

(通信)符号理論入門 (誤り検出と誤り訂正) (9章)

1

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。

2

通信路符号の数学的表現

$$\mathbf{u} = (\underbrace{u_1, u_2, \dots, u_n}_{n\text{ビット}}) = (\underbrace{x_1, \dots, x_k}_{\text{情報ビット}}, \underbrace{p_1, \dots, p_{n-k}}_{\text{冗長ビット}})$$

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

符号語=情報部分+冗長部分

ただし、

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

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

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

3

パリティ検査(符号)

まず、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。

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

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。

4

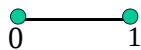
ハイパーキューブ

(定義)ハイパーキューブ

次のように再帰的に定義される構造をハイパーキューブという。 n 次元のハイパーキューブを $HC(n)$ と書く。

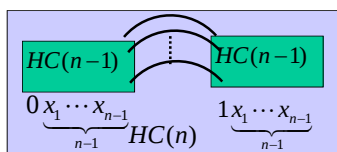
(1)1次元のハイパーキューブ(基礎)

線分 $HC(1)$



(2)次元のハイパーキューブ(帰納)

$HC(n-1)$ と $HC(n-1)$ を対応する頂点同士、辺で結び、最上位ビットだけが異なるように0, 1を割り振る。



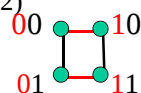
5

例

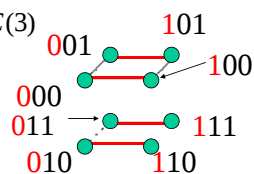
$HC(1)$



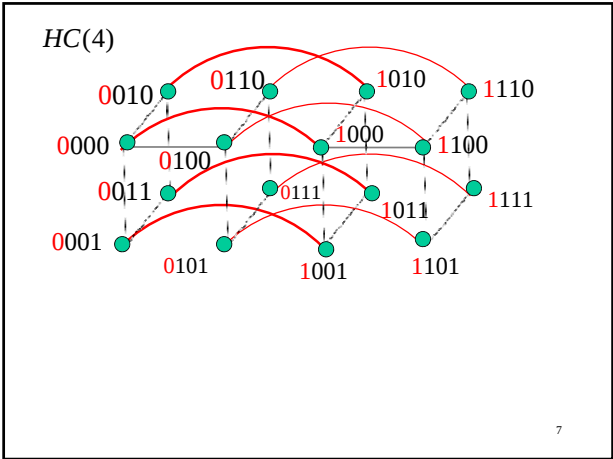
$HC(2)$



$HC(3)$



6



練習

HC(5) を図示せよ。

排他的論理和

(定義) 排他的論理和

次の真理値で定められる論理関数を排他的論理和という。
論理変数 X と論理変数 y の排他的論理和を $x \oplus y$ と書く。

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

排他的論理和は2進数の加算、減算に対応する。

2を法とする計算

$X \pmod 2$ で X を2で割った余りを意味する。(この計算を2を法とする計算という。)

$x + y \pmod 2$ を考える。これは、以下のように計算できる。

$x \pmod 2$	$y \pmod 2$	$x + y$	$x + y \pmod 2$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	2	0

排他的論理和と同一

$x - y \pmod 2$ を考える。これは、以下のように計算できる。

$x \pmod 2$	$y \pmod 2$	$x - y$	$x - y \pmod 2$
0	0	0	0
0	1	-1	1
1	0	1	1
1	1	0	0

排他的論理和と同一。、2を法とする加算とも同一。

$-1 \pmod 2 = 1$

練習

次の式を計算せよ。

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

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

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

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

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

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

パリティ(偶奇性)

