情報理論(No.8)　　2016/11/12

今後の講義予定

11／19:通常(第9回)

11／26:通常(第10回)

12／03:通常(第11回)

12／10:通常(第12回)

講義目次

- 11. 誤り訂正符号の基礎
  - 11.7 単一誤り訂正符号：(7，４)ハミング符号
  - 11.8 ハミング符号の復号法
  - 11.9 ハミング符号化と復号の例
  - 11.10 ハミング符号の一般化：パリティ検査符号
  - 11.11 パリティ検査行列
  - 11.12 ハミング符号の符号器
  - 11.13 ハミング符号の復号器
- 12. 誤り訂正符号(ブロック符号)
  - 12.1 より一般的な誤り訂正符号
  - 12.2 誤り訂正符号の分類
  - 12.3 符号理論(誤り訂正符号)の講義範囲
  - 12.4 線形符号
  - 12.5 線形符号：水平垂直パリティ検査符号
  - 12.6 符号長n＝7，情報点k＝4の符号

講義目次

- 12. 誤り訂正符号(ブロック符号)
  - 12.7 線形符号の生成行列
  - 12.8 既約梯形標準形への変換法
  - 12.9 (n=7, k=4) ハミング符号の行列G, H
  - 12.10 符号化
  - 12.11 復号化
  - 12.12 ハミング符号の一般化
  - 12.13 パリティ検査符号の効率的復号法
  - 12.14 パリティ検査符号の剰余類分割
  - 12.15 Gから符号語の生成
  - 12.16 剰余類分割表
  - 12.17 線形符号を群符号として見る
  - 12.18 群
  - 12.19 群としての線形符号
  - 12.20 剰余類展開

11.7 単一誤り訂正符号：(7, 4) ハミング符号

- 情報点数k=4、符号長n=7の符号。（検査点数m=3）

【ハミング符号の構成例】

- 情報点を (x_1, x_2, x_3, x_4) ,検査点を (c_1, c_2, c_3) とし、c_1, c_2, c_3を次のように選ぶ。加算は2を法とする。

$$c_1 = x_1 + x_2 + x_3 \pmod 2$$
$$c_2 = x_1 + x_2 + x_4 \pmod 2$$
$$c_3 = x_1 + x_3 + x_4 \pmod 2$$

c_1, c_2, c_3を求める式

mod 2加算の性質($x + x = 0$) より、

$$x_1 + x_2 + x_3 + c_1 = 0$$
$$x_1 + x_2 + x_4 + c_2 = 0$$
$$x_1 + x_3 + x_4 + c_3 = 0$$

$x_1, x_2, x_3, x_4, c_1, c_2, c_3$に関する連立方程式

11.8 ハミング符号の復号法

$$x_1 + x_2 + x_3 + c_1 = q_1$$
$$x_1 + x_2 + x_4 + c_2 = q_2$$
$$x_1 + x_3 + x_4 + c_3 = q_3$$

} 式H

と置くと、**誤りが発生するとq_1, q_2, q_3の値が変わる。**

下記の検査表に従って、誤り個所を検査する。

（誤り文字）	q_1	q_2	q_3	（2進数表記）
x_1	1	1	1	(7)
x_2	1	1	0	(6)
x_3	1	0	1	(5)
x_4	0	1	1	(3)
c_1	1	0	0	(4)
c_2	0	1	0	(2)
c_3	0	0	1	(1)
誤りなし	0	0	0	(0)

問題：
x_1～c_3に関する式Hをどう作るか？

11.9 ハミング符号化と復号の例

- 情報点として下記のものがあると、

  i_1＝0010（x_1=0, x_2=0, x_3=1, x_4=0）

  i_2＝0110（x_1=0, x_2=1, x_3=1, x_4=0）

  i_3＝1100（x_1=1, x_2=1, x_3=0, x_4=0）

- 検査点を次の式H、

  $x_1 + x_2 + x_3 + c_1 = 0$

  $x_1 + x_2 + x_4 + c_2 = 0$

  $x_1 + x_3 + x_4 + c_3 = 0$

  } 式H

  により付け加えると、下記の符号語（w_1,w_2,w_3）が得られる。

  w_1=0010101

  w_2=0110011

  w_3=1100001

  ⇐ 上のi_1, i_2, i_3に対する符号語である

- 受信系列0100011に対して、（q_1, q_2, q_3）＝（1, 0, 1）が得られるので、x_3が誤りと判定され、0110011と復号される

  どの符号語とも違うので誤りが起こっていることが分かる

11.10 ハミング符号の一般化：パリティ検査符号

$$x_1 + x_2 + x_3 + c_1 = 0$$
$$x_1 + x_2 + x_4 + c_2 = 0$$
$$x_1 + x_3 + x_4 + c_3 = 0$$

$c_1, c_2, c_3 \rightarrow x_5, x_6, x_7$と置き直すと変数$x_1, \cdots, x_7$に関する式になる

は、一般化すると、

$$h_{11}x_1+h_{12}x_2+\ldots+h_{1n}x_n = 0$$
$$h_{21}x_1+h_{22}x_2+\ldots+h_{2n}x_n = 0$$
$$\ldots$$
$$h_{m1}x_1+h_{m2}x_2+\ldots+h_{mn}x_n = 0$$

$\pmod 2$

⇒ **パリティ検査方程式**という

と書ける。

符号語$(x_1, x_2, \ldots, x_n)$はこの線形方程式を満たす集合になる。

$$H=\begin{pmatrix} h_{11} & h_{12} & \ldots & h_{1n} \\ \ldots & & & \\ h_{m1} & h_{m2} & \ldots & h_{mn} \end{pmatrix}$$

行数m=検査点数

列数n=符号長

⇒ **パリティ検査行列**という（m行n列）

11.11 パリティ検査行列

- 符号語 x に対して、$xH^T = Hx^T = 0$を満足する行列Hを**パリティ検査行列**と呼ぶ（T：転置行列）。（正確には**既約梯形標準形**のH）

$$H = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1k} & 1 & 0 & 0 & \ldots & 0 \\ p_{21} & p_{22} & \cdots & p_{2k} & 0 & 1 & 0 & \ldots & 0 \\ \ldots & & & & & & & & \\ p_{n-k,1} & p_{n-k,2} & \cdots & p_{n-k,k} & 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

これは、符号語 xが誤っていないかを検査する行列。
誤りがなければ、$xH^T = Hx^T = 0$が成立する。

（注）Tは転置を示す． 小文字(t)でH^tとも表記する

11.11 パリティ検査行列：例とその性質

- パリティ検査行列Hは、いくつかの変形が有り得る
  - 情報点と検査点の位置を変えると、別のH’になる

$$H' = \begin{pmatrix} 1\,0\,1\,0\,1\,0\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \end{pmatrix}$$

- Hを並べ替えて、下記の形にしたものを**既約梯形標準形**という

$$H = \overset{m}{\updownarrow} \left(\begin{array}{c:c} I_m & P \end{array} \right) \quad \text{又は} \quad \left(\begin{array}{c:c} P & I_m \end{array} \right)$$

