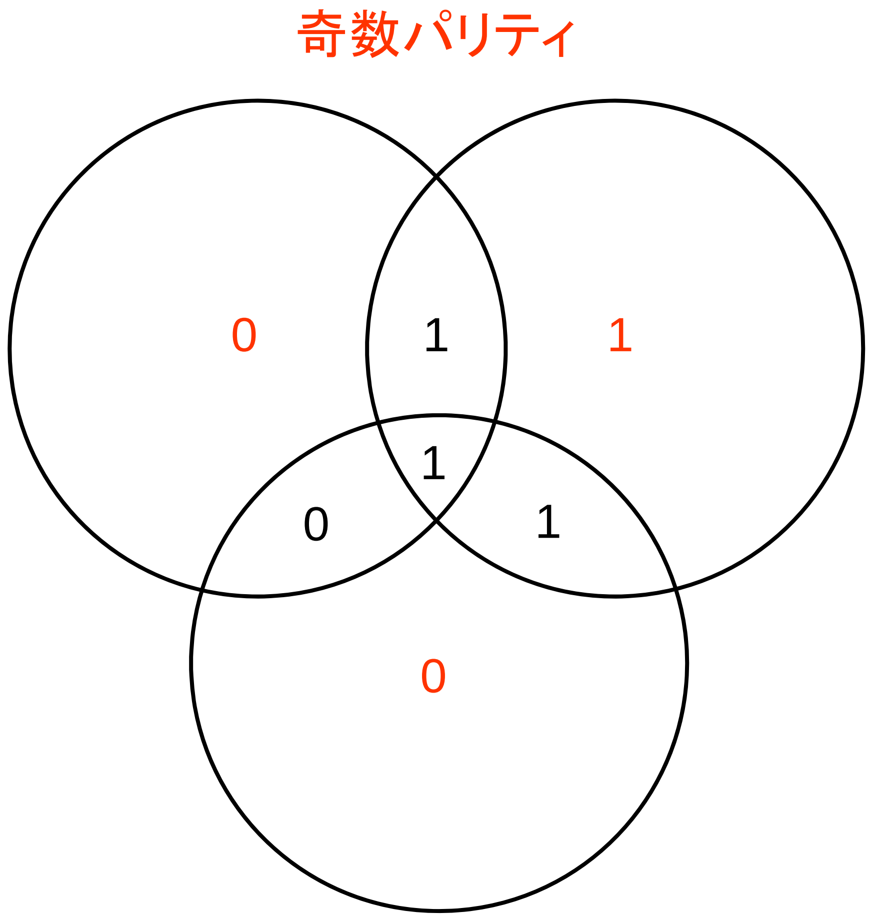




誤り訂正符号の例

- メッセージ (1011)
- (7,4) ハミング符号 (1001011)





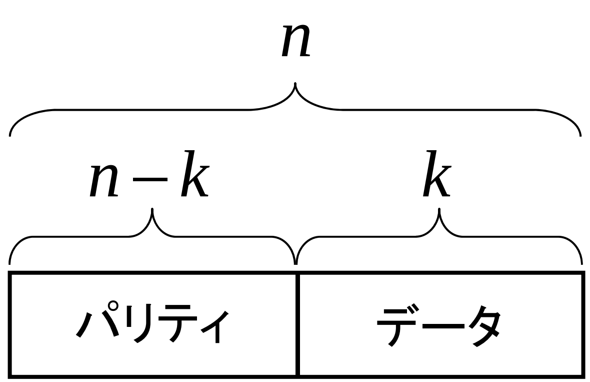
線形ブロック符号

- (n, k) ブロック符号（組織符号）

メッセージ：　$\mathbf{m} = \begin{bmatrix} m_0 & m_1 & \cdots & m_{k-1} \end{bmatrix}$

パリティ：　$\mathbf{b} = \begin{bmatrix} b_0 & b_1 & \cdots & b_{n-k-1} \end{bmatrix}$

