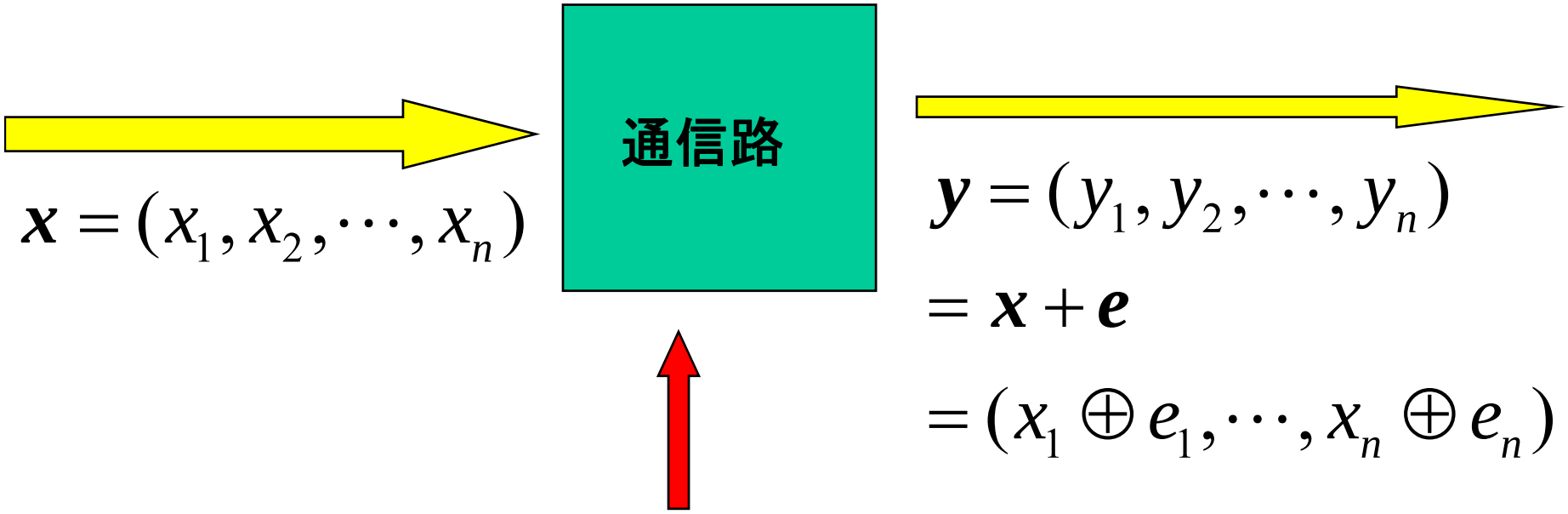
誤り訂正検出の原理と
具体的符号

誤り検出・訂正の原理

通信路モデルにおける誤り



$\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$

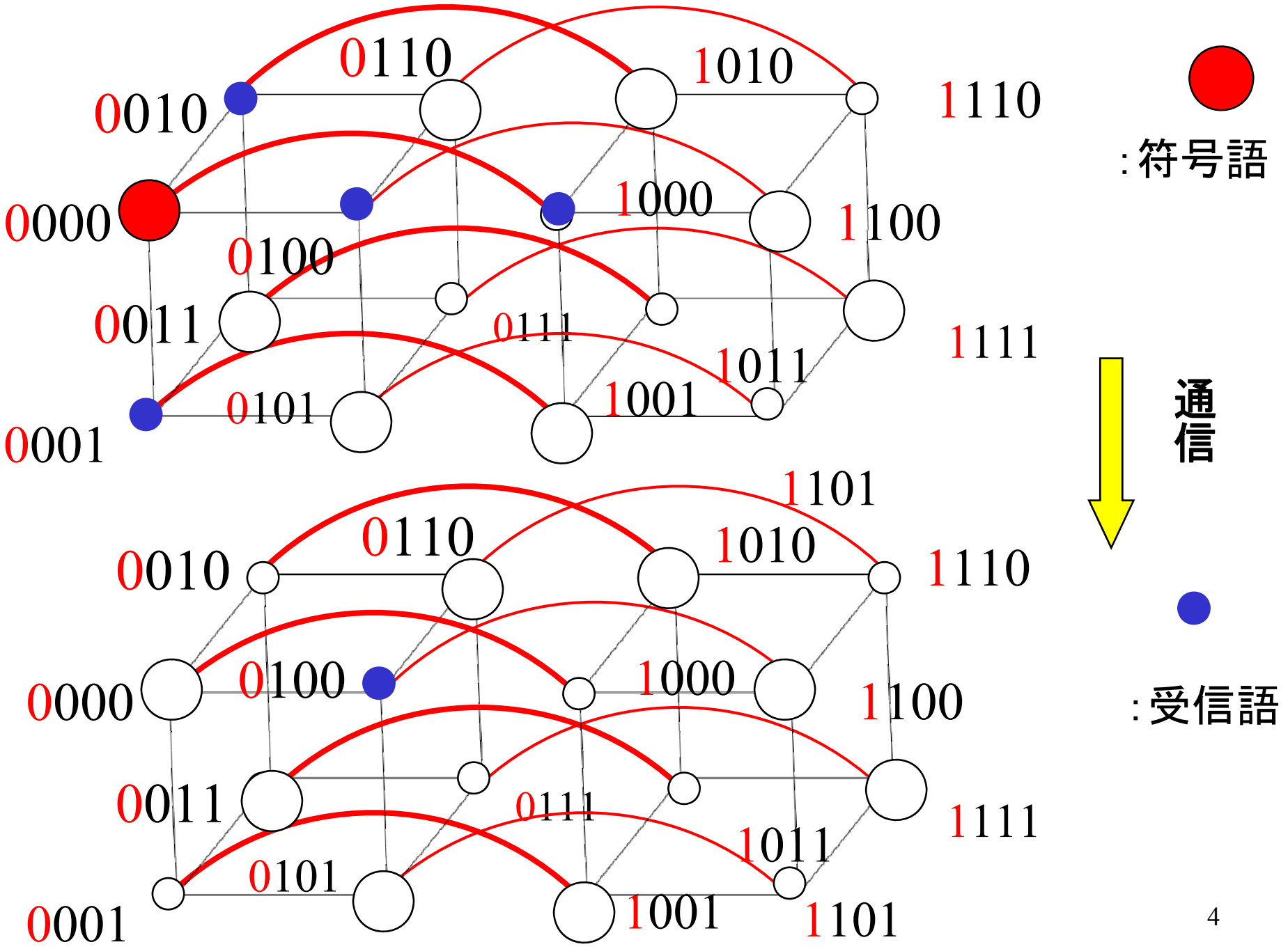
$\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$

