情報理論(No.10)

2016/11/26

今後の講義予定

12／03:通常(第11回)

12／10:通常(第12回)

12／17:通常(第13回)

01／07:通常(第14回)

講義目次

12.32 高度な巡回符号のための代数学　(5) 拡大体

- 拡大体 (Extension field)
  - ある体を部分体(基礎体 (Ground field) という)として含む別の体のこと。
- 拡大体の作り方
  - P (x) をGF (p) 上の多項式とする。P (x) がGF (p) 上で既約ならば、P (x) を法とするGF (p) 上の多項式環の剰余類は体をなす。
    - P (x) の次数がmならば、この体はp^m個の元を有する。これを基礎体のGF (p) から拡大された拡大体といいGF (p^m) で表す。
    - この既約多項式P (x) を法として作られる拡大体は、元の体GF (p) にP (x) =0の根を付加してできたものと同等。
- 拡大体の例
  - 基礎体のGF (2) = {0,1} に、虚数単位 (i) を付加することで拡大された4元をもつ体 {0, 1, i, i+1} が導かれる。これは、GF (2) に$x^2+1=0$の根 (i) を付加して作られたものと同じ。
  - P (x) =0の根をαと書くと、 {0, 1, i, i+1} = {0,1, α , α +1} , と表せる。ここで$\alpha^2+1=0$。

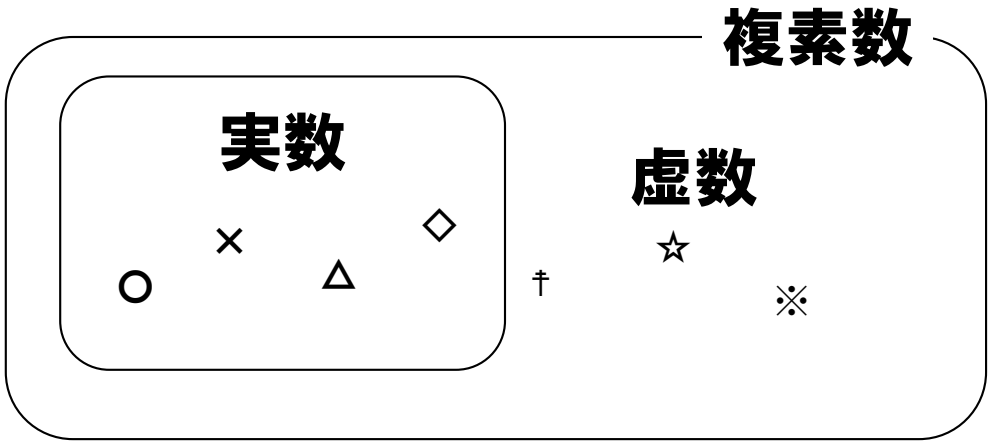
12.32 高度な巡回符号のための代数学　(5) 拡大体

- 有限体の位数(元の数)は，素数(p)のべき乗(p^m，但しp=素数，m=整数)しかあり得ないことが分かっている．
  - (例)有限体をGF(q) で表せば，GF(2)，GF(5)，GF(7)，$GF(2^2)=GF(4)$，$GF(5^3)=GF(125)$など
- 位数が素数pの有限体GF(p)は集合{0,1,..,p−1}を考え，これに対してmod pで加算，乗算を行えば構成できる．→講義資料No.7の数学的準備(5)
- しかしp^2以上の位数の有限体は本方法では構成できない．
  - (例)$q=2^2=4$の場合，{0,1,2,3=q^2-1}をmod 4で演算すると，2の乗法での逆元2^{-1}が存在しない(2×α=1となるα)．従って，体とならない　→同資料No.6数学的準備(6)
- 従って，別の方法を考える必要がある．

⇒「実数体から複素数体を導く」やり方が参考になる

12.32 高度な巡回符号のための代数学　(5) 拡大体

- 実数から複素数への導出
  - 実数体の上で規約な多項式x^2+1の根（$x^2+1=0$の解）i（虚数単位という）を実数体に付加することにより導出
    - {実数} ＋ {i} を作り，さらに体を構成できるように，必要な元を全て追加したものが {複素数}　・・・・下図
- 【定義】体の拡大
  - 体Fに，F上で規約な多項式の根を追加して，より大きな体を作ることを体の拡大という．Fを基礎体という．



