

10. 誤り検出符号と誤り訂正符号

- 誤り検出符号
 - パリティ検査符号
- 誤り訂正符号
 - 垂直水平パリティ符号
 - ハミング符号

誤り検出符号 (パリティ検査符号)

通信路符号と冗長性

ここからは、通信路符号化において、主に2元符号を考察していく。通信路アルファベットを $B = \{0, 1\}$ とする。

(定義) 情報ビットと検査ビット

通信路符号語は、情報源符号語に加えて意識的に冗長部分を付加して構成される。情報を表す記号列を**情報部分**といい、冗長性を表す記号列を**冗長部分**という。特に、2元符号の場合、情報部分を**情報ビット**、冗長部分を**検査ビット**という。

通信路符号の数学的表現

$$\mathbf{w} = (\underbrace{w_1, w_2, \dots, w_n}_{n\text{ビット}}) = (\underbrace{x_1, \dots, x_k}_{\substack{\text{情報ビット} \\ k\text{ビット}}}, \underbrace{p_1, \dots, p_{n-k}}_{\substack{\text{冗長ビット} \\ n-k\text{ビット}}})$$
$$= (\mathbf{x}, \mathbf{p})$$

(通信路)符号語 = 情報部分 + 冗長部分

ただし、 $\mathbf{x} = (x_1, x_2, \dots, x_k)$

$\mathbf{p} = (p_1, p_2, \dots, p_{n-k})$

$$\begin{cases} 1 \leq i \leq k, w_i = x_i \in B = \{0, 1\} \\ k+1 \leq i \leq n, w_i = p_{i-k} \in B = \{0, 1\} \end{cases}$$

パリティ(偶奇性)

(定義)パリティ

符号語 $w = (w_1, \dots, w_n) \in B^n$ に対して、次式が成り立つとき、**偶数パリティ**を持つという。

$$w_1 \oplus w_2 \oplus \dots \oplus w_n = 0$$

$$\left(\sum_{i=1}^n w_i \pmod{2} = 0 \right)$$

また、次式が成り立つとき、**奇数パリティ**を持つという。

$$w_1 \oplus w_2 \oplus \dots \oplus w_n = 1$$

$$\left(\sum_{i=1}^n w_i \pmod{2} = 1 \right)$$

例

次の符号が偶数パリティを持つか、奇数パリティを持つかを判定せよ。

$$\mathbf{w} = (w_1, \dots, w_n)$$

$$= (0, 0, 1, 1, 0, 1, 0, 1)$$

$$= 00110101$$

略記法

$$\sum w_i \pmod{2} = 4 \pmod{2} = 0$$

よって、偶数パリティを持つ。

符号に現れる1の
個数が**偶数**

これ以降では、 $(\text{mod } 2)$ を省略することもある。

練習

次の式を計算せよ。

$$(1) \quad 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1$$

$$(2) \quad 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1$$

$$(3) \quad 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0$$

$$(4) \quad 3 + 4 + 7 + 5 + 8 + 9 + 1 \pmod{2}$$

$$(5) \quad 9 - 3 + 6 - 4 + 8 - 7 - 5 \pmod{2}$$

$$(6) \quad 5 + 4 - 3 - 8 - 6 - 9 + 2 \pmod{2}$$

練習

次の符号が偶数パリティを持つか、奇数パリティを持つかを判定せよ。

(1) (1,1,1,0,1,1,0,1)

(2) (0,1,0,1,1,0,1,1)

(3) (0,0,0,1,1,0,1,1)

(4) 10111000

(5) 11001100

(6) 01001100

パリティ検査(符号)

1番単純な通信路符号としてパリティ検査について考える。パリティ検査は1誤り検出符号になっている。
パリティ検査符号は以下の符号語の形式になる。

$$\mathbf{w} = \left(\underbrace{x_1, x_2, \dots, x_{n-1}}_{n-1 \text{ ビット}}, \underbrace{p}_{1 \text{ ビット}} \right)$$

情報ビット

冗長ビット

これらに関する概念を順にみていく。

パリティ検査(符号)の定義

(定義)パリティ検査(符号)