符号語：　$\mathbf{c} = \begin{bmatrix} c_0 & c_1 & \cdots & c_{n-1} \end{bmatrix}$



- 二元線形符号

$\mathbf{c}_i + \mathbf{c}_j = \mathbf{c}_k$ ⟶ 2つの異なる符号語の和は第3の符号語

- 二元演算

$x_i + x_j = (x_i + x_j) \bmod 2$ ⟶ ExOR

$x_i \times x_j = (x_i \times x_j) \bmod 2$ ⟶ AND

符号語間距離

■ ハミング距離

符号語間の異なる要素の数 ⟶ 大きいほど良い符号

例: $\mathrm{d}(\mathbf{c}_1, \mathbf{c}_2) = \mathbf{c}_1 + \mathbf{c}_2 = 3$

• 符号語

$$\mathbf{c}_1 = [1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1]$$
$$\mathbf{c}_2 = [1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0]$$

■ ハミング重み

符号語と全ゼロ符号とのハミング距離

$w(\mathbf{c}) = \mathrm{d}(\mathbf{c}, \mathbf{0})$ 例: $w(\mathbf{c}_1) = 3$ $w(\mathbf{c}_2) = 4$

■ 線形符号の特性

符号語間のハミング距離は第三の符号語のハミング重みに等価

$$\mathrm{d}(\mathbf{c}_0, \mathbf{c}_1) = w(\mathbf{c}_0 + \mathbf{c}_1) = w(\mathbf{c}_2)$$

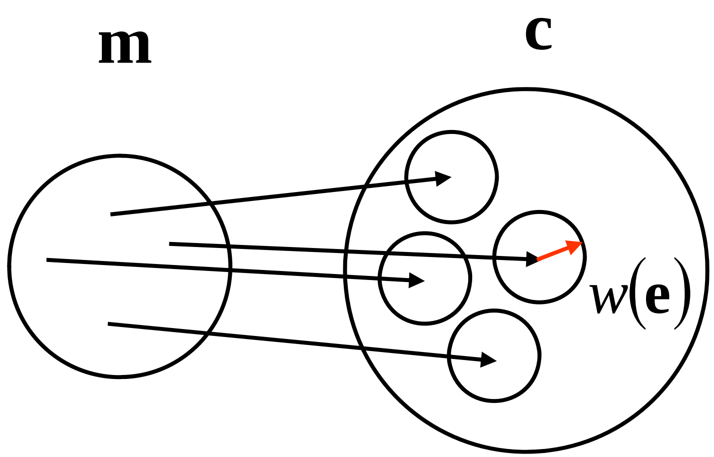
誤りベクトル

■ 誤りベクトル

ビット誤り

誤りベクトル：　$\mathbf{e} = \underbrace{\begin{bmatrix} 0 & 0 & 1 & \cdots & 0 \end{bmatrix}}_{n}$

誤りの数（重み）　$w(\mathbf{e})$



■ 受信ベクトル

符号語：　$\mathbf{c} = \begin{bmatrix} c_0 & c_1 & \cdots & c_{n-1} \end{bmatrix}$

誤りベクトル：　$\mathbf{e} = \begin{bmatrix} 0 & 0 & 1 & \cdots & 0 \end{bmatrix}$

受信ベクトル：　$\mathbf{r} = \mathbf{c} + \mathbf{e}$

$\mathbf{c} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

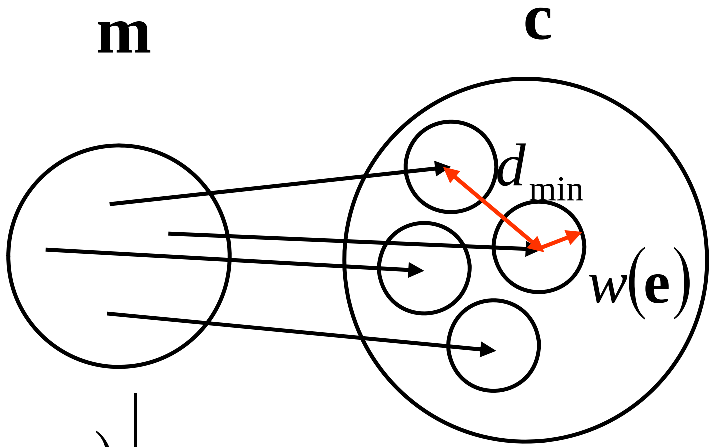
$\mathbf{e} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$