12.32 高度な巡回符号のための代数学　(5) 拡大体

- **拡大体の要素のべき表現、ベクトル表現**
  - GF (p) 上の既約多項式の根(α)のべき乗で、拡大体の要素が表わされる。**m次既約多項式**で拡大する場合、次のとおり。
    $$\mathrm{GF}(\mathrm{p}^{\mathrm{m}}) = \{0, 1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{\mathrm{p}^{\mathrm{m}}-2}\}$$
  - 上記のように、すべての非零元を根のべき乗で表せる規約多項式を原始多項式という。
  - 例：GF (2) 上の多項式x^2+x+1は既約。この根をαとする。αを GF (2) = {0,1} に付加した拡大体をつくる。
    - 0,1,αを元として含む。
    - 乗算で閉じることから、αのべき乗も元になる。α^2, α^3, α^4,…も元。
    - $\alpha^2+\alpha+1=0 \Rightarrow \alpha^2=-\alpha-1=\alpha+1$, $\alpha^3=\alpha(1+\alpha)=\alpha+\alpha^2=1=\alpha^0$, $\alpha^4=\alpha$,…以後繰り返し。
    - 即ち、αのべき乗で異なるものは、$1=\alpha^0$, α, α^2の3つのみ。
    - {0,1, α, α^2} で体をなす。GF (4) と表記。 ⇒加法と乗法の表は次ページのとおり。

12.32 高度な巡回符号のための代数学　(5) 拡大体
GF(2)の2次拡大体：GF(4)

加法

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

乗法

·	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

- ある種の既約多項式を選ぶと、GF(q)の非0の全ての元を根(α)のべき乗、$\alpha^0=1$, α, α^2, α^3,…で表すことができる。
  この既約多項式を「原始多項式」という。この多項式の根を原始元という。

12.32 高度な巡回符号のための代数学　(6) 原始多項式

- GF (2) 上m次原始多項式
  - 16次までの原始多項式を、それぞれ1つずつ示す：

m	原始多項式	m	原始多項式
1	$1+x$	9	$1+x^4+x^9$
2	$1+x+x^2$	10	$1+x^3+x^{10}$
3	$1+x+x^3$	11	$1+x^2+x^{11}$
4	$1+x+x^4$	12	$1+x+x^4+x^6+x^{12}$
5	$1+x^2+x^5$	13	$1+x+x^3+x^4+x^{13}$
6	$1+x+x^6$	14	$1+x+x^6+x^{10}+x^{14}$
7	$1+x+x^7$	15	$1+x+x^{15}$
8	$1+x^2+x^3+x^4+x^8$	16	$1+x+x^3+x^{12}+x^{16}$

  - 上記多項式により、拡大体GF (2^m) が生成される。
    - 全ての元は、根 (α) のべき乗を用いて表わせる。

$$\mathrm{GF}(2^m)=\{0,1,\alpha,\alpha^2,\ldots,\alpha^{2^m-2}\},\alpha^{2^m-1}=1$$

12.32 高度な巡回符号のための代数学（7）べき乗表現、ベクトル表現

- GF (2^m) の元のべき乗表現とベクトル表現
  - 原始多項式の根（α）のべき乗 α^i は、GF (2) の元を係数とする $1, \alpha, \alpha^2, \cdots, \alpha^{m-1}$ の1次式で表せる：
    - $\alpha^i = p_0 + p_1\alpha + p_2\alpha^2 + \cdots + p_{m-1}\alpha^{m-1}$

      ここで、$p_0, p_1, \cdots, p_{m-1} \in GF(2) = \{0, 1\}$
    - α^i =の表現は、係数を並べたベクトル $(p_0, p_1, \cdots, p_{m-1})$ としても表現できる。両者は等価。
  - 例：m=3の場合，$1+x+x^3$ の根をαとし、これから拡大されるGF (2^3) の元のべき乗表現とベクトル表現は次のようになる。

12.32 高度な巡回符号のための代数学（7）べき乗表現、ベクトル表現

- GF (2^3) の元の表現
  - 原始元（α）は，$x^3+x+1=0$の根

（※）ベクトルは左からαの2次−1次−0次の順序

べき乗	$\alpha^2,\alpha,1$の一次結合	ベクトル（※）
0	0	0 0 0
1	1	0 0 1
α	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha+1$	0 1 1
α^4	$\alpha^2+\alpha$	1 1 0
α^5	$\alpha^2+\alpha+1$	1 1 1
α^6	α^2+1	1 0 1
α^7	1	0 0 1