1ビットの検査ビット(パリティビット) $p \in B$ を持ち、偶数パリティだけを符号語とするような符号を(偶数)パリティ検査符号という。情報ビットを $\mathbf{x} = (x_1, \dots, x_{n-1}) \in B^{n-1}$ とすると次式が成り立つ。

$$\mathbf{w} = (x_1, \dots, x_{n-1}, p) \in B^n$$

$$x_1 \oplus \dots \oplus x_{n-1} \oplus p = 0$$

$$\therefore p = x_1 \oplus \dots \oplus x_{n-1}$$

偶数パリティ検査では、情報ビットが偶数パリティを持てばパリティビットは0で、奇数パリティを持てばパリティビットは1。

例

次の情報源符号語から、偶数パリティ検査符号を構成せよ。

$$(1) \quad \mathbf{x}_1 = (x_1^1, \dots, x_7^1) = (1, 0, 1, 1, 1, 0, 0) = 1011100$$

$$p^1 = \sum x_1^1 \pmod{2} = 4 \pmod{2} = 0$$

よって、以下のように通信路符号語が得られる。

$$\mathbf{w}_1 = (x_1^1, \dots, x_7^1, p^1) = (1, 0, 1, 1, 1, 0, 0, 0) = (1011100, 0) \\ = 10111000$$

略記法

$$(2) \quad \mathbf{x}_2 = (x_1^2, \dots, x_7^2) = (0, 1, 1, 1, 1, 0, 1) = 0111101$$

$$p^2 = \sum x_1^2 \pmod{2} = 5 \pmod{2} = 1$$

よって、以下のように通信路符号語が得られる。

$$\mathbf{w}_2 = (x_1^2, \dots, x_7^2, p^2) = (0, 1, 1, 1, 1, 0, 1, 1) = (0111101, 1) \\ = 01111011$$

練習

以下のような情報源記号が与えられているとき、偶数パリティ検査符号を求めよ。

$$(1) \quad \mathbf{x}_1 = (1, 1, 1, 0, 1, 1, 0)$$

$$(2) \quad \mathbf{x}_2 = (0, 1, 0, 1, 1, 0, 1)$$

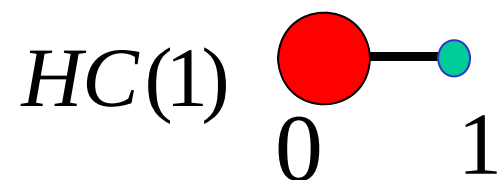
$$(3) \quad \mathbf{x}_3 = (0, 0, 0, 1, 1, 0, 1)$$

$$(4) \quad \mathbf{x}_4 = 1011100$$

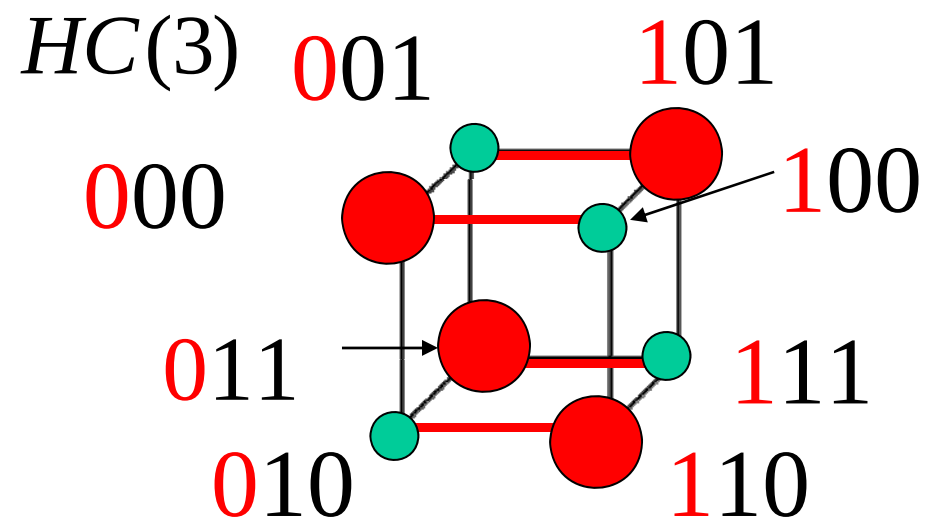
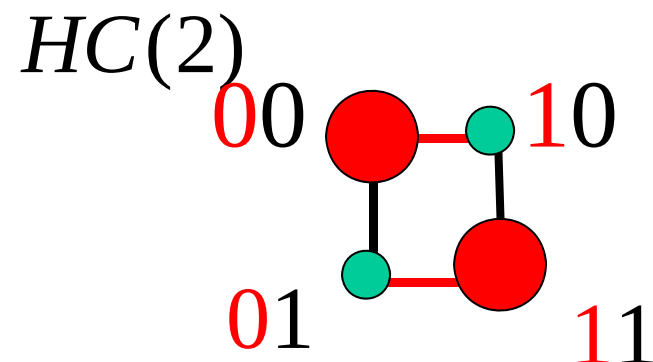
$$(5) \quad \mathbf{x}_5 = 1100110$$