I_mは下記の形の対角行列

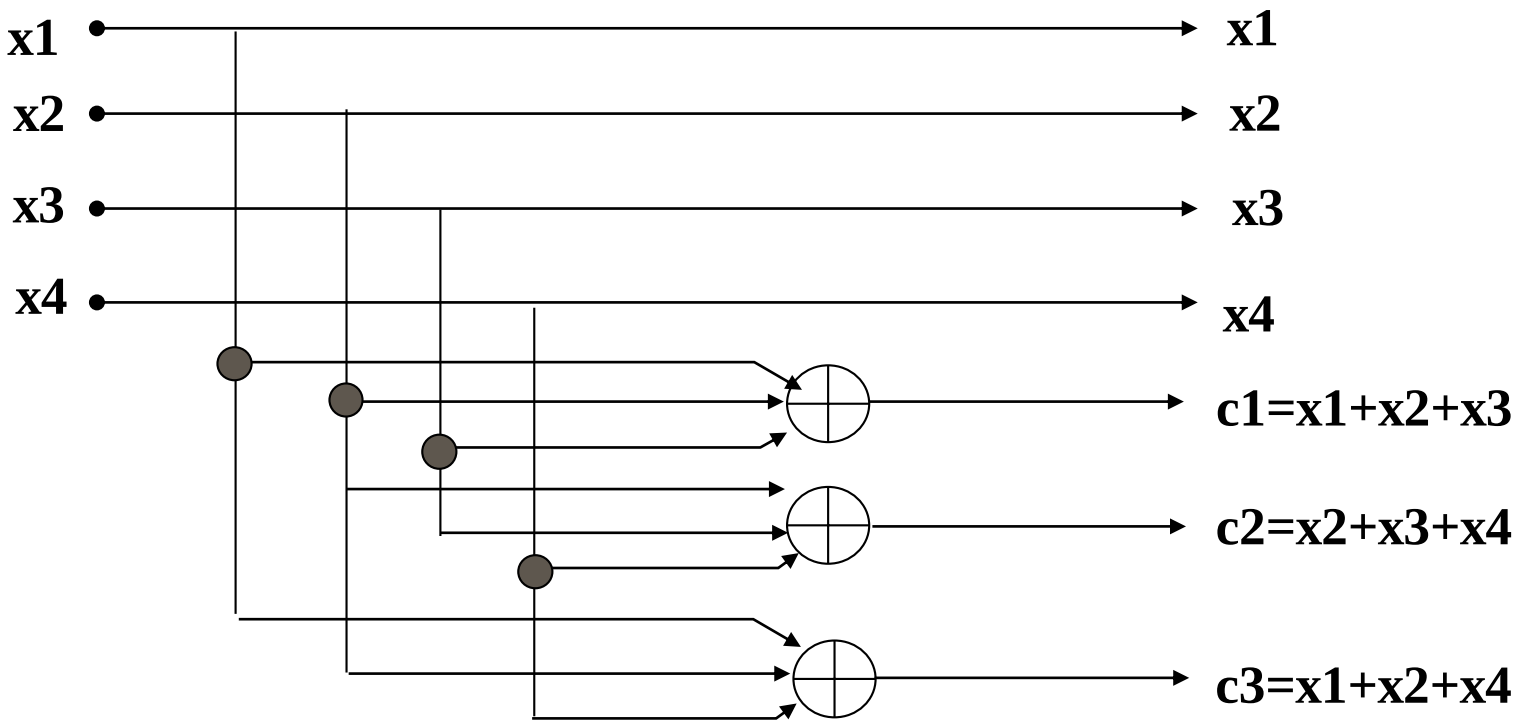
m　　n−m=k

$$I_m = \begin{pmatrix} 1\,0\,0\cdots0 \\ 0\,1\,0\cdots0 \\ \cdots \\ 0\,0\cdots1 \end{pmatrix}$$

11.12 ハミング符号の符号器

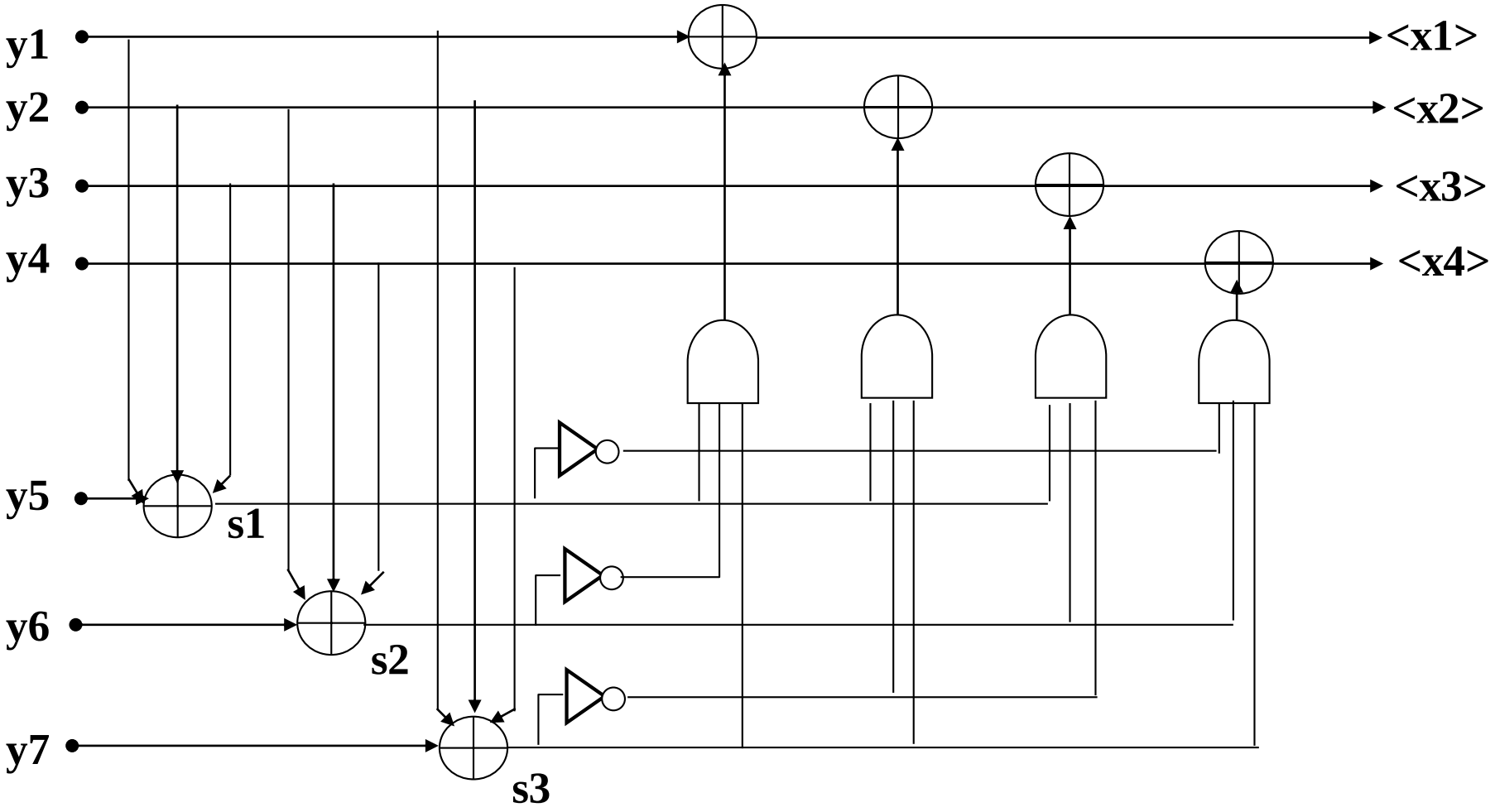
$$\left.\begin{aligned} x_1 + x_2 + x_3 + c_1 &= 0 \\ x_2 + x_3 + x_4 + c_2 &= 0 \\ x_1 + x_2 + x_4 + c_3 &= 0 \end{aligned}\right\} \quad \text{(mod 2で加算)}$$

で構成される(7,4)ハミング符号の符号器は下記の通り:



(備考) ⊕ **: 加算器 (mod 2での）**

11.13 ハミング符号の復号器



12. 誤り訂正符号(ブロック符号)