$= \boldsymbol{x} + \boldsymbol{e}$

$= (x_1 \oplus e_1, \cdots, x_n \oplus e_n)$

$\boldsymbol{e} = (e_1, e_2, \cdots, e_n)$

誤りの混入


0110
1010
0010
1110
0000
1000
1100
0100
0011
0111
1111
1011
0101
1001
0001
1101
0110
1010
0010
1110
0000
0100
1000
1100
0011
0111
1111
1011
0101
0001
1001
1101
通信
:符号語
:受信語

前のスライドにおいては、
符号は

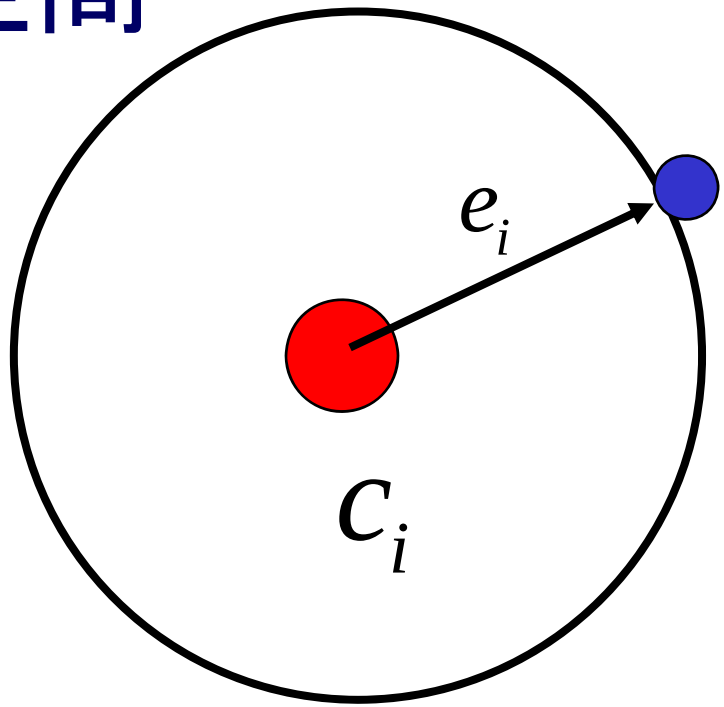
$$C = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$$

である。
このとき符号語 $c_i = 0000 \in C$ を伝送したとき、系列
$y_i = 0100 \notin C$
を受信したとする。
このとき、 誤り $e_i = 0100$ が混入される。

しかし、受信語がからは誤りが特定されない。

$$\begin{aligned} y_i &= 0100 \\ &= 0101 + 0001? \\ &= 0110 + 0010? \\ &= 0000 + 0100? \\ &= 1100 + 1000? \end{aligned}$$

誤り空間



$$\boldsymbol{y}_i = \boldsymbol{c}_i + \boldsymbol{e}_i$$

$(\mathrm{mod}\, 2)$

は省略する。

$$h(\boldsymbol{y}_i, \boldsymbol{c}_i) = h(\boldsymbol{0}, \boldsymbol{e}_i) = w(\boldsymbol{e}_i)$$

0ベクトルからのハミング距離を考えると便利なことが多い。

誤り空間例

1ビットの誤りが起こるとする。すなわち、

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

の誤り空間を考える。

このとき、各符号語 $\boldsymbol{c}_i \in C$ の誤り空間 $\boldsymbol{E}^1(\boldsymbol{c}_i)$ は以下のように表される。

（1） $\boldsymbol{c}_1 = 0000$

$$\boldsymbol{E}^1(\boldsymbol{c}_1) = \{0000, 0001, 0010, 0100, 1000\}$$

（2） $\boldsymbol{c}_2 = 1010$

$$\boldsymbol{E}^1(\boldsymbol{c}_2) = \{1010, 1011, 1000, 1110, 0010\}$$

練習1

情報ビットが4ビットで、偶数パリティのパリティビットが1ビットの5ビットの符号空間 C を考える。
この符号空間において、以下の符号語に対する1ビットの誤り空間を求めよ。

(1) $\boldsymbol{c}_1 = 00000$ $\quad\quad$ $\boldsymbol{E}^1(\boldsymbol{c}_1)$

(2) $\boldsymbol{c}_2 = 10001$ $\quad\quad$ $\boldsymbol{E}^1(\boldsymbol{c}_2)$

(3) $\boldsymbol{c}_3 = 01010$ $\quad\quad$ $\boldsymbol{E}^1(\boldsymbol{c}_3)$

(4) $\boldsymbol{c}_4 = 10111$ $\quad\quad$ $\boldsymbol{E}^1(\boldsymbol{c}_4)$

練習2

情報ビットが3ビットで、偶数パリティのパリティビットが1ビットの4ビットの符号空間 C を考える。
この符号空間において、以下の符号語に対する2ビットの誤り空間を求めよ。