$$(6) \quad \mathbf{x}_6 = 0100110$$

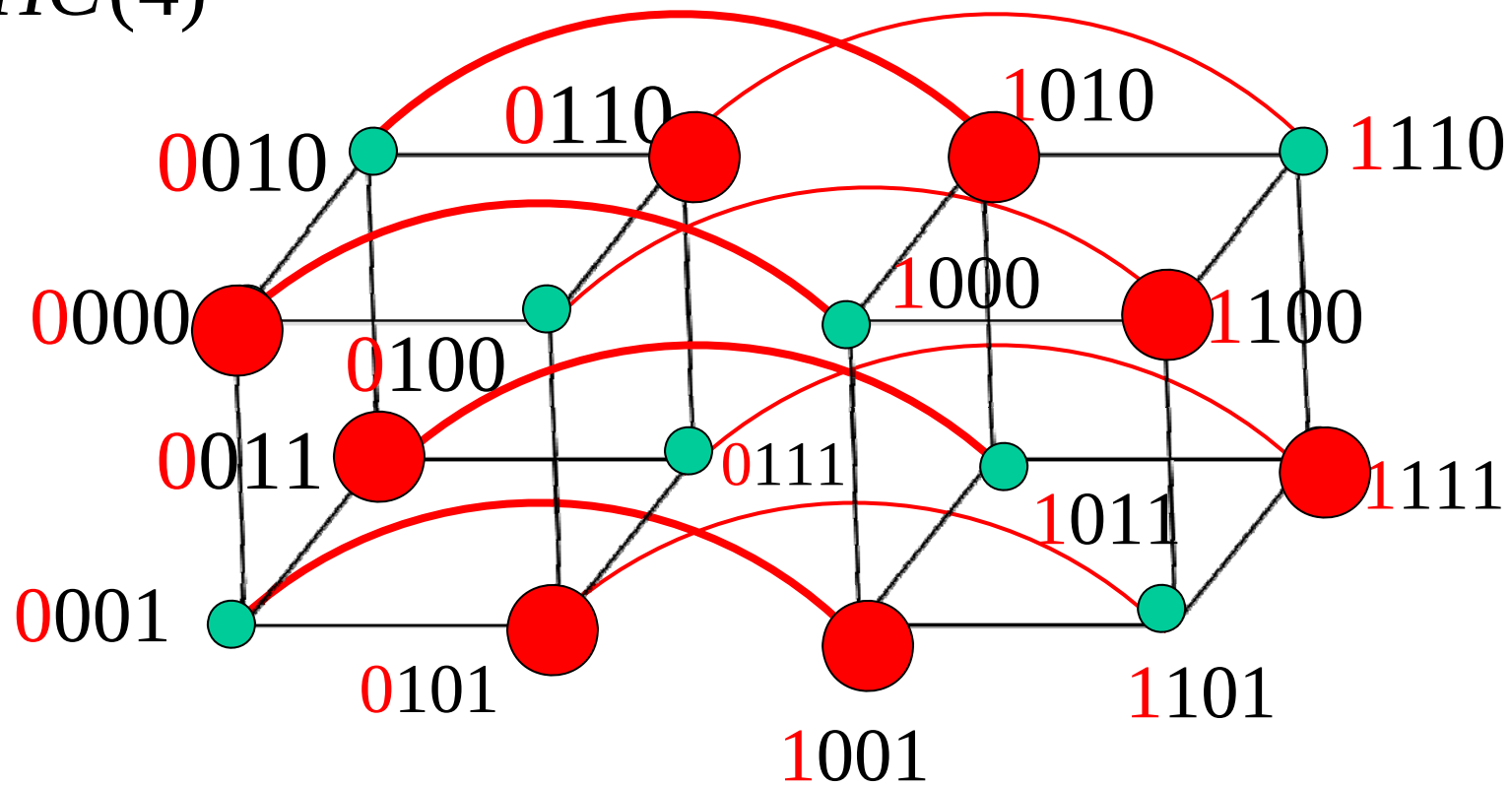
偶数パリティ符号における符号語



● : 符号語



$HC(4)$



● : 符号語

練習

情報ビットが4ビット $x \in B^4$ で、パリティビットが1ビット $p \in B$ の偶数パリティ符号 $w \in B^5$ を考える。この符号語になりえるハイパーキューブ $HC(5)$ 上頂点を図示せよ。

パリティ検査符号の誤り検出原理

性質: パリティ検査符号語間のハミング距離

偶数パリティ検査符号 W において、
各符号語 $\forall i, j, i \neq j, w_i, w_j \in W$ のハミング距離
で以下が成り立つ。

$$d_h(w_i, w_j) \geq 2(= s + 1)$$