12.1 より一般的な誤り訂正符号
12.2 誤り訂正符号の分類
12.3 符号理論(誤り訂正符号)の講義範囲
12.4 線形符号
12.5 線形符号:水平垂直パリティ検査符号
12.6 符号長n＝7, 情報点k＝4の符号
12.7 線形符号の生成行列
12.8 既約梯形標準形への変換法
12.9 (n=7, k=4) ハミング符号の行列G, H
12.10 符号化
12.11 復号化
12.12 ハミング符号の一般化
12.13 パリティ検査符号の効率的復号法
12.14 パリティ検査符号の剰余類分割
12.15 Gから符号語の生成
12.16 剰余類分割表
12.17 線形符号を群符号として見る
12.18 群
12.19 群としての線形符号
12.20 剰余類展開

12.1 より一般的な誤り訂正符号

- ハミング符号以外にどのような符号があるか
- それらは、どのように構成するか（符号化するか）
- それらは、どのように復号化するか

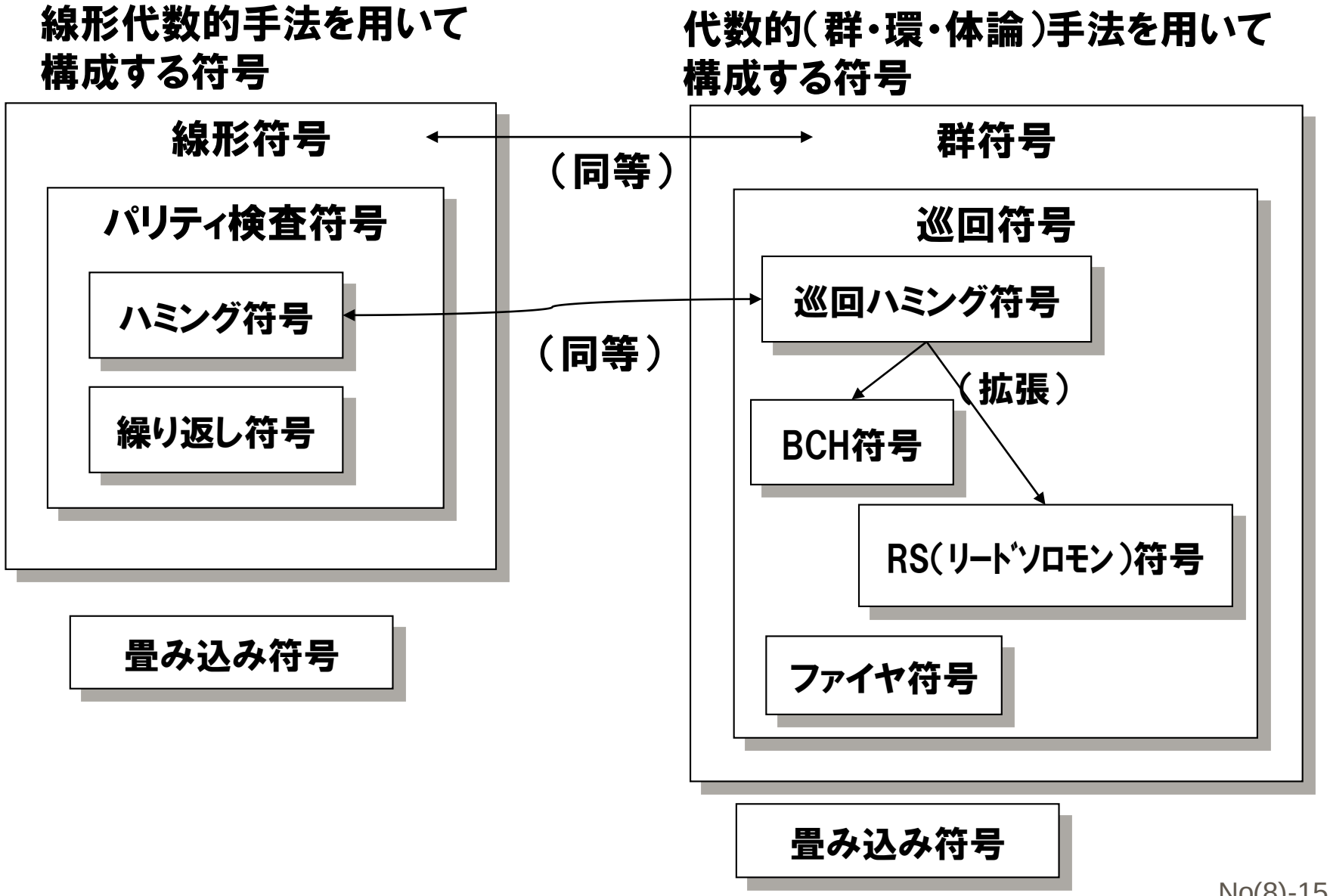
12.2 誤り訂正符号の分類

- ブロック符号
  - 線形符号
    - パリティ検査符号
      - 水平垂直パリティ検査符号
      - 繰り返し符号
    - ハミング符号
    - 巡回符号（サイクリック符号）
      - 巡回ハミング符号
      - BCH符号
      - リードソロモン（RS）符号
  - 非線形符号
- 畳込み符号

符号理論：

誤り訂正（および検出）符号を扱う情報理論の一分野を符号理論という

12.3 符号理論(誤り訂正符号)の講義範囲



12.4 線形符号

情報系列(情報点) $i = (i_1, i_2, i_3, \ldots, i_k)$ を符号語 $x = (i_1, i_2, i_3, \ldots, i_k, p_1, p_2, \ldots, p_{n-k})$ に符号化するとき、$p_1, p_2, \ldots, p_{n-k}$ を検査点と呼ぶ。

線形符号とは検査点が情報点の線形関数で与えられる符号：

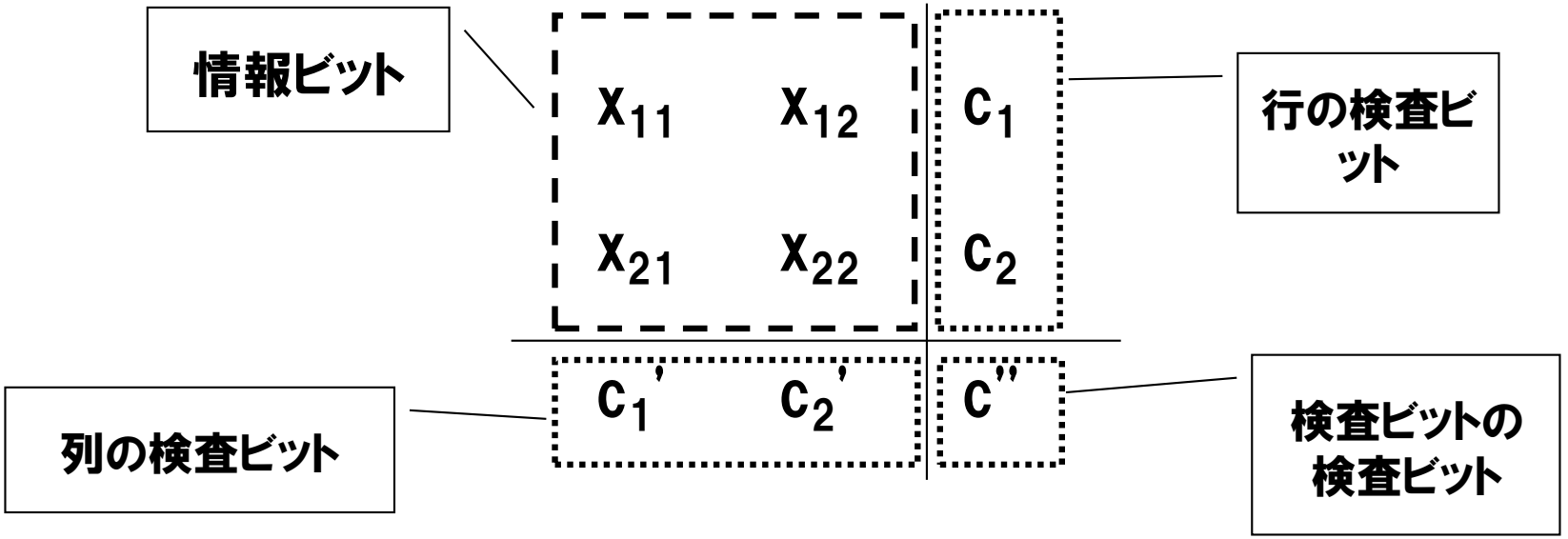
$$\left.\begin{aligned} p_1 &= p_{11} i_1 + p_{12} i_2 + \ldots + p_{1k} i_k \\ p_2 &= p_{21} i_1 + p_{22} i_2 + \ldots + p_{2k} i_k \\ &\ldots \\ p_{n-k} &= p_{n-k,1} i_1 + p_{n-k,2} i_2 + \ldots + p_{n-k,k} i_k \end{aligned}\right\} \pmod 2$$