$\mathbf{r} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

最小距離

- 最小距離

$$d_{\min} = \min_{i,j} d(\mathbf{c}_i, \mathbf{c}_j) = \min_i w(\mathbf{c}_i)$$



誤りの数 $w(\mathbf{e})$ が下記を満たせば

$\longrightarrow$ 誤り訂正可能

$$d_{\min} \geq 2w(\mathbf{e}) + 1 \quad \text{or} \quad w(\mathbf{e}) \leq \left\lfloor \frac{1}{2}(d_{\min} - 1) \right\rfloor$$

- (3,1) 繰返し符号の場合

$$d_{\min} = 3$$

$w(\mathbf{e}) \leq 1$ まで訂正可能

$\longrightarrow$ 多数決復号

$$\overbrace{\qquad\qquad\qquad\qquad}^{n=3}$$

1	1	1

符号生成

■ 生成行列

$$\mathbf{G} = \begin{bmatrix} \mathbf{P} & \mathbf{I}_k \end{bmatrix} \in R^{k \times n}$$

- 係数行列

$$\mathbf{P} = \begin{bmatrix} p_{0,0} & \cdots & p_{0,n-k-1} \\ \vdots & \ddots & \vdots \\ p_{k-1,0} & \cdots & p_{k-1,n-k-1} \end{bmatrix}$$

- 単位行列

$$\mathbf{I}_k = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

■ 符号の生成

$$\mathbf{c} = \mathbf{mG} = \begin{bmatrix} \mathbf{mP} & \mathbf{m} \end{bmatrix} = \begin{bmatrix} \overbrace{\mathbf{b}}^{\text{パリティ}} & \underbrace{\mathbf{m}}_{\text{メッセージ}} \end{bmatrix}$$

■ (3,1) 繰返し符号の場合

$$\mathbf{m} = 0 \quad \text{or} \quad 1 \qquad \mathbf{G} = \begin{bmatrix} \underbrace{1 \quad 1}_{\text{パリティ}} & \underbrace{1}_{\text{メッセージ}} \end{bmatrix}$$

(7,4) ハミング符号

- 生成行列

$$\mathbf{G} = \begin{bmatrix} \mathbf{P} & \mathbf{I}_k \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

係数行列

符号化率：

$$r = k/n = 4/7$$

- 最小距離 $d_{\min} = 3$

メッセージ	符号	ハミング重み	メッセージ	符号	ハミング重み
0000	0000000	0	1000	1101000	3
0001	1010001	3	1001	0111001	4
0010	1110010	4	1010	0011010	3
0011	0100011	3	1011	1001011	4
0100	0110100	3	1100	1011100	4
0101	1100101	4	1101	0001101	3
0110	1000110	3	1110	0101110	4
0111	0010111	4	1111	1111111	7

パリティ検査行列

- パリティ検査行列

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}_{n-k} & \mathbf{P}^T \end{bmatrix} \in R^{(n-k)\times n}$$

- パリティ検査行列の特徴

$$\mathbf{G}\mathbf{H}^T = \begin{bmatrix} \mathbf{P} & \mathbf{I}_k \end{bmatrix} \begin{bmatrix} \mathbf{I}_{n-k} \\ \mathbf{P} \end{bmatrix} = \mathbf{P} + \mathbf{P} = \mathbf{0} \longrightarrow$$

$$\mathbf{c}\mathbf{H}^T = \mathbf{m}\mathbf{G}\mathbf{H}^T = \mathbf{0} \longrightarrow$$ 符号語との直交性

双対符号

$\mathbf{H}$ と $\mathbf{G}$ は

交換可能

- (3,1) 繰返し符号の場合

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \longrightarrow \mathbf{G}\mathbf{H}^T = \mathbf{0}$$