$$(\because s = 1)$$

証明

各符号語 $w_i, w_j \in W$ は全て偶数パリティを持つので、ハミング距離が $d_h(w_i, w_j) = 1$ となることは無い。また、異なる符号語では、 $d_h(w_i, w_j) = 0$ となることも無い。

QED

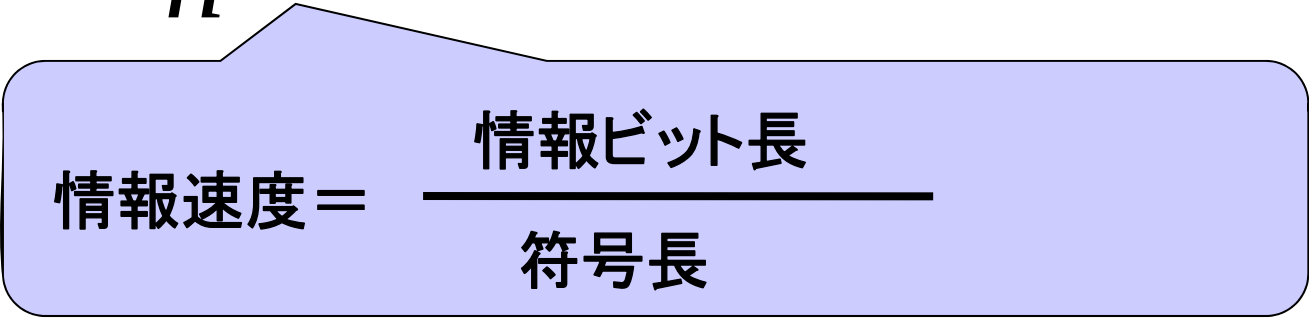
パリティ検査符号の情報伝送速度

情報ビットが $n-1$ で、検査ビットが1ビットの
 n ビットのパリティ検査符号

$$\mathbf{w} = \left(\underbrace{x_1, x_2, \dots, x_{n-1}}_{n-1 \text{ ビット}}, \underbrace{p}_{1 \text{ ビット}} \right)$$