または、左辺を右辺に移項するとmod 2なので0になり、

$$\left.\begin{aligned} p_{11} i_1 + p_{12} i_2 + \ldots + p_{1k} i_k + p_1 &= 0 \\ p_{21} i_1 + p_{22} i_2 + \ldots + p_{2k} i_k + p_2 &= 0 \\ &\ldots \\ p_{n-k,1} i_1 + p_{n-k,2} i_2 + \ldots + p_{n-k,k} i_k + p_{n-k} &= 0 \end{aligned}\right\} \pmod 2$$

12.5 線形符号：水平垂直パリティ検査符号

- パリティ検査ビットを、2方向（行方向、列方向）に対して「行、列の1の数が偶数になるよう」追加する （偶パリティ検査符号）
  - $c_1=x_{11}+x_{12}$　　$c_2=x_{21}+x_{22}$
  - $c_1'=x_{11}+x_{21}$　　$c_2'=x_{12}+x_{22}$
- さらに、検査ビットの行の1の数が偶数になるよう、検査ビットの検査ビットを追加する
  - $c''=c_1+c_2=x_{11}+x_{12}+x_{21}+x_{22}=c_1'+c_2'$

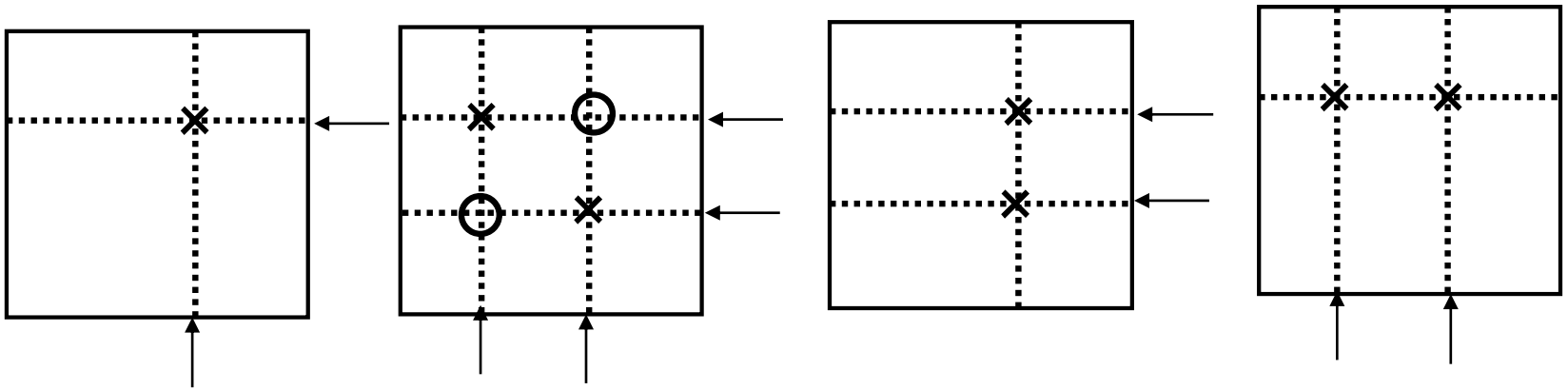


12.5 水平垂直パリティ検査符号: 誤り訂正能力

パリティ検査ビットを調べることで、

- 1個の誤り訂正が可能　⇒　パターン(ａ)
- 2個の誤り検出が可能　⇒　パターン(ｂ)(ｃ)(ｄ)