（1） $\boldsymbol{c}_1 = 1111$

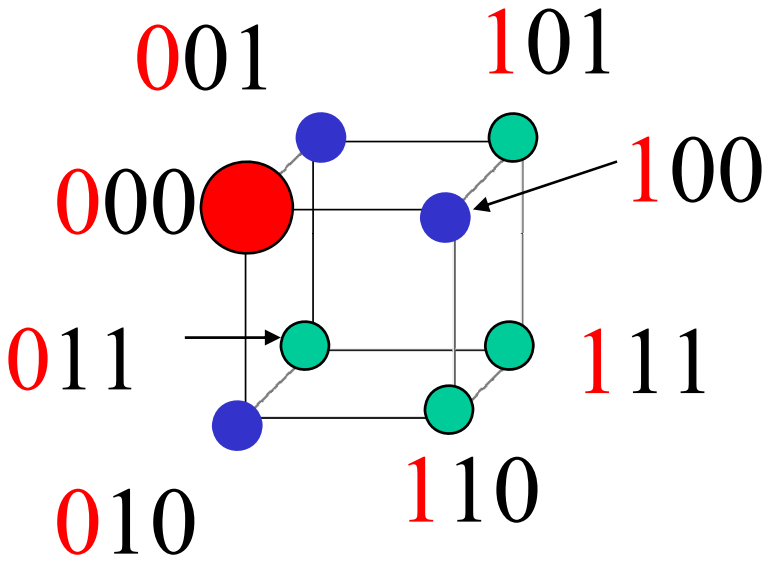
$\boldsymbol{E}^2(\boldsymbol{c}_1)$

（2）

$\boldsymbol{c}_2 = 1010$

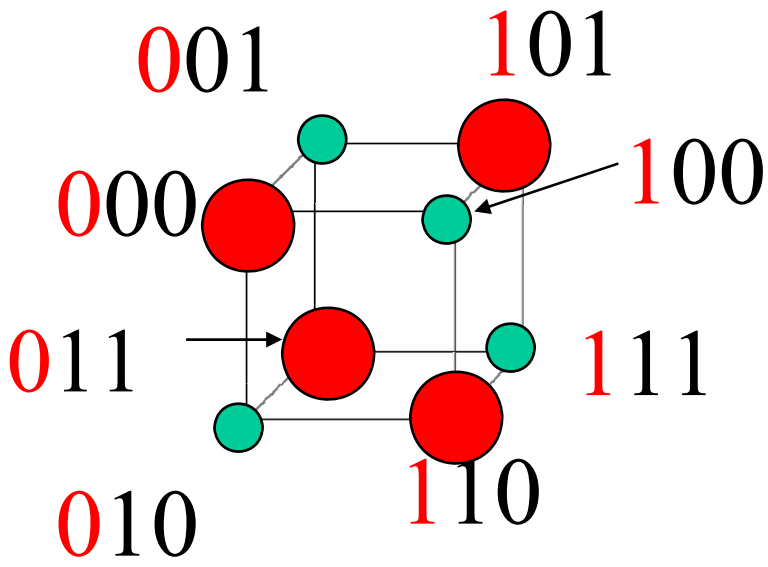
$\boldsymbol{E}^2(\boldsymbol{c}_2)$

誤り空間と誤り検出



$$\boldsymbol{c}_1 = 000$$

$$\boldsymbol{E}^1(\boldsymbol{c}_1) = \{000, 001, 010, 100\}$$

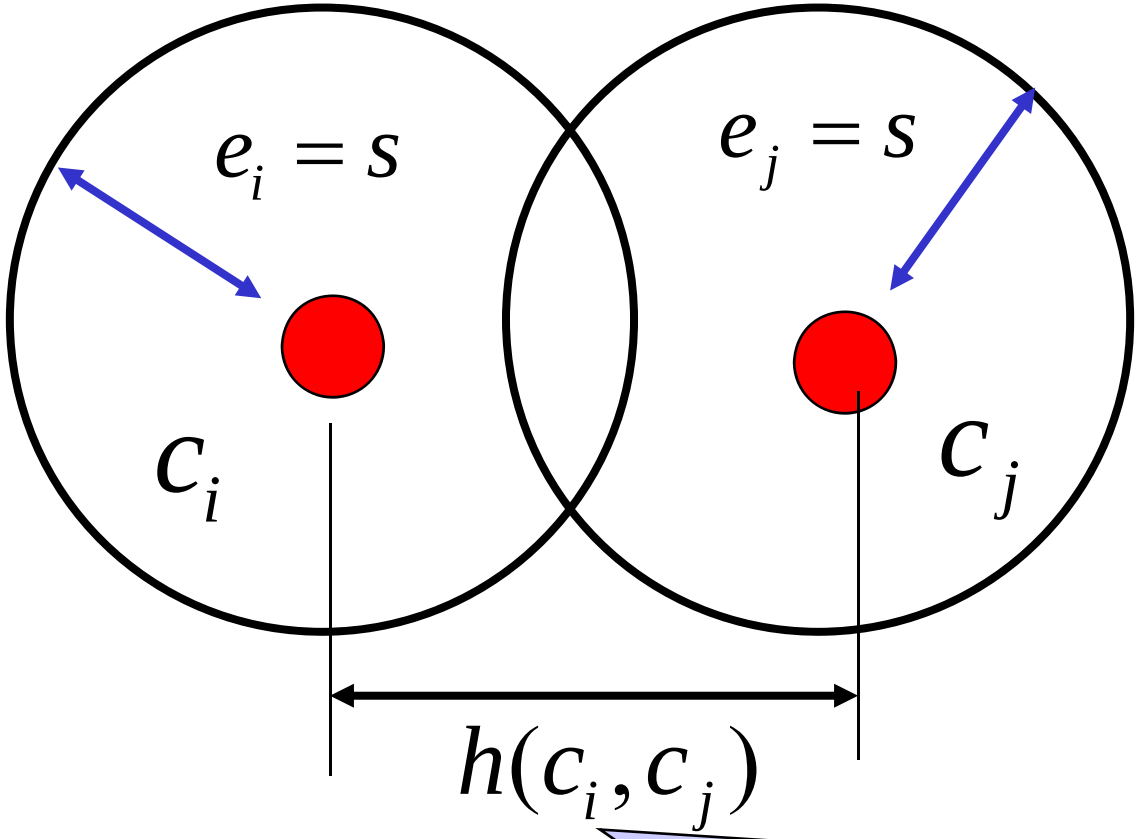


$$C = \{000, 011, 101, 110\}$$

$$\boldsymbol{E}^1(\boldsymbol{c}_i) \cap \boldsymbol{c}_j = \phi \quad i \neq j$$