の情報速度 R_p は次式で表わされる。

$$R_p = \frac{n-1}{n} \text{ [bit / 記号]}$$


$$\text{情報速度} = \frac{\text{情報ビット長}}{\text{符号長}}$$

誤り訂正符号

代表的誤り訂正符号

- 垂直水平パリティ符号

パリティ検査符号の拡張による誤り訂正符号

- ハミング符号

誤りベクトルの考察による誤り訂正符号

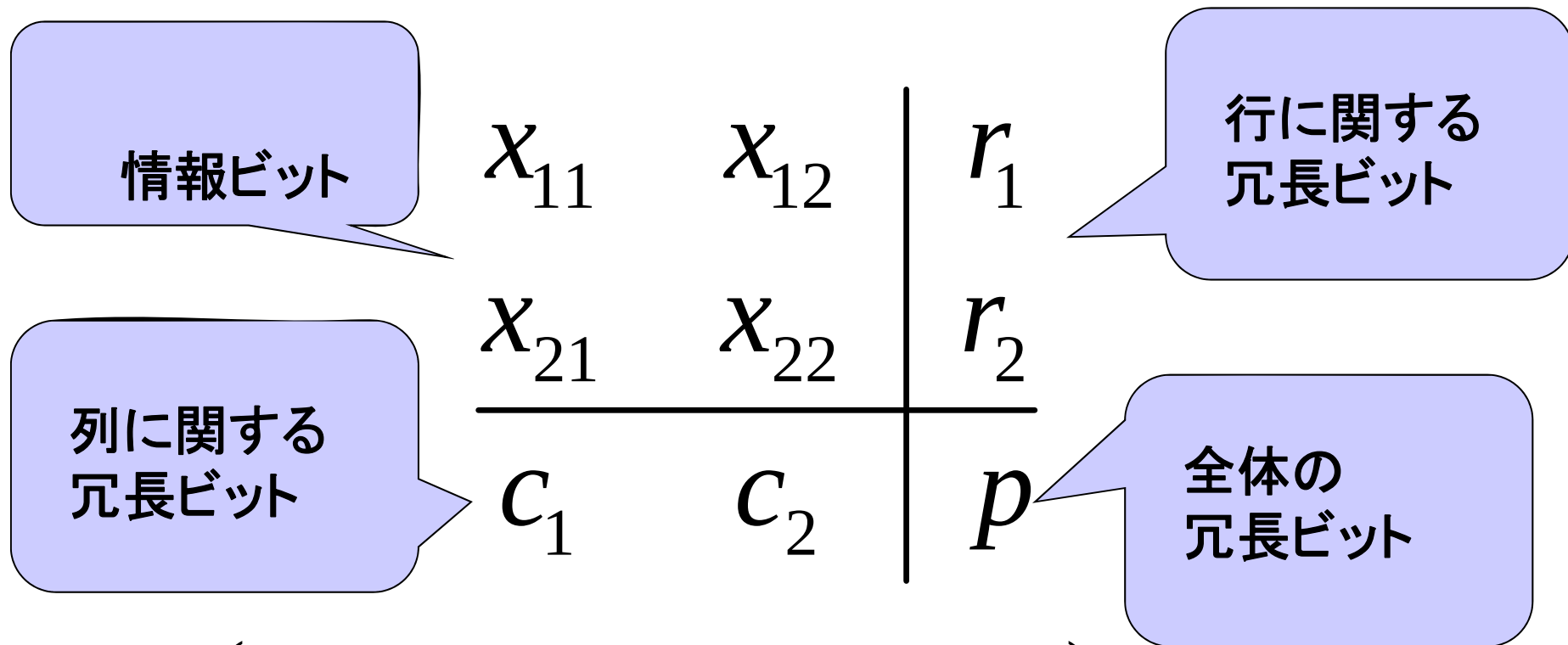
垂直水平パリティ符号

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を拡張し、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。

$$\begin{aligned}\mathbf{w} &= (w_1, w_2, \dots, w_9) \\ &= (x_1, x_2, x_3, x_4, p_1, p_2, p_3, p_4, p_5) \\ &= (\mathbf{x}, \mathbf{p})\end{aligned}$$