理由：誤りが生じた箇所の検査ビットが1、となる



(ａ)誤り訂正可能
検査行、列の共通に含まれている情報ビットが誤りと判定

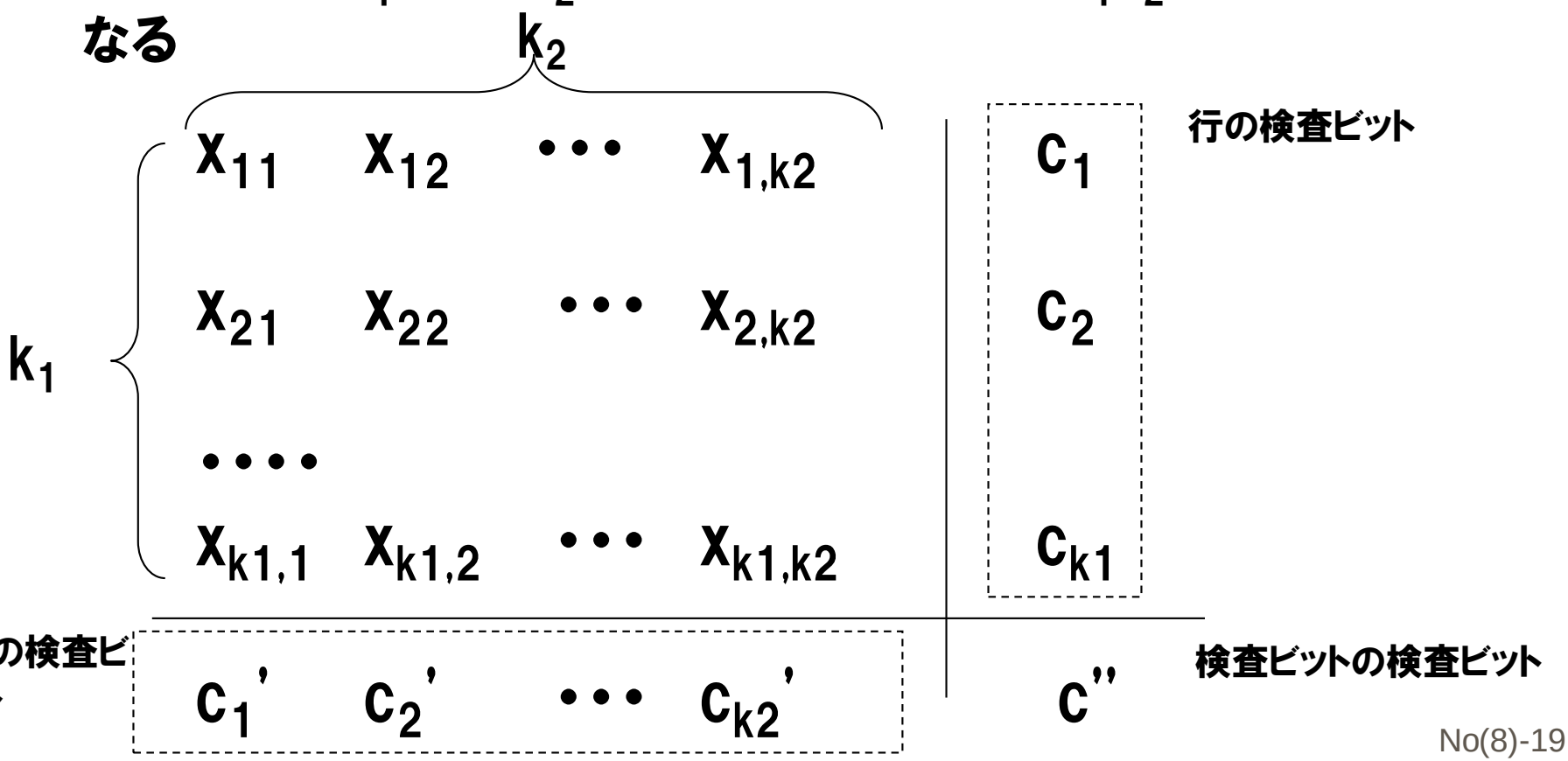
(ｂ)誤り検出可能
○か×かを区別できない（逆の位置でも同じ結果）

(ｃ)誤り検出可能
どの列の誤りかを区別できない（列検査ビットが0）

(ｄ)誤り検出可能
どの行の誤りかを区別できない（行検査ビットが0）

12.5 水平垂直パリティ検査符号: 一般化

- k_1k_2個の情報ビットを、$k_1 \times k_2$の配列に並べ、全ての行、列の1の数が偶数になるよう、k_1+k_2+1個の検査ビットを追加する
- 符号語は、$(k_1+1)(k_2+1)$の配列。これを1次元に並べれば、符号長$n=(k_1+1)(k_2+1)$, 情報ビット数$k=k_1k_2$、の線形符号となる



12.6 符号長n＝7，情報点k＝4の符号

$i=(i_1, i_2, i_3, i_4)$ を $x=(i_1, i_2, i_3, i_4, p_1, p_2, p_3)$ に符号化する例

（符号Aの例）

$$p_1 = i_1 + i_2 + i_3$$
$$p_2 = i_2 + i_3 + i_4$$
$$p_3 = i_1 + i_2 + i_4$$

（符号Bの例）

$$p_1 = i_1 + i_2 + i_3$$
$$p_2 = i_1 + i_2 + i_4$$
$$p_3 = i_1 + i_3 + i_4$$

$i_1, i_2, \ldots$に全ての系列を割り当てて、$p_1, p_2, \ldots$を求めて符号語を作る

i_1	i_2	i_3	i_4	p_1	p_2	p_3
0	0	0	0	0	0	0
1	0	0	0	1	0	1
0	1	0	0	1	1	1
…						

i_1	i_2	i_3	i_4	p_1	p_2	p_3
0	0	0	0	0	0	0
1	0	0	0	1	1	1
0	1	0	0	1	1	0
…						

検査ビットの作り方により異なる符号（上記の符号A,Bなど）ができる

12.7 線形符号の生成行列

線形符号の符号語 $x = (i_1, i_2, .., i_k, p_1, ..., p_{n-k})$**は、**
次の行列Gにより、 $x = i \cdot G$ **で与えられる。**

$$G = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & p_{11} & p_{21} & \cdots & p_{n-k,1} \\ 0 & 1 & 0 & \dots & 0 & p_{12} & p_{22} & \cdots & p_{n-k,2} \\ & & & \dots & & & & & \\ 0 & 0 & 0 & \dots & 1 & p_{1k} & p_{2k} & \cdots & p_{n-k,k} \end{pmatrix}$$

これは、情報ビット $i = (i_1, i_2, ..., i_k)$ **から、符号語** x **を**
作り出すので、生成行列と呼ばれる。（特に上記の形は、既約梯形標準形のG）

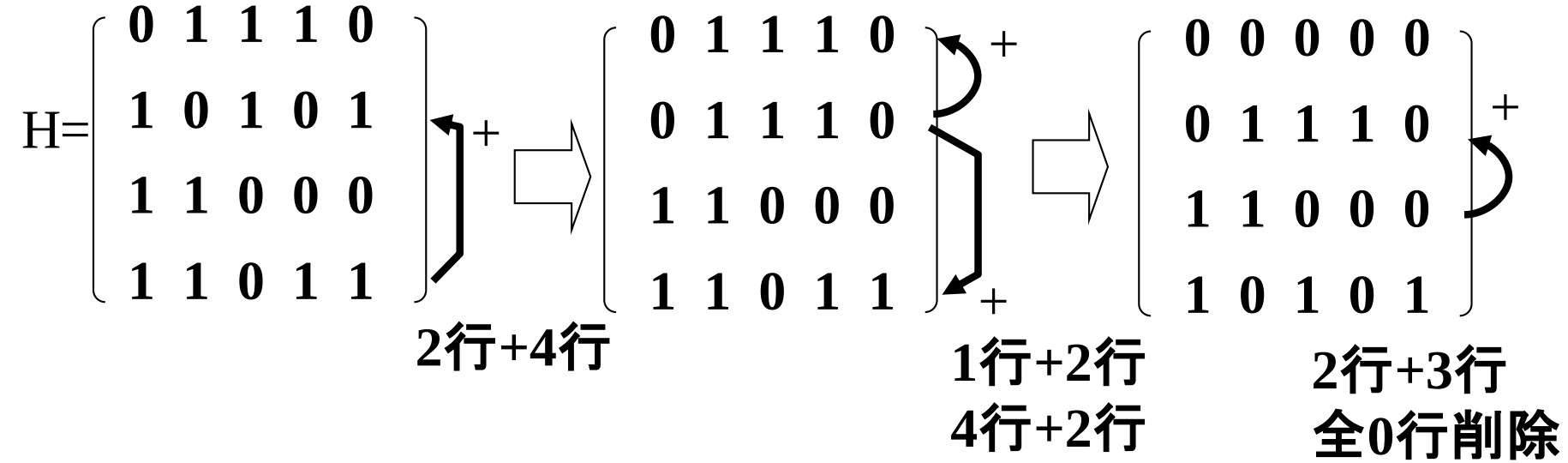
最初のk×k行列が単位行列になる形

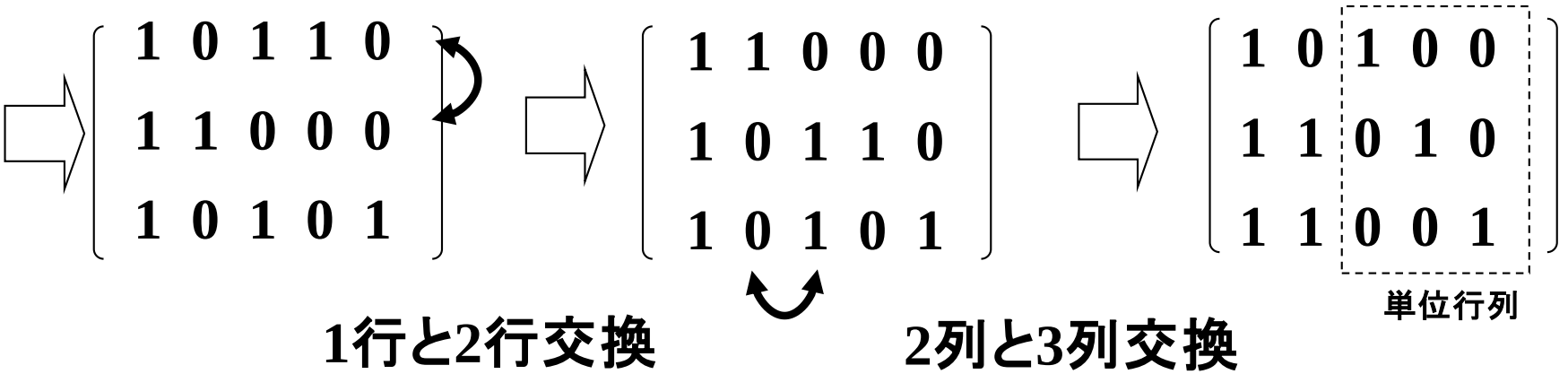
12.8 既約梯形標準形への変換法

- 任意の生成行列G、あるいはパリティ検査行列Hを既約梯形標準形に変換することができる。(*)
- 変換は、以下の基本行操作と列交換を施すことにより行える。（以下は、2元符号のHを例にとる）
  - Hの任意の2つの行を交換する
  - Hの任意の行に別の行を加える
  - 全てが0の行を取り除く
  - 必要なら、列を交換する　(*)