(定義)パリティ

符号語 $\mathbf{u} = (u_1, \dots, u_n) \in B^n$ 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。

$$u_1 \oplus u_2 \oplus \dots \oplus u_n = 0$$

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

また、次式が成り立つとき、**奇数パリティ**を持つという。

$$u_1 \oplus u_2 \oplus \dots \oplus u_n = 1$$

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

13

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。

$$\mathbf{u} = (u_1, \dots, u_n) = (0, 0, 1, 1, 0, 1, 0, 1)$$

$$= 00110101$$

略記法

$$\sum u_i \pmod{2} = 0$$

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。

14

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

15

パリティ検査(符号)

(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。

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

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

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

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。

16

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。

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

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

よって、以下のように通信路符号語が得られる。

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

$$= (1011100, 0)$$

略記法

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

$$p^2 = \sum x_i^2 \pmod{2} = 1$$

よって、以下のように通信路符号語が得られる。

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

$$= (0111101, 1)$$

17

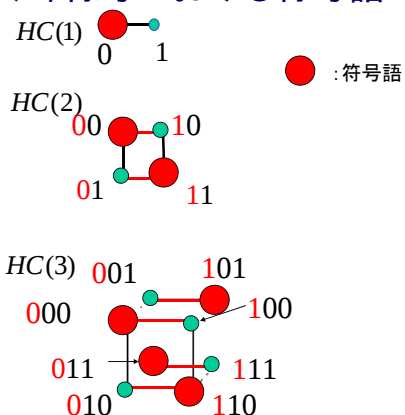
練習

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) $\mathbf{x}_1 = (1, 1, 1, 0, 1, 1, 0)$
- (2) $\mathbf{x}_2 = (0, 1, 0, 1, 1, 0, 1)$
- (3) $\mathbf{x}_3 = (0, 0, 0, 1, 1, 0, 1)$
- (4) $\mathbf{x}_4 = 1011100$
- (5) $\mathbf{x}_5 = 1100110$
- (6) $\mathbf{x}_6 = 0100110$

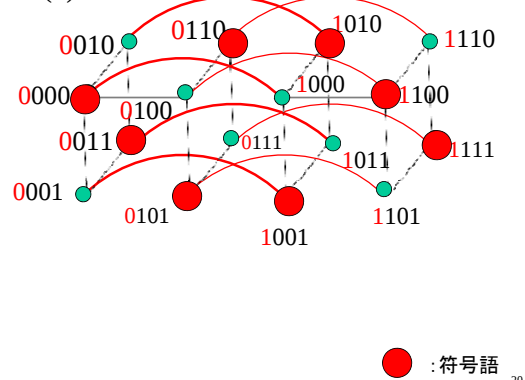
18

偶数パリティ符号における符号語



19

HC(4)



20

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 $u \in B^5$ 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。

21

ハミング距離

(定義)ハミング距離

長さ n の2元符号 (n 次元ブールベクトル)

$$x = (x_1, \dots, x_n) \in B^n$$

$$y = (y_1, \dots, y_n) \in B^n$$

に対して、次式で定義される距離 $h(x, y)$ をハミング距離という。

$$h(x, y) = \sum_{i=1}^n \delta(x_i, y_i)$$

異なる
ビットの
総数

ただし、

$$\delta(x_i, y_i) = \begin{cases} 0 & x_i = y_i \\ 1 & x_i \neq y_i \end{cases}$$

ビットが異なるとき
に1で等しいとき0。

22

ハミング距離は次のようにも書ける。

$$h(x, y) = \sum_{i=1}^n |x_i - y_i|$$

$$h(x, y) = \sum_{i=1}^n (x_i - y_i)^2$$

23

例

次の2つの系列のハミング距離を求めよ。

$$x = 100101 \in B^6$$

$$y = 101110 \in B^6$$

解

$$\begin{array}{c} 100101 \\ \downarrow \downarrow \downarrow \\ 101110 \end{array}$$

$$h(x, y) = 3$$

24

練習

次のハミング距離を求めよ。

(1)

$$h(011, 110)$$

(2)

$$h(1100, 0110)$$

(3)