$$w = (x_{11}, x_{12}, x_{21}, x_{22}, r_1, r_2, c_1, c_2, p)$$

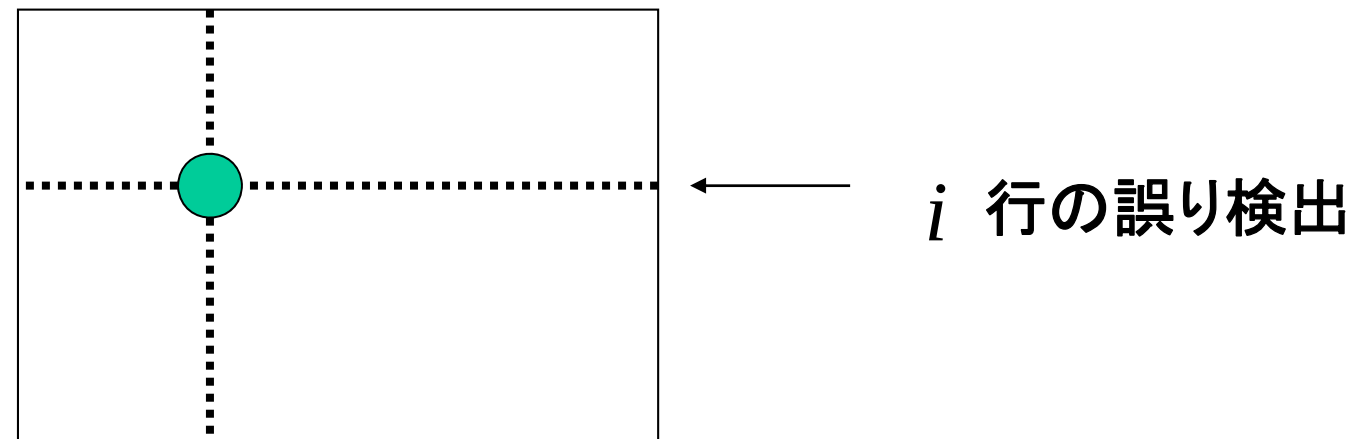
ただし、冗長ビットは次式で定める。

$$r_1 = x_{11} \oplus x_{12} \quad r_2 = x_{21} \oplus x_{22}$$

$$c_1 = x_{11} \oplus x_{21} \quad c_2 = x_{12} \oplus x_{22}$$

$$p = r_1 \oplus r_2 = c_1 \oplus c_2 = x_{11} \oplus x_{12} \oplus x_{21} \oplus x_{22}$$