(*) 列交換を行うと、符号語の記号順序が変わるので、厳密には異なる符号となるが、誤り検出・訂正能力は同じなので、同値な符号という。

12.8 既約梯形標準形への変換：Hの変換例





12.9 (n=7, k=4) ハミング符号の行列G, H

(符号A)

$$p_1 = i_1 + i_2 + i_3$$
$$p_2 = i_2 + i_3 + i_4$$
$$p_3 = i_1 + i_2 + i_4$$

この規則からHを求める

$$G_A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

転置

$$H_A = \begin{matrix} i1 & i2 & i3 & i4 & p1 & p2 & p3 \end{matrix}$$
$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(符号B)

$$p_1 = i_1 + i_2 + i_3$$
$$p_2 = i_1 + i_2 + i_4$$
$$p_3 = i_1 + i_3 + i_4$$

この規則からHを求める

$$G_B = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

転置

$$H_B = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

12.10 符号化（1）：Gから符号語を生成

情報系列ベクトル（i）を生成行列（G）に掛けて生成する

G_Aにiを掛ける

$$x = i\,G_A = (i_1\ i_2\ i_3\ i_4)\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

i_1,i_2,i_3,i_4に全てのビットパターンを入れる

情報系列		符号語	
(1 0 0 0)		(1 0 0 0 1 0 1)	---→
(0 1 0 0)		(0 1 0 0 1 1 1)	---→
(0 0 1 0)	G_Aを掛ける	(0 0 1 0 1 1 0)	---→
…		…	
(1 1 0 0)		(1 1 0 0 0 1 0)	---→
(1 1 1 1)		(1 1 1 1 1 1 1)	---→

各行が符号語（全部で16個）

（符号A）

12.10 符号化 (2) :Hから符号語を生成

Hに符号ベクトル $(x_1,\cdots,x_n)$ を掛けた方程式を作る

方程式を作る

$$H_A x^T = 0$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} (x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7)^T = 0$$

$$\left.\begin{aligned} x_1 + x_2 + x_3 + x_5 &= 0 \\ x_2 + x_3 + x_4 + x_6 &= 0 \\ x_1 + x_2 + x_4 + x_7 &= 0 \end{aligned}\right\}$$

3元連立方程式なので、
4つが自由に選べ、残り
3つが方程式で決定される

自由変数を情報点ベクトル $(x_1,\cdots,x_k)$ とし 残りを解いて決定する

x_1, x_2, x_3, x_4を自由に選び、x_5, x_6, x_7を方程式で決定する。

$(1\ 0\ 0\ 0) \rightarrow (1\ 0\ 0\ 0\ 1\ 0\ 1)$ ----→

$(0\ 1\ 0\ 0) \rightarrow (0\ 1\ 0\ 0\ 1\ 1\ 1)$ ----→

各系列が符号語
（全部で16個）

…

（符号語A）と同じ符号語

12.11 復号化：シンドロームの定義

- 符号語　$x=(x_1,x_2,\ldots,x_n)$ を送信し、受信系列 $y=(y_1,y_2,\ldots,y_n)$ を受信したとする
- もし受信系列に何の誤りもなければ、$H\cdot y=0$　となる。途中に誤りを起こせば、$H\cdot y\neq 0$となる。
- これは系列 $y = x + e$ が受信され、

  $H\cdot y = H\cdot (x + e) = H\cdot x+ H\cdot e= H\cdot e$　が残ったものと説明できる。　e を**誤りパターン**と呼び、

  $s = H\cdot y$　を**シンドローム（症候群）**と呼ぶ。

12.11 復号化：シンドロームの性質

- 符号語 xの第 i 番目の桁に誤りが生じたとすれば、誤りパターン e は、

  i-1 個

  $e_i = (0, 0, \ldots, 1, 0 \ldots 0)$ となる。

- 受信系列 $y=x+e_i$ で与えられる。従ってｼﾝﾄﾞﾛｰﾑは、

  $s = H \cdot y = H \cdot (x + e_i) = H \cdot x + H \cdot e_i = H \cdot e_i$

  となる。

- 従って、**シンドローム（s）は パリティ検査行列（H）の第 i 列目と一致する**ことを示している。
  - 2元線形符号で、Hの列ベクトルが零(0)でなく、しかもそれらが互いに全て異なれば、この符号は単一誤り訂正符号となる

12.11 復号化：多重誤り訂正符号のシンドローム

- パリティ検査行列 H 、符号語 xが、伝送途中で i 番目と j 番目が誤り、受信系列 y を受信したとする
- $y = x + e_i + e_j$ （e_iは第i番目ビットの誤りパターン）
- シンドローム s は、

  $s=H\cdot y=H\cdot(x + e_i + e_j) =H\cdot e_i +H\cdot e_j$

  となる。従って、Hの第 i列＋第j列、になる。
- 2重誤り訂正可能であるためには下記が成立する必要有り
  - 任意の二重誤りパターンが互いに異なる：$H\cdot(e_i+e_j)\neq H\cdot(e_k+e_l)$
  - 二重誤りパターンと単一誤りパターンが異なる：$H\cdot(e_i+e_j)\neq H\cdot e_k$
  - 単一誤りパターン同士も異なる：$H\cdot e_i\neq H\cdot e_j$
  - 誤りパターンが零でない：$H\cdot e_i\neq 0$
- Hの任意の4個以下の列ベクトルの和が非零ならば、二重誤り訂正符号となる

12.11 復号化：シンドローム計算による復号

- $s = H \cdot e$を満たす重み最小の e を求める

  単一誤りに対しては、ｼﾝﾄﾞﾛｰﾑと一致する行列Hの列ベクトルの列番号が誤り個所を示す。すなわち、

  $s = H \cdot e_i$ ＝Hの第 i 列

- 符号語を、$x=y+e_i$ として求める
  - 単一誤りに対してはy の第 i 番目の記号 y_i を訂正する。

12.11 受信系列からシンドローム計算

- 受信系列が $y = (y_1\ y_2\ y_3\ y_4\ y_5\ y_6\ y_7)$ とすると、シンドローム $s = H y^T$ を計算する。

$$s_1 = y_1 + y_2 + y_3 + y_5$$
$$s_2 = y_2 + y_3 + y_4 + y_6$$
$$s_3 = y_1 + y_2 + y_4 + y_7$$

← H_A の場合

- 例: $y = (1\ 1\ 0\ 0\ 1\ 1\ 0)$ の場合、

  $s_1 = 1, s_2 = 0, s_3 = 0$ となる。これより、$s = (1\ 0\ 0)$ となり、H_A の5列目と一致するので、y_5 が誤っていることが分かる。

  従って、y_5 を1 → 0と訂正し、送られた符号語は 1 1 0 0 0 1 0と判定する。(これは、情報系列 $i = (1\ 1\ 0\ 0)$ に対する符号語)