1ビット誤り検出を可能とする関係式。

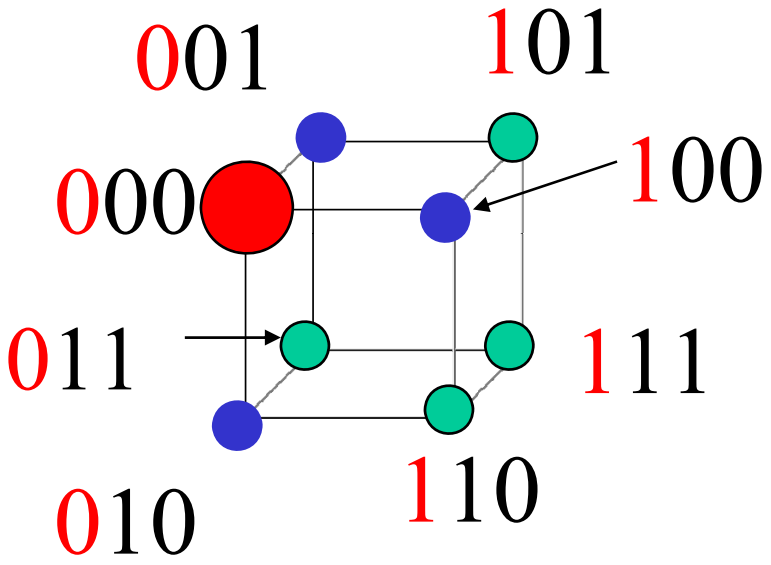
誤り検出の模式図



s ビット誤りを検出するためには次式が成り立つ必要がある。

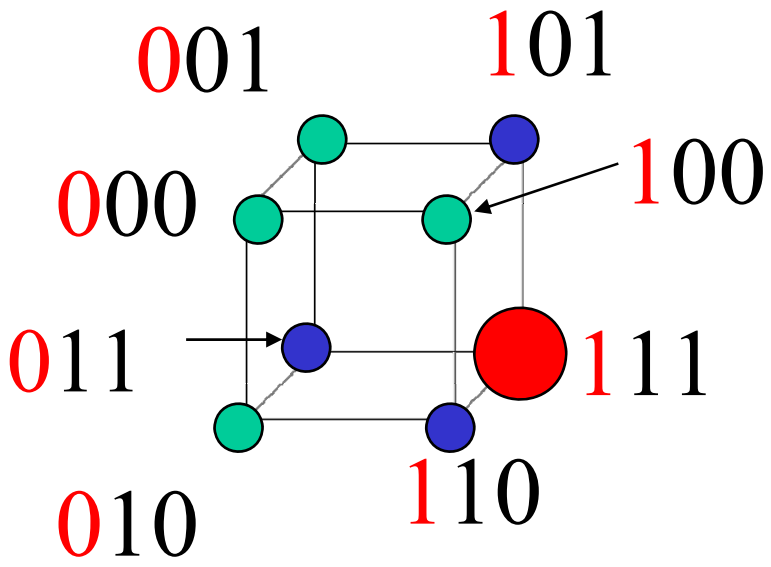
$$\forall i, j \quad h(c_i, c_j) \geq s + 1$$