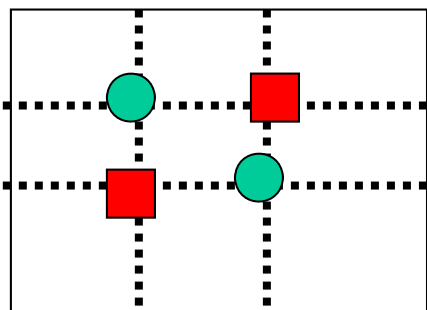
垂直水平パリティ符号における誤り訂正の原理



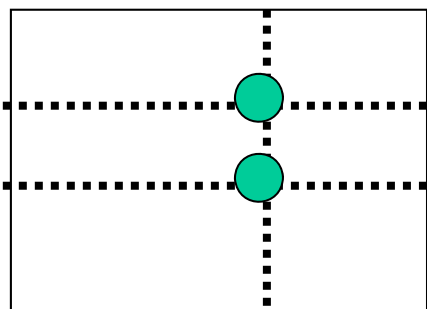
j 列の誤り検出

誤っている (i, j) 要素を
特定 → 1ビット誤り訂正

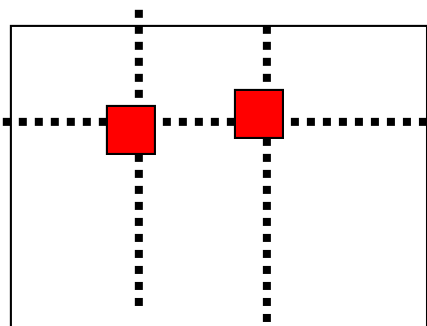
垂直水平パリティ符号における誤り訂正能力



2ビット誤りを検出可能であるが、丸と四角のどちらの組が誤りかは判定できない。

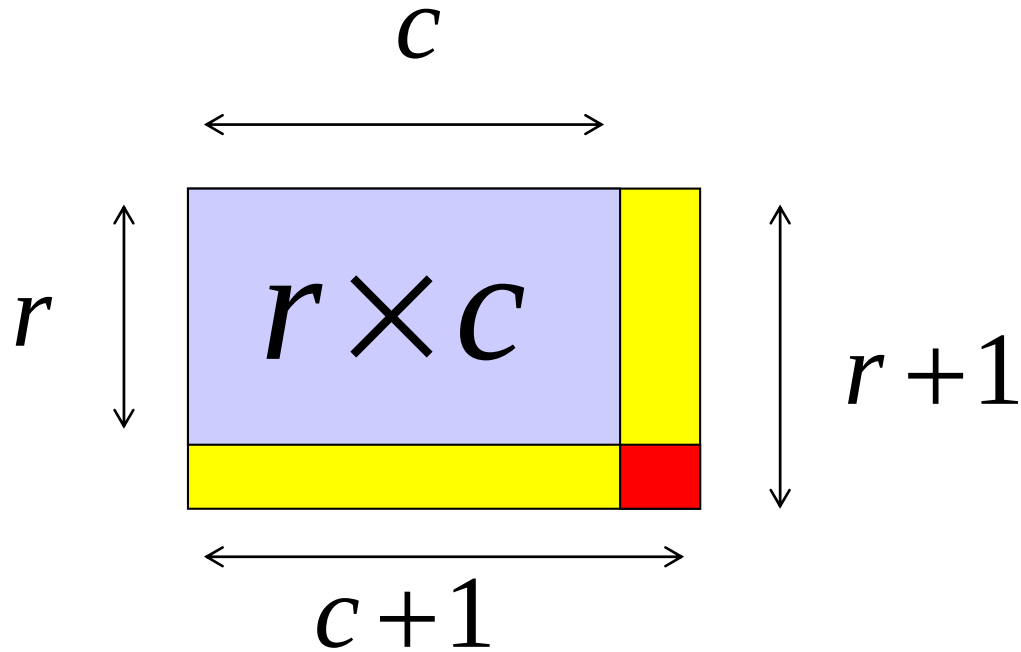


2ビット誤りを検出可能である。行は特定できるが、どの列かは特定不能。



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

$$\mathbf{w} = (x_{11}, x_{12}, x_{21}, x_{22}, r_1, r_2, c_1, c_2, p)$$

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。

$$\mathbf{x} = 0101 = x_{11}x_{12}x_{21}x_{22}$$

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

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

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

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

練習

$$w = (x_{11}, x_{12}, x_{21}, x_{22}, r_1, r_2, c_1, c_2, p)$$

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)

$$x_1 = 0001$$

(2)

$$x_2 = 1001$$

(3)

$$x_3 = 1101$$

(4)

$$x_4 = 1110$$

誤り訂正例

$$\mathbf{w} = (x_{11}, x_{12}, x_{21}, x_{22}, r_1, r_2, c_1, c_2, p)$$

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。

$$\mathbf{y} = \mathbf{w} + \mathbf{e} = 000111000$$

0	0	1
0	1	1
0	0	0

パリティの検査から、
 x_{21} が誤っていることが判明する。

行ベクトル毎、列ベクトル毎にパリティ検査を行い、誤りっている行と列の交差している箇所が誤りである。

誤りベクトルと、正しい符号は以下である。

$$\mathbf{e} = 010000000 \quad \mathbf{w} = \mathbf{y} + \mathbf{e} = 010111000$$

練習

$$w = (x_{11}, x_{12}, x_{21}, x_{22}, r_1, r_2, c_1, c_2, p)$$

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)

$$y_1 = 100101011$$

(2)

$$y_2 = 111101101$$

(3)

$$y_3 = 100110110$$

(4)

$$y_4 = 111001010$$

垂直水平パリティ符号の符号語間距離

$$\mathbf{w} = (x_{11}, x_{12}, x_{21}, x_{22}, r_1, r_2, c_1, c_2, p)$$

で定義される垂直水平パリティ符号の各符号語間の距離において、次式がなりたつ。

$$\forall i, j, i \neq j \quad d_h(\mathbf{w}_i, \mathbf{w}_j) \geq 3$$

$$\mathbf{w}_i = (\mathbf{x}_i, \mathbf{p}_i) \quad \mathbf{w}_j = (\mathbf{x}_j, \mathbf{p}_j) \quad \text{において、}$$