12.12 ハミング符号の一般化

- ハミング符号では単一誤りに対しては、検査行列の各列がシンドロームパターンとして現れる
  - 単一誤り訂正ができるためには、検査行列のすべての列が互いに異なり、全ゼロでなければよい
- m次元の2元ベクトルをすべて列として並べた行列を検査行列とする符号を考える
- このような行列（H）の行数はm、列数は2^m-1である。Hを検査行列とする符号の符号長はHの列数に一致し、検査ビット数はHの行数に一致する
- 従って、符号長$n=2^m-1$、情報ビット数$k=2^m-1-m$、検査ビット数$m=n-k$、の単一誤り訂正符号が構成できる。これが一般のハミング符号である。

12.12 ハミング符号の一般化: m=4の場合

- m=4の場合、全ゼロ以外の4次元2元ベクトルを並べると、以下のとおり4行15列の行列となる
- これが、n=15, m=4, k=n-m=11、の単一誤り訂正ハミング符号

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

12.13 パリティ検査符号の効率的復号法

- $s = H \cdot e$を満たす重み最小のeを求める。sの個数は2^r個（r次元ベクトル）。
  - 方法1
    - 行列Hに対して誤りパターンを重みの小さい順に掛ける演算を、得られたシンドロームに$H \cdot e$が一致するまで続ける
  - 方法2
    - 2^r個のシンドロームとその各々に対応する重み最小の誤りパターンの対応表を用意し、表から誤りを見つける
- 方法2による復号法は、数学の群論を使って整然と記述できる
  - 群Gの部分群Hによる剰余類分割

12.14 パリティ検査符号の剰余類分割

- 符号長n=6, 情報点数k=3, 検査点数r=3
- パリティ検査行列Hと生成行列G

$$H=\left(\begin{array}{c:ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \qquad G=\left(\begin{array}{ccc:ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

- 符号語 $x=(x_1, x_2, x_3, x_4, x_5, x_6)$ をGから構成する

12.15 Gから符号語の生成

- $x^{(1)} = (0,0,0,0,0,0)$　・・・・オールゼロ符号語
- $x^{(2)} = (1,0,0,0,1,1)$　・・・・Gの第1行
- $x^{(3)} = (0,1,0,1,0,1)$　・・・・Gの第2行
- $x^{(4)} = (0,0,1,1,1,0)$　・・・・Gの第3行
- $x^{(5)} = (1,1,0,1,1,0)$　・・・・Gの第1+第2行
- $x^{(6)} = (1,0,1,1,0,1)$　・・・・Gの第1+第3行
- $x^{(7)} = (0,1,1,0,1,1)$　・・・・Gの第2+第3行
- $x^{(8)} = (1,1,1,0,0,0)$　・・・・Gの第1+第2+第3行

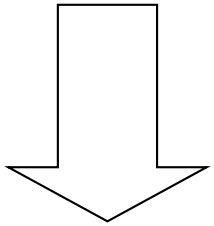
12.16 剰余類分割表

第1行目に符号語を並べる

剰余類首	剰余類							シンドローム
000000	100011	010101	001110	110110	101101	011011	111000	000
000001	100010	010100	001111	110111	101100	011010	111001	001
000010	100001	010111	001100	110100	101111	011001	111010	010
000100	100111	010001	001010	110010	101001	011111	111100	100
001000	101011	011101	000110	111110	100101	010011	110000	110
010000	110011	000101	011110	100110	111101	001011	101000	101
100000	000011	110101	101110	010110	001101	111011	011000	011
100100	000111	110001	101010	010010	001001	111111	011100	111

12.17 線形符号を群符号として見る

- 線形符号の性質を深く調べるために、線形符号が代数学の群をなすことを示す
- 線形符号＝群符号



まず、群論の復習を行う

12.18 群の定義：群の公理

【定義】集合Gがあり、Gに属する任意の元の間に演算が定義されており、次の性質を満たすとき、Gを群と呼ぶ。

演算は、2つの元、a, bに対して第3の元cが定まる2項演算；c＝a＋b（和）又はc＝ab（積）

（1）a, b∈G、ならばc＝a＋b∈G

（2）a, b, c∈Gならば、（a＋b）＋c＝a＋（b＋c）（結合律）

（3）ある元i∈Gが存在し、任意の元a∈Gに対し、a＋i＝i＋a＝a
（i：単位元、i＝0）（＊）

（4）任意の元a∈Gに対して、－a∈Gとなる元があり、a＋（－a）＝（－a）＋a＝iが成り立つ（－a：逆元）（＊）

（＊）演算が乗法の場合：ai＝ia＝a； $a \cdot a^{-1} = a^{-1} \cdot a = i$（単位元i＝1）

（5）a＋b＝b＋a（又はab＝ba）（可換律；可換群の場合）

12.18 群の例(その１)

- 例1：全ての実数の集合、加法について群
- 例2：0を除く全ての実数の集合、乗法について群
- 例3：0を除く全ての複素数の集合、乗法について群
- 例4：全ての正則なn×n行列、行列の乗法について群 （但し可換群ではない）
- 例5：集合{0, 1}、2を法とする加法について群

大雑把に言えば、1種類の演算(足し算や掛算のようなもの)が定義された一般化した「数」の概念

12.18 群の例(例6:乗法群)

- 集合{1,2,...,p−1}, pを法とする乗法について群(但しpは素数)

例えば、p＝7を法とする乗法群

・	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$6 \times 4 \pmod 7$
$= 24 \pmod 7$
$= 3$

12.18 部分群と剰余類

【定義】部分群

- ある群Gにおいて、その部分集合S自身が群をなすもの

- 例：X={0,1,...,5}で6を法とする加法群で、S1={0,2,4}は、それ自身で群をなすので部分群。同様に，S2={0,3}も部分群。

【性質】群Gとその部分群Sが与えられたとき、GをSで展開できる

1）Sの元s_1，s_2，．．s_rを第1行目に並べる

2）Sに含まれない元$g_1 \in G$を選び、$g_1 s_i$（i＝1，2，．．．，r）を求め、これを第2行目に並べる

3）同様に第1、第2行目に現れない$g_2 \in G$を選び、$g_2 s_i$を求め、第3行目に並べる

4）以下、これをGの元が全て現れるまで繰り返す

12.18 部分群による群の展開:剰余類展開

- 部分群(S)による群(G)の展開

S:	s_1	s_2	s_3	…	s_r
g_1S:	g_1	g_1s_2	g_1s_3	…	g_1s_r
g_2S:	g_2	g_2s_2	g_2s_3	…	g_2s_r
g_3S:	g_3	g_3s_2	g_3s_3	…	g_3s_r
.					
.					
g_tS:	g_t	g_ts_2	g_ts_3	…	g_ts_r