誤り空間と誤り訂正



$$\boldsymbol{c}_1 = 000$$

$$\boldsymbol{E}^1(\boldsymbol{c}_1) = \{000, 001, 010, 100\}$$



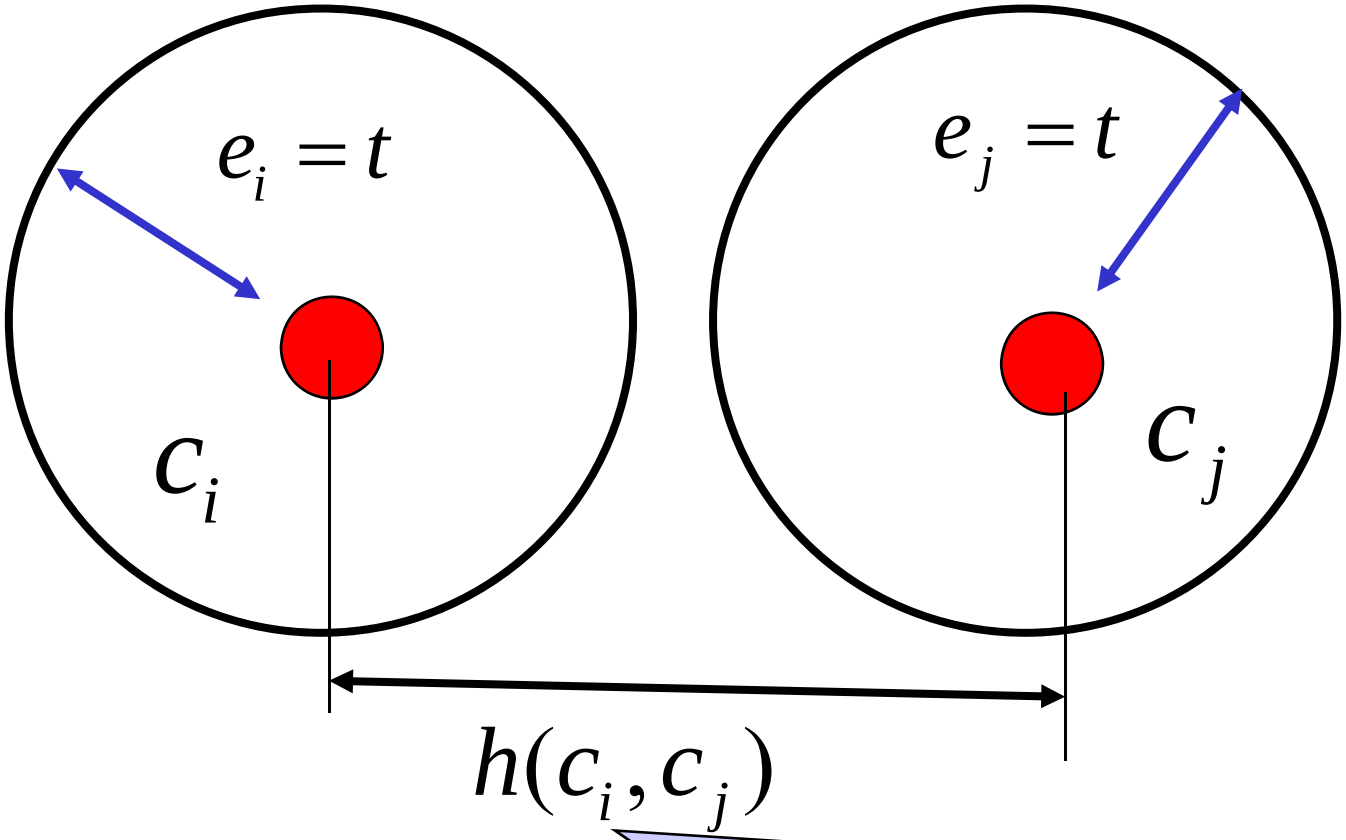
$$\boldsymbol{c}_2 = 111$$

$$\boldsymbol{E}^1(\boldsymbol{c}_2) = \{111, 110, 101, 011\}$$

$$\boldsymbol{E}^1(\boldsymbol{c}_1) \cap \boldsymbol{E}^1(\boldsymbol{c}_2) = \phi$$

1ビット誤り訂正を可能とする関係式。

誤り訂正の模式図



t ビット誤りを訂正するためには次式が成り立つ必要がある。

$$\forall i, j \quad h(c_i, c_j) \geq 2t + 1$$

誤り訂正の具体的符号

- 垂直水平パリティ検査符号
- ハミング符号

垂直水平パリティ符号

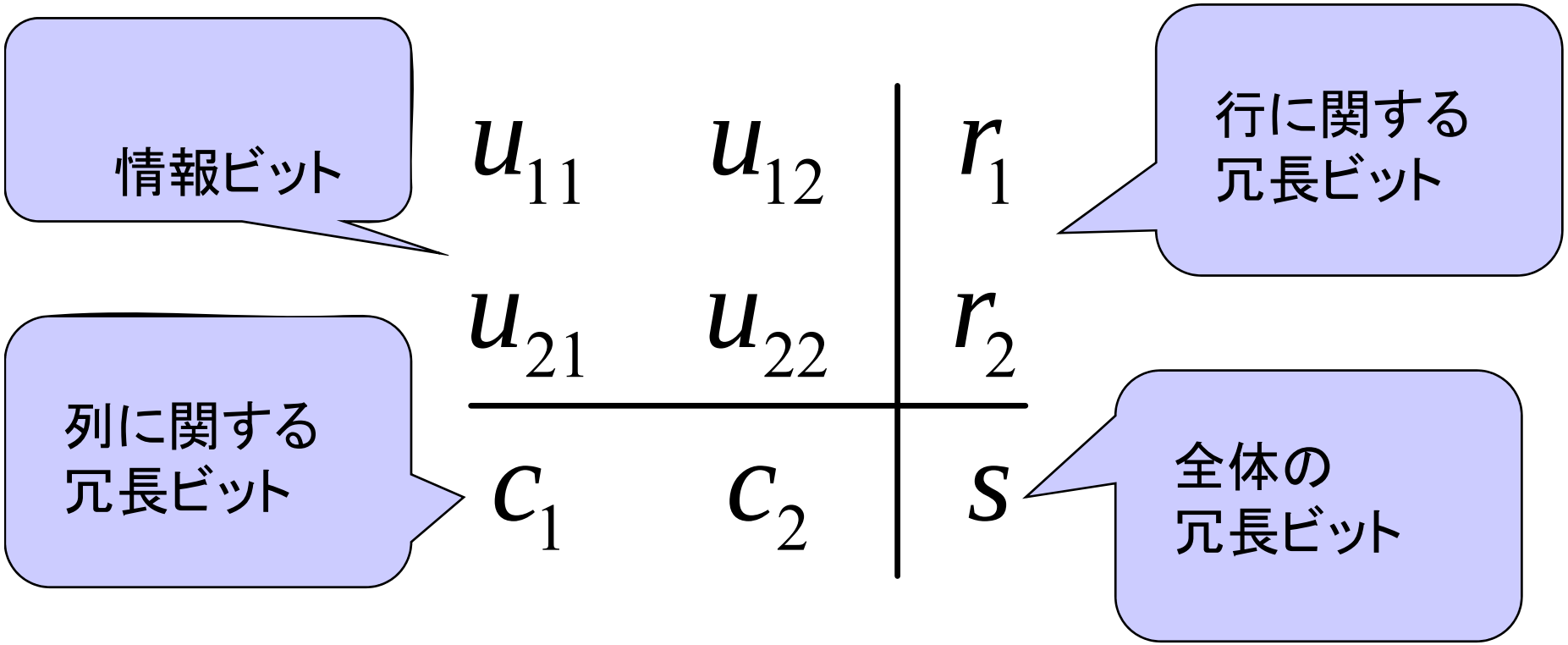
1ビット誤り検出可能な符号であるパリティ検査符号の考え方に基づいて1ビット誤り訂正可能な符号を構成できる。