$d_h(\mathbf{x}_i, \mathbf{x}_j) = 1$ のとき、行と列の検査1ビットずつ異なる。

$d_h(\mathbf{x}_i, \mathbf{x}_j) = 2$ のとき、少なくとも行と列のどちらかが、検査ビットが2か所異なる。

垂直水平パリティ符号の情報速度

$$w = (x_{11}, x_{12}, x_{21}, x_{22}, r_1, r_2, c_1, c_2, p)$$

で定義される 2×2 の情報ビットを持つ垂直水平パリティ符号の情報速度 $R_{VHP}(2 \times 2)$ は、次式で表わされる。

$$R_{VHP}(2 \times 2) = \frac{4}{9} \quad [bit / \text{記号}]$$

より一般に、 $r \times c$ の情報ビットを持つ垂直水平パリティ符号の情報速度 $R_{VHP}(r \times c)$ は、次式で表らわされる。

$$R_{VHP}(r \times c) = \frac{rc}{(r+1)(c+1)} \quad [bit / \text{記号}]$$

ハミング符号

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。)

$$\mathbf{w} = (w_1, w_2, \dots, w_7)$$

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

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

(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

$$\mathbf{w} = (w_1, w_2, \dots, w_7)$$

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

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

冗長ビットを次の規則で定める。

$$p_1 = x_1 + x_2 + x_3$$

$$p_2 = x_2 + x_3 + x_4$$

$$p_3 = x_1 + x_2 + x_4$$

(mod 2) での演算。

(mod 2) は省略する。

なぜ、この式で定義するかは、後で示す。

検査方程式

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

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 $y = (y_1, y_2, \dots, y_7)$ 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δρο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

$$\therefore \begin{cases} s_1 = (w_1 + e_1) + (w_2 + e_2) + (w_3 + e_3) + (w_5 + e_5) \\ s_2 = (w_2 + e_2) + (w_3 + e_3) + (w_4 + e_4) + (w_6 + e_6) \\ s_3 = (w_1 + e_1) + (w_2 + e_2) + (w_4 + e_4) + (w_7 + e_7) \end{cases}$$

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

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

各列がシンδροームの定義式に対応する。

$$s_3 = e_1 + e_2 + e_4 + e_7$$

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

各行の誤りベクトルに2進数を割り当てる。

例

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

$$x = 0101$$

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

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

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

$$\therefore w = (x, p) = 0101100$$

練習

$w = (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$ 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) $x_1 = 0001$

(2) $x_2 = 1001$

(3) $x_3 = 1101$

(4) $x_4 = 1110$

例

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

$$y = (y_1, y_2, \dots, y_7) = 0111100$$

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

$$\mathbf{y} = (y_1, y_2, \dots, y_7) = 0111100$$

$$\begin{aligned} \mathbf{w} &= \mathbf{y} + \mathbf{e} = 0111100 \oplus 0010000 \\ &= 0101100 \end{aligned}$$

練習

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

$$y_1 = 1001011$$

(2)

$$y_2 = 1001001$$

(3)

$$y_3 = 1101011$$

(4)

$$y_4 = 0110001$$

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δροーム長: m

ちなみに、符号 $W = \{000, 111\}$ は、
 $n = 3, m = 2, k = 1$ となり、
(3、1)ハミング符号。

練習

2ビットのシンδροームを持つ、 $(3,1)$ ハミング符号を定義せよ。

ハミング符号の符号語間距離

$w = (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$ 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、次式が成り立つ。

$$\forall i, j, i \neq j \quad d_h(w_i, w_j) \geq 3$$

$w_i = (x_i, p_i)$ $w_j = (x_j, p_j)$ において、

$d_h(x_i, x_j) = 1$ のとき、定義より少なくとも冗長ビットが2ビットは異なる。(例えば、 x_1 が異なれば、 p_1 と p_3 も異なる。)

$d_h(x_i, x_j) = 2$ のとき、定義より少なくとも冗長ビットが1ビット異なる。(例えば、 x_1 と x_2 が異なれば、 p_2 も異なる。)

ハミング符号の情報速度

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

で定義される(7, 4)ハミング符号の情報速度 $R_H(7, 4)$ は、次式で表わされる。

$$R_H(7, 4) = \frac{4}{7} \text{ [bit / 記号]}$$

より一般に、シンドローム長が m のハミング符号は、情報ビットが、

$$n = 2^m - 1$$

冗長ビットが

$$k = n - m = 2^m - m - 1$$

の $(2^m - 1, 2^m - m - 1)$ ハミング符号になり、情報速度は次式表わされる。

$$R_H(2^m - 1, 2^m - m - 1) = \frac{2^m - m - 1}{2^m - 1} \text{ [bit / 記号]}$$