部分群の元

各行を，剰余類と言う

各剰余類の最初の元を，剰余類首という

剰余類首＝$\{s_1, g_1, g_2, g_3, \cdots, g_t\}$

12.18 剰余類展開の例

- 例6のX={0,1,...,5}の部分群S={0,2,4}を用いた展開

  S:　0　2　4

  1S:　1　3　5

  剰余類＝S, 1S, 剰余類首＝{0, 1}

- 例6のX={0,1,...,5}の部分群S={0,3}を用いた展開

  S:　0　3

  1S:　1　4

  2S:　2　5

  剰余類＝S, 1S, 2S, 剰余類首＝{0, 1, 2}

12.18 剰余類展開例：無限群の例

- 集合G={整数全体；0，±1、±2、．．．}は加法について群、部分集合S={4の整数倍；0，±4、±8、．．}はそれ自身で加法群、従って部分群

  剰余類展開は下記のとおり：

S:	…−12	−8	−4	0	4	8	12…
1S:	…−11	−7	−3	1	5	9	13…
2S:	…−10	−6	−2	2	6	10	14…
3S:	…−9	−5	−1	3	7	11	15…

剰余類首＝{0, 1, 2, 3}

S= {0} ,1S= {1} ,2S= {2} 、3S= {3} と表現する

．．．4で割った余りの集合

12.18 剰余類展開に関する定理

【定理】

- 群Gのどの元も部分群Sのいずれかの剰余類に1回だけ現れる　⇔群Gの全ての元をその剰余類で隈なく分割できる

【定義】

- 位数(いすう):集合の元の数
  - 例6のG＝{0,1,2,3,4,5}の場合は，位数=6
- S上のGの指標:部分群Sに関する群Gの剰余類数
  - 例6の部分群S= {0,2,4} の場合は，指標=2 （S，1Sの2つ）

【性質】

- Sの位数× S上のGの指標＝Gの位数

12.19 群としての線形符号

【定理】

- 2元線形符号は「2を法とする加法」について群をなす

（証明：群の公理を満たすことの証明）

- 線形符号をCとし、パリティ検査行列をHとする

（1）$w_1, w_2 \in C$ならば、$Hw_1 = 0$、$Hw_2 = 0$．　これより$H(w_1 + w_2) = 0$。従って、$w_1 + w_2 \in C$

（2）結合律は明らかに成立する

（3）単位元（ゼロ元）は$0 = (0,0,\cdots,0)$ なり、$H0 = 0$が成立する．また任意の$w \in C$に対し$0+w=w+0=w$を満たす

（4）任意の$w \in C$に対し、w自身が逆元となる．なぜならば，$w+w=0 \in C$が成立するから．

以上より，群の公理を満たすので，Cは群をなす．

12.19 部分群としての線形符号

- G＝{長さnの2元系列全体}は，演算＝2を法とする加法，により群をなす
- 線形符号CはGの部分集合(C⊆G)で群をなすので部分群となる
- 従って、線形符号Cによる2元系列Gの剰余類展開が可能である：

- 例：　$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

- 上記のHに対する符号語$w_i \in C$は下記の4個である：

$w_1 = (0\ 0\ 0\ 0)$, $w_2 = (1\ 0\ 0\ 1)$, $w_3 = (1\ 1\ 1\ 0)$, $w_4 = (0\ 1\ 1\ 1)$

（なぜならば，各w_iについて，$H \cdot w_i = 0$となるから）

4個の2元系列は全部で16種類あるが，そのうち上記の4種類のみが符号語となっている

12.20 線形符号による剰余類展開

	w_1	w_2	w_3	w_4	
	0000	1001	1110	0111	← ①
u1=	1000	0001	0110	1111	← ②
u2=	1100	0101	0010	1011	← ③
u3=	0100	1101	1010	0011	← ④

剰余類首

- w_1 (0000), w_2 (1001), w_3 (1110), w_4 (0111) の4つが符号語。これらを第1行に並べる 【①】
- これら以外のビット列を選び、これを第2行先頭に置く(u_1)。u_1+w_iを第2行の要素に並べる 【②】
- 同様に、第2行要素に含まれないビット列を選び第3行先頭に置く(u_2)。u_2+w_iを第3行に並べる【③】
- 以下繰り返して、全てのビット列を網羅的に並べる【④】
- u_1,u_2,u_3,及び先頭のw_1を剰余類首という

12.20 剰余類展開に関する定理

【定理】

- 2つの2元系列(ベクトル)v_1, v_2が同じシンドロームをもてば、これらは同じ剰余類に属する。異なるシンドロームを持てば異なる剰余類に属する。

(証明)

- v_1,v_2のシンドロームが等しいとする。$Hv_1=Hv_2$
- $H(v_1-v_2)=0$, v_1-v_2が符号語$s_i \in C$
- v_1の剰余類首をu_kとすれば、適当な$s_j \in C$に対して, $v_1=u_k+s_j$, $v_1-v_2=s_i$と書ける
- これより、$v_2=v_1-s_i=u_k+s_j-s_i$.　v_2もu_kを剰余類首とする同じ剰余類に含まれる
- 逆も同様の論理で証明できる

12.20 剰余類展開と復号表：標準配列

- 剰余類展開表を復号表として利用
- 受信系列vに対して、vが属する剰余類（どの行か）を調べ、その剰余類首u_kをvから引けば（加えれば）復号できる
  - $v = u_k + w_i$, $w_i \in C$、$w_i = v - u_k = v + u_k$

【定義】標準配列

- 剰余類展開による復号表を符号の標準配列と呼ぶ

【標準配列による復号法】

- シンドロームと剰余類首の対応表だけ受信側で記憶
- 受信系列→シンドロームを計算→剰余類首を求める→受信系列から引く（加える）［剰余類首＝誤りパターン］

12.20 標準配列による復号

- 剰余類展開に基づく復号表
  - 展開表全てを記憶させておく必要はない
  - 剰余類首とシンドロームの対応のみ記憶すればよい
- 復号法
  - 受信系列（v）に対するシンドロームを計算する
  - シンドロームに対する剰余類首（u_k）を求める
  - v－u_kを求め、これを送信された符号語と復号する
    - 剰余類首を誤りパターンと見なすことを意味する
  - 剰余類の中で誤りパターンとして生起確率の高いものを剰余類首として選べば、誤り率最小の復号法となる
  - BSC通信路では、最も重みの小さい（１の個数が少ない）パターンを剰余類首に選べばよい

12.20 標準配列による復号と誤り率(１)

- 符号の誤り訂正能力以内の誤りならば、どのような誤りも訂正可能
- 誤り率pの2元対称通信路(BSC)で群符号を用いて伝送したとき、受信側で正しく復号される確率Pcは、

$$Pc = \Sigma_{i=0\cdots n} N_i \ (1-p)^{n-i} \ p^i \quad ,$$

係数N_i:重みiの剰余類首数

特に、t重誤り訂正符号では、t個までの誤りを訂正できる(t+1以上は訂正不能)ので、$N_i = {}_nC_i$ を考慮すると、

$$Pc = \Sigma_{i=0\cdots t} \ {}_nC_i \ (1-p)^{n-i} p^i$$

ここで、

$${}_nC_i = n!/(n-i)!\,i!$$

2項係数、n個からi個取り出す組合せ数

12.20 標準配列による復号と誤り率(２)

- 例: $H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$
  - 符号語$w_i \in C$は下記の4個

    $w_1 = (0\ 0\ 0\ 0)$, $w_2 = (1\ 0\ 0\ 1)$, $w_3 = (1\ 1\ 1\ 0)$, $w_4 = (0\ 1\ 1\ 1)$

	w_1	w_2	w_3	w_4
	0000	1001	1110	0111
u1=	1000	0001	0110	1111
u2=	1100	0101	0010	1011
u3=	0100	1101	1010	0011

（誤り率最小の復号表ではない）標準配列

12.20 標準配列による復号と誤り率(３)

	w_1	w_2	w_3	w_4
	0000	1001	1110	0111
u1=	1000	0001	0110	1111
u2=	0010	1011	1100	0101
u3=	0100	1101	1010	0011

上記は（誤り率最小の）標準配列である

- 重み分布：$N_0=1$, $N_1=3$
  - 重み1の誤りパターンは総数4であるが、このうち3つまでが訂正できることを示す。
- 正しく復号される確率 $Pc=(1-p)^4+3(1-p)^3p$
- 最小重みのパターンを剰余類首に選んだ標準配列による復号法は**最小距離復号法**と呼ぶ