$$h(011001, 101010)$$

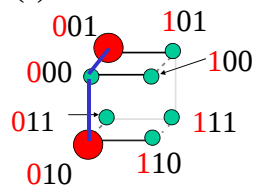
(4)

$$h(00011011, 10010110)$$

25

ハミング距離とハイパーキューブ

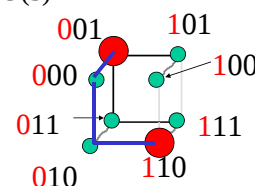
HC(3)



$$h(001, 010) = 2$$

ハイパーキューブ上での
経路長がハミング距離

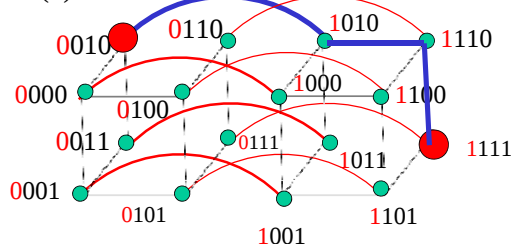
HC(3)



$$h(001, 110) = 3$$

26

HC(4)



$$h(0010, 1111) = 3$$

27

練習

次の2つの系列 $x = 1100 \in B^4, y = 1011 \in B^4$
をハイパーキューブ $HC(4)$ 上に図示し、ハミング距離
を求めよ。

28

距離の3公理

(公理) 距離の公理

任意の n 次元ベクトル $x, y, z \in K^n, (K = B \text{ や } \mathbb{R} \text{ や } \mathbb{C})$
に対して、次の3つの性質を満たす関係 $d: K^n \times K^n \rightarrow \mathbb{R}$
を距離という。

(1) $d(x, x) = 0$ 逆に、 $d(x, y) = 0$ なら $x = y$ (2) $d(x, y) = d(y, x)$

同一地点間の距離は0

距離は対称的

(3) $d(x, y) + d(y, z) \geq d(x, z)$

三角不等式

ユークリッド距離だけが距離なのでは
ない。様々な距離の概念がある。

29

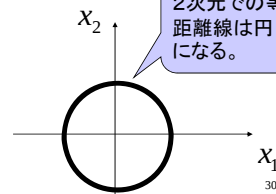
様々な距離1 (ユークリッド距離)

$$x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{R}^n$$

$$d_2(x, y) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2}$$

最もよく用いられる
距離

$$= \left\{ \sum_{i=1}^n |x_i - y_i|^2 \right\}^{\frac{1}{2}}$$

2次元での等
距離線は円
になる。

30

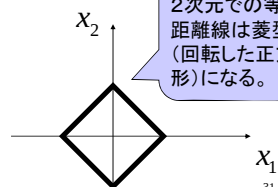
様々な距離2(マンハッタン距離)

$$\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$$

$$d_1(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n |x_i - y_i|$$

碁盤の目状の町での最短路。

$$= \left\{ \sum_{i=1}^n |x_i - y_i|^1 \right\}^{\frac{1}{1}}$$



31

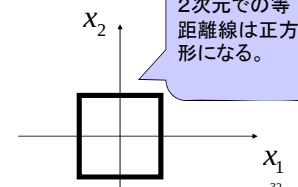
様々な距離3(L_∞ 距離)

$$\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$$

$$d_\infty(\mathbf{x}, \mathbf{y}) = \max_{i=1}^n \{|x_i - y_i|\}$$

ある軸での最大値

$$= \lim_{p \rightarrow \infty} \left\{ \sum_{i=1}^n |x_i - y_i|^p \right\}^{\frac{1}{p}}$$



32

様々な距離4(L_p 距離)

$$\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$$

$$d_p(\mathbf{x}, \mathbf{y}) = \left\{ \sum_{i=1}^n |x_i - y_i|^p \right\}^{\frac{1}{p}}$$

マンハッタン距離は別名 L_1 距離ともいう。

ユークリッド距離は別名 L_2 距離ともいう。

33