12.32 高度な巡回符号のための代数学 (7) べき乗表現、ベクトル表現

- GF (2^4) の元の表現
  - 原始元 (α) は, $x^4+x+1=0$の根

(※)ベクトルは左からαの3次−2次−1次−0次の順序

べき乗	$\alpha^3,\alpha^2,\alpha,1$の一次結合	ベクトル (※)	べき乗	$\alpha^3,\alpha^2,\alpha,1$の一次結合	ベクトル (※)
0	0	0 0 0 0	α^8	α^2+1	0 1 0 1
1	1	0 0 0 1	α^9	$\alpha^3+\alpha$	1 0 1 0
α	α	0 0 1 0	α^{10}	$\alpha^2+\alpha+1$	0 1 1 1
α^2	α^2	0 1 0 0	α^{11}	$\alpha^3+\alpha^2+\alpha$	1 1 1 0
α^3	α^3	1 0 0 0	α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1 1 1 1
α^4	$\alpha+1$	0 0 1 1	α^{13}	$\alpha^3+\alpha^2+1$	1 1 0 1
α^5	$\alpha^2+\alpha$	0 1 1 0	α^{14}	α^3+1	1 0 0 1
α^6	$\alpha^3+\alpha^2$	1 1 0 0	(α^{15})	1	0 0 0 1
α^7	$\alpha^3+\alpha+1$	1 0 1 1	−	−	−

12.32 高度な巡回符号のための代数学 (8) 最小多項式

- GF (2^4) の元の最小多項式

  $M_i(x)$ ：α^iを根としてもつ最小次数の多項式

  - 原始元 (α) は，$x^4+x+1=0$の根

元	最小多項式		元	最小多項式	
0		x	α^8	$M_8(X)$	x^4+x+1
1	$M_0(X)$	$x+1$	α^9	$M_9(X)$	$x^4+x^3+x^2+x+1$
α	$M_1(X)$	x^4+x+1	α^{10}	$M_{10}(X)$	x^2+x+1
α^2	$M_2(X)$	x^4+x+1	α^{11}	$M_{11}(X)$	x^4+x^3+1
α^3	$M_3(X)$	$x^4+x^3+x^2+x+1$	α^{12}	$M_{12}(X)$	$x^4+x^3+x^2+x+1$
α^4	$M_4(X)$	x^4+x+1	α^{13}	$M_{13}(X)$	x^4+x^3+1
α^5	$M_5(X)$	x^2+x+1	α^{14}	$M_{14}(X)$	x^4+x^3+1
α^6	$M_6(X)$	$x^4+x^3+x^2+x+1$	(α^{15})	$M_{15}(X)$	$x+1$
α^7	$M_7(X)$	x^4+x^3+1	–		–

12.32 高度な巡回符号のための代数学: 拡大体の符号理論への応用

- これまで述べてきた数学(体、拡大体)の理論が、より高度な符号を作り出すために使われる
- これら高度な符号は、実用上も重要な符号である

12.33 重要な巡回符号：BCH符号

- **巡回ハミング符号**
  - GF (2^m) の原始元 (α) の最小多項式(原始多項式)を生成多項式とする符号長$n=2^m-1$の巡回符号
- **BCH (Bose-Chaudhuri-Hocquenghem) 符号**
  - 上記の巡回ハミング符号を一般化して、α, α^2, α^4, …, α^{2t}の全てを根としてもつ最小次数の多項式を生成多項式とする巡回符号をBCH符号という
  - GF (2^m) の非零の元 α^iの最小多項式
    - 多項式F (x) が α^iを根として持てば、$\alpha^{2i}, \alpha^{4i}, \alpha^{8i}$…も根としてもつ。

      $\because [F(x)]^2 = (f_0+f_1x+f_2x^2+\cdots+f_lx^l)^2 = f_0+f_1x^2+\cdots+f_lx^{2l} = F(x^2)$

      $\alpha^{i2^j} = \alpha^i$ となる最小整数$j=d_i$とする。このとき、F (x) は

      $\alpha^i, \alpha^{2i}, \alpha^{4i}, \alpha^{8i}, \ldots, \alpha^{i2^{d_i-1}}$ のd_i個の根をもつ。

12.33 重要な巡回符号:BCH符号

- $M_i(x) = (x - \alpha^i)(x - \alpha^{2i})(x - \alpha^{4i})(x - \alpha^{8i})\ldots(x - \alpha^{i2^{d_i - 1}})$ はGF(2)上のα^{i}の最小多項式。ところで、$\alpha^{2^m} = \alpha$ (mは拡大体の次数)であるから、$\alpha^{i2^m} = \alpha^i$ となり、$d_i \le m$ が成り立つので、$M_i(x)$ はm次以下。

- BCH符号の生成多項式は、$M_1(x)$, $M_2(x)$,…,$M_{2t}(x)$ の全てで割り切れる最小次数多項式。しかし、$M_1(x) = M_2(x) = M_4(x) = \cdots$ が成り立つため、偶数番目のものは除いてよい。結局、生成多項式は、奇数番のみ取り出した　　$G(x) = LCM[M_1(x), M_3(x), M_5(x), \ldots, M_{2t-1}(x)]$　と表わせる。
  - LCM:最小公倍多項式
  - t個の$M_i(x)$ の次数はm以下なので$G(x)$ の次数はmt以下