まず、情報ビット4ビット、冗長ビット5ビットからの9ビットの垂直水平パリティ符号の構成法を示す。

$$\boldsymbol{w} = (w_1, w_2, \cdots, w_9)$$

$$= (x_1, x_2, x_3, x_4, p_1, p_2, p_3, p_4, p_5)$$

$$= (\boldsymbol{x}, \boldsymbol{p})$$



$$\boldsymbol{w} = (u_{11}, u_{12}, u_{21}, u_{22}, r_1, r_2, c_1, c_2, s)$$

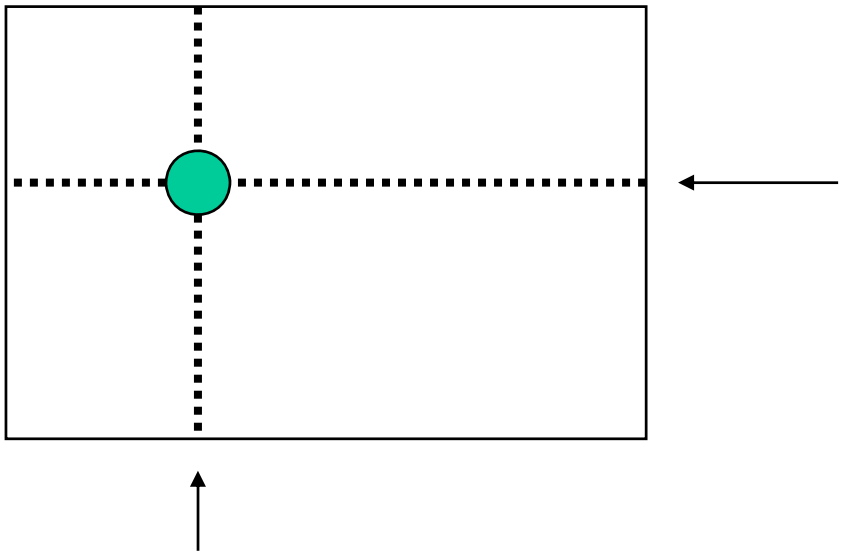
ただし、冗長ビットは次式で定める。

$$r_1 = u_{11} \oplus u_{12} \qquad r_2 = u_{21} \oplus u_{22}$$

$$c_1 = u_{11} \oplus u_{21} \qquad c_2 = u_{12} \oplus u_{22}$$

$$s = r_1 \oplus r_2 = c_1 \oplus c_2 = u_{11} \oplus u_{12} \oplus u_{21} \oplus u_{22}$$