シンドローム

- 誤りベクトル

受信ベクトル：$\mathbf{r} = \mathbf{c} + \mathbf{e}$

誤りベクトル：$\mathbf{e} = \begin{bmatrix} 0 & 0 & 1 & \cdots & 0 \end{bmatrix}$

⟶ 誤りパターン 2^n 誤りの数（重み） $w(\mathbf{e})$

- シンドローム

$$\mathbf{s} = \mathbf{r}\mathbf{H}^T = (\mathbf{c} + \mathbf{e})\mathbf{H}^T$$

$$= \mathbf{c}\mathbf{H}^T + \mathbf{e}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$$

⟶ 誤りのみに異存するベクトル（誤り検出可能）

- (3,1) 繰返し符号の場合

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \mathbf{e} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \longrightarrow \mathbf{s} = \begin{bmatrix} 0 & 1 \end{bmatrix}$$

コセット

- 同一の誤りベクトルを持つ異なる符号語の受信ベクトル

$$\mathbf{r}_{i,j}=\mathbf{c}_i+\mathbf{e}_j \quad i=1,\cdots,2^k \qquad j=1,\cdots,2^n$$

$$\mathbf{r}_i\mathbf{H}^T=\mathbf{c}_i\mathbf{H}^T+\mathbf{e}_j\mathbf{H}^T=\mathbf{e}_j\mathbf{H}^T=\mathbf{s}_j$$ 同一のシンドローム

- コセット（同一のシンドロームを持つセット）

$$\varpi_j=\{\mathbf{r}_{0,j},\mathbf{r}_{1,j},\cdots,\mathbf{r}_{2^k-1,j}\} \qquad j=1,\cdots,2^{n-k}$$

2^n の受信ベクトル空間の内、2^k は同一のシンドロームを持つ

⟶ 誤りベクトルの種類が 2^{n-k} 通り以内、

かつ $d_{\min}\geq 2w(\mathbf{e})+1$ であれば一意に誤り訂正可能

- (3,1) 繰返し符号の場合

$$d_{\min}=3 \qquad \begin{array}{ll}\mathbf{e}_0=[0\quad 0\quad 0] & \mathbf{e}_2=[0\quad 1\quad 0]\\ \mathbf{e}_1=[0\quad 0\quad 1] & \mathbf{e}_3=[1\quad 0\quad 0]\end{array}$$

⟶ 一意に訂正可能

シンドローム復号

- (7,4)ハミング符号のパリティ検査行列

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}_{n-k} & \mathbf{P}^T \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- シンドローム復号

$$d_{\min} = 3$$

誤り訂正能力 = 1 [bit]

$$\mathbf{s} = \mathbf{r}\mathbf{H}^T = \hat{\mathbf{e}}\mathbf{H}^T$$

シンドロームによる誤り訂正

$$\hat{\mathbf{c}} = \mathbf{r} + \hat{\mathbf{e}}$$

シンドローム $\mathbf{s}$	エラーベクトル $\hat{\mathbf{e}}$
000	0000000
100	1000000
010	0100000
001	0010000
110	0001000
011	0000100
111	0000010
101	0000001

8通り

まとめ

1. 線形ブロック符号による前方誤り訂正

   k ビットデータと *n* – *k* ビットパリティによる組織符号

2. 誤り訂正能力と最小ハミング距離

$$w(\mathbf{e}) \leq \left\lfloor \frac{1}{2}(d_{\min} - 1) \right\rfloor$$

3. ハミング符号とシンドローム復号

   生成行列を用いた符号化とパリティ検査行列を用いた復号

中間試験

- 日時: 11月29日(火) 3･4限
- 場所: 未定
- 出題範囲:

  通信伝送のモデル、情報源符号化、
  データ圧縮、通信路容量、通信路符号化、
  誤り訂正符号
- 言語: 日本語
- 備考:
  教科書の演習と類似した問題を出題
  持ち込みは不可