12.33 重要な巡回符号：BCH符号

- BCH符号の性質
  - G(x)の次数はmt以下になるので、従って検査点数はmt以下になる。
  - 最小距離は2t+1以上。
    ＝＞証明は難しいが、次項のBCH符号の最小距離を参照

結局

- 長さ$n=2^m-1$
- 情報点数$k \geqq 2^m-1-mt$
- 検査点数$n-k \leqq mt$
- 最小距離$d_{min} \geqq 2t+1$
  - 少なくともt個の誤りを訂正可能。
  - t=1の場合は巡回ハミング符号になる。

12.33 重要な巡回符号：BCH符号

- αを原始多項式$1+x+x^4$の根とする。
- GF (2^4) の元の最小多項式は、下記の通り：

べき表現	ベクトル表現	最小多項式
0	(0 0 0 0)	x
1	(1 0 0 0)	$1+x$
α	(0 1 0 0)	$1+x+x^4 = M_1(x)$
α^2	(0 0 1 0)	$1+x+x^4 = M_2(x)$
α^3	(0 0 0 1)	$1+x+x^2+x^3+x^4 = M_3(x)$
α^4	(1 1 0 0)	$1+x+x^4 = M_4(x)$
α^5	(0 1 1 0)	$1+x+x^2 = M_5(x)$
α^6	(0 0 1 1)	$1+x+x^2+x^3+x^4 = M_6(x)$
α^7	(1 1 0 1)	$1+x^3+x^4 = M_7(x)$
α^8	(1 0 1 0)	$1+x+x^4 = M_8(x)$
α^9	(0 1 0 1)	$1+x+x^2+x^3+x^4 = M_9(x)$
・・・		

12.33 重要な巡回符号：BCH符号

- 符号長n=15 $(=2^4-1)$ のBCH符号の例

t	k	d_{min}	生成多項式
1	11	3	$1+x+x^4 = M_1(x)$
2	7	5	$1+x^4+x^6+x^7+x^8$
			$=LCM[M_1(x), M_3(x)]$
3	5	7	$1+x+x^2+x^4+x^5+x^8+x^{10}$
			$=LCM(M_1(x), M_3(x), M_5(x)]$
7	1	15	$1+x+x^2+\cdots+x^{13}+x^{14}$

12.33 重要な巡回符号：(n, k) = (15, 7) BCH符号

- 符号長$n=2^4-1=15$, 検査点$m=4$, 情報点$k=7$であるので, $n-k=8 \leqq 4t$より, $t=2$ (tは最小).
- 位数15の原始元αを, 4次の原始多項式$x^4+x+1=0$の根とする.
- $t=2$なので, α, α^2, α^3, α^4を根とする多項式が生成多項式となる.
- このうち, α, α^2, α^4を根とする最小多項式$M(X)$はすべて同じとなる(αが根ならα^{2i}も根). 即ち
  $M_1(X)=M_2(X)=M_4(X) = x^4+x+1$
- α^3を根とする最小多項式は, $M_3(X)=x^4+x^3+x^2+x+1$
- 従って, 生成多項式$G(X)=LCM\ (M_1(X), M_3(X)) = (x^4+x+1)(x^4+x^3+x^2+x+1) = x^8+x^7+x^6+x^4+1$

12.33 重要な巡回符号：(n, k) = (15, 7) BCH符号

- $M_3(X) = x^4+x^3+x^2+x+1$

  これはα^3, α^6, α^{12}, $\alpha^{24} = \alpha^9$ ($\alpha^{15}=1$なので)を根にもつので,

  $(\alpha^3)^4+$

  $(\alpha^3)^3+(\alpha^3)^2+\alpha^3+1=\alpha^{12}+\alpha^9+\alpha^6+\alpha^3+1=(\alpha^3+\alpha^2+\alpha+1)+$

  $(\alpha^3+\alpha)+(\alpha^3+\alpha^2)+\alpha^3+1=0$

  α^4以上はα^3以下の一次結合で表現しなおすことにより上の式が導かれる.

- $G(X) = LCM(M_1(X), M_3(X)) = M_1(X)M_3(X)$

$$
\begin{array}{ll}
 & x^4+x^3+x^2+x+1 \\
\times & x^4+x+1 \\
\hline
 & x^8+x^7+x^6+\cancel{x^5}+\cancel{x^4} \\
 & \quad \cancel{x^5}+\cancel{x^4}+\cancel{x^3}+\cancel{x^2}+x \\
+ & \quad\quad \cancel{x^4}+\cancel{x^3}+\cancel{x^2}+x+1 \\
\hline
 & x^8+x^7+x^6+x^4+1
\end{array}
$$

12.33 重要な巡回符号：(n, k) = (15, 5) BCH符号

- 符号長$n=2^4-1=15$, 検査点$