垂直水平パリティ符号における誤り訂正の原理

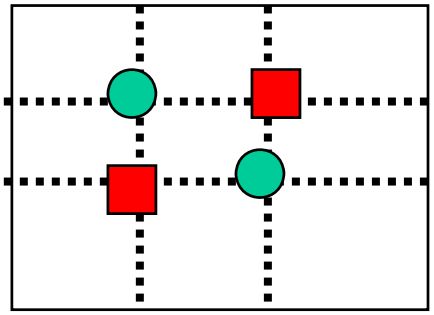


i 行の誤り検出

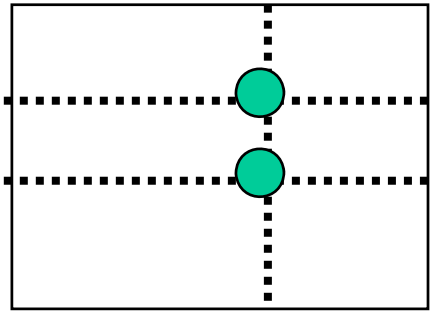
j 列の誤り検出

誤っている (i, j) 要素を
特定→1ビット誤り訂正

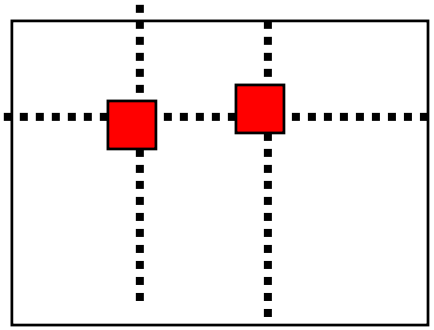
垂直水平パリティ符号における誤り訂正能力



2ビット誤りを検出可能であるが、丸と四角のどちらがあやまりかを判定できない。

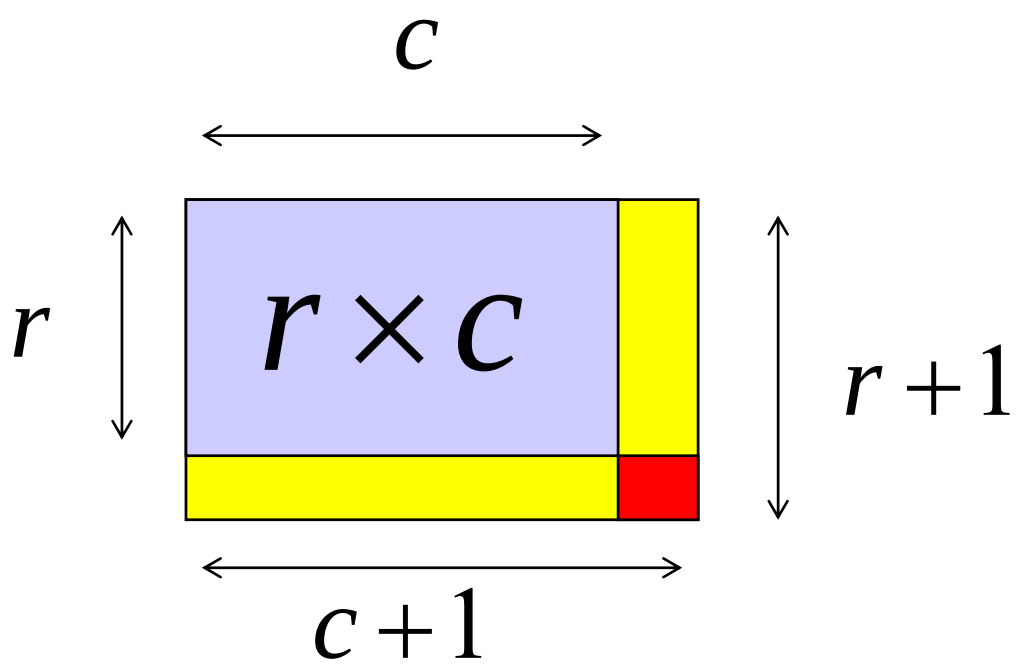


2ビット誤りを検出可能である。行は特定できるが、どの列がは特定不能。



2ビット誤りを検出可能である。列は特定できるが、どの行かは特定不能。

一般的な垂直水平パリティ符号



一般に、情報ビットが $r \times c$ であるとき、
符号ビットを $(r+1)\times(c+1)$ として構成できる。
したがって冗長ビットは $r+c+1$ である。

例

$$\boldsymbol{w} = (u_{11}, u_{12}, u_{21}, u_{22}, r_1, r_2, c_1, c_2, s)$$

の垂直水平パリティ符号を考える。このとき、次の情報ビットから垂直水平符号を求めよ。

$$\boldsymbol{x} = 0101 = u_{11}u_{12}u_{21}u_{22}$$

$$\therefore r_1 = u_{11} \oplus u_{12} = 0 \oplus 1 = 1, r_2 = u_{21} \oplus u_{22} = 0 \oplus 1 = 1,$$

$$c_1 = u_{11} \oplus u_{21} = 0 \oplus 0 = 0, r_2 = u_{12} \oplus u_{22} = 1 \oplus 1 = 0,$$

$$s = u_{11} \oplus u_{12} \oplus u_{21} \oplus u_{22} = 0$$

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

練習

$$\boldsymbol{w} = (u_{11}, u_{12}, u_{21}, u_{22}, r_1, r_2, c_1, c_2, s)$$

の垂直水平パリティ符号を考える。このとき、次の情報ビットから垂直水平パリティ符号を求めよ。

（1）

$$\boldsymbol{x}_1 = 0001$$

（2）

$$\boldsymbol{x}_2 = 1001$$

（3）

$$\boldsymbol{x}_3 = 1101$$

（4）

$$\boldsymbol{x}_4 = 1110$$

例

$$\boldsymbol{w} = (u_{11}, u_{12}, u_{21}, u_{22}, r_1, r_2, c_1, c_2, s)$$

の垂直水平パリティ符号を考える。このとき、次の符号から誤りを訂正せよ。

$$\boldsymbol{w}^e = 000111000$$

0	0	1
0	1	1
0	0	0

パリティの検査から、
u_{21} が誤っていることが判明する。

したがって、正しい符号は以下である。

$$\boldsymbol{w} = 010111000$$

練習

$$\boldsymbol{w} = (u_{11}, u_{12}, u_{21}, u_{22}, r_1, r_2, c_1, c_2, s)$$

の垂直水平パリティ符号を考える。このとき、このとき、次の符号から誤りを訂正せよ。

（1）

$$\boldsymbol{w}^e{}_1 = 100101011$$

（2）

$$\boldsymbol{w}^e{}_2 = 111101101$$

（3）

$$\boldsymbol{w}^e{}_3 = 100110110$$

（4）

$$\boldsymbol{w}^e{}_4 = 111001010$$

ハミング符号

垂直水平パリティ符号より効率的に冗長ビットを作り出す方法が知られている。

まず、情報ビット4ビット、冗長ビット3ビットからの7ビットのハミング符号の構成法を示す。(これを(7，4)ハミング符号という。)

$$\boldsymbol{w} = (w_1, w_2, \cdots, w_7)$$

$$= (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$$

$$= (\boldsymbol{x}, \boldsymbol{p})$$

$(7,4)$ ハミング符号という。

(n,k) 符号

n： 符号総長

k： 情報ビット長

(7，4)ハミング符号

$$\boldsymbol{w} = (w_1, w_2, \cdots, w_7)$$

$$= (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$$

$$= (\boldsymbol{x}, \boldsymbol{p})$$

冗長ビットを次の規則で定める。

$$p_1 = x_1 + x_2 + x_3$$

$$p_2 = \quad x_2 + x_3 + x_4$$

$$p_3 = x_1 + x_2 \quad + x_4$$

$(\mathrm{mod}\,2)$ での演算。

$(\mathrm{mod}\,2)$ は省略する。

検査方程式

$$\boldsymbol{w} = (w_1, w_2, \cdots, w_7) = (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$$

に対して、冗長ビットの決め方から次の関係式が成り立つ。

$$\begin{cases} w_1 + w_2 + w_3 + w_5 = 0 & (\because x_1 + x_2 + x_3 + p_1 = 0) \\ w_2 + w_3 + w_4 + w_6 = 0 & (\because x_2 + x_3 + x_4 + p_2 = 0) \\ w_1 + w_2 + w_4 + w_7 = 0 & (\because x_1 + x_2 + x_4 + p_3 = 0) \end{cases}$$

この関係式を検査方程式という。誤りが混入しなければ、
検査方程式を満足するはずである。

シンドローム

検査方程式から、誤りの位置を特定するための情報を抽出することができる。受信語が　$\boldsymbol{y} = (y_1, y_2, \cdots, y_7)$ であるとき、受信語から次式で定義される3ビット $s_1 s_2 s_3$ をシンドロームという。

$$\begin{cases} s_1 = y_1 + y_2 + y_3 + y_5 \\ s_2 = y_2 + y_3 + y_4 + y_6 \\ s_3 = y_1 + y_2 + y_4 + y_7 \end{cases}$$

受信語の誤り位置を診断するための情報

検査方程式の右辺で、送信記号 w_i を受信記号 y_i に置き換える。

誤りベクトルとシンドローム

$$\begin{cases} s_1 = y_1 + y_2 + y_3 + y_5 \\ s_2 = y_2 + y_3 + y_4 + y_6 \\ s_3 = y_1 + y_2 + y_4 + y_7 \end{cases}$$

通信路により誤りの混入

$$\therefore \begin{cases} s_1 = (w_1 + e_1) + (w_2 + e_2) + (w_3 + e_3) + (w_5 + e_5) \\ s_2 = (w_2 + e_2) + (w_3 + e_3) + (w_4 + e_4) + (w_6 + e_6) \\ s_1 = (w_1 + e_1) + (w_2 + e_2) + (w_4 + e_4) + (w_7 + e_7) \end{cases}$$

$$\therefore \begin{cases} s_1 = e_1 + e_2 + e_3 + e_5 \\ s_2 = e_2 + e_3 + e_4 + e_6 \\ s_3 = e_1 + e_2 + e_4 + e_7 \end{cases}$$

検査方程式より

ハミング符号の誤り訂正原理

7ビットからなる符号には、1ビット誤りベクトルは7個しかない。
正しい場合を含めて8通りを区別できれば良い。

e_1	e_2	e_3	e_4	e_5	e_6	e_7	s_1	s_2	s_3
1	0	0	0	0	0	0	1	0	1
0	1	0	0	0	0	0	1	1	1
0	0	1	0	0	0	0	1	1	0
0	0	0	1	0	0	0	0	1	1
0	0	0	0	1	0	0	1	0	0
0	0	0	0	0	1	0	0	1	0
0	0	0	0	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0

一般のハミング符号

(n,k) ハミング符号

符号長: $n = 2^m - 1$

情報ビット長: $k = n - m = 2^m - 1 - m$

冗長ビット長: $n - k = m$

シンドローム長: m

例

$\boldsymbol{w} = (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$、次のように冗長ビットを定める(7，4)ハミング符号を考える。

$$p_1 = x_1 + x_2 + x_3 \quad p_2 = x_2 + x_3 + x_4 \quad p_3 = x_1 + x_2 + x_4$$

このとき、次の情報ビットに対して符号語を求めよ。

$$\boldsymbol{x} = 0101$$

$$p_1 = x_1 + x_2 + x_3 = 0 + 1 + 0 = 1$$

$$p_2 = x_2 + x_3 + x_4 = 1 + 0 + 1 = 0$$

$$p_3 = x_1 + x_2 + x_4 = 0 + 1 + 1 = 0$$

$$\therefore \boldsymbol{w} = (\boldsymbol{x}, \boldsymbol{p}) = 0101100$$

練習

$\boldsymbol{w} = (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$ に対して、 次のように冗長ビットを定める(7，4)ハミング符号を考える。

$$p_1 = x_1 + x_2 + x_3 \quad p_2 = x_2 + x_3 + x_4 \quad p_3 = x_1 + x_2 + x_4$$

このとき、次の情報ビットに対して符号語を求めよ。

(1) $\boldsymbol{x}_1 = 0001$

(2) $\boldsymbol{x}_2 = 1001$

(3) $\boldsymbol{x}_3 = 1101$

(4) $\boldsymbol{x}_4 = 1110$

例

$\boldsymbol{w} = (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$ に対して、次のように冗長ビットを定める(7，4)ハミング符号を考える。

$$p_1 = x_1 + x_2 + x_3 \quad p_2 = x_2 + x_3 + x_4 \quad p_3 = x_1 + x_2 + x_4$$

このとき、次の受信語に対して誤り訂正を行え。

$$\boldsymbol{y} = (y_1, y_2, \cdots, y_7) = 0111100$$

まず、シンドロームを求める。

$$s_1 = y_1 + y_2 + y_3 + y_5 = 0 + 1 + 1 + 1 = 1$$

$$s_2 = y_2 + y_3 + y_4 + y_6 = 1 + 1 + 1 + 0 = 1$$

$$s_3 = y_1 + y_2 + y_4 + y_7 = 0 + 1 + 1 + 0 = 0$$

よって、シンドローム $\boldsymbol{s} = s_1 s_2 s_3 = 110$ より、誤りベクトルが一意に $\boldsymbol{e} = (e_1, e_2, \cdots, e_7) = 0010000$ と特定できる。
したがって、次のように誤り訂正できる。

$$\boldsymbol{y} = \left(y_1, y_2, \cdots, y_7 \right) = 0111100$$

$$\boldsymbol{w} = \boldsymbol{y} + \boldsymbol{e} = 0111100 \oplus 0010000$$

$$= 0101100$$

練習

$\boldsymbol{w} = (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$ に対して、次のように冗長ビットを定める(7，4)ハミング符号を考える。

$p_1 = x_1 + x_2 + x_3 \quad p_2 = x_2 + x_3 + x_4 \quad p_3 = x_1 + x_2 + x_4$

このとき、次の受信語に対して誤り訂正を行え。

(1)

$$\boldsymbol{y}_1 = 1001011$$

(2)

$$\boldsymbol{y}_2 = 1001001$$

(3)

$$\boldsymbol{y}_3 = 1101011$$

(4)

$$\boldsymbol{y}_4 = 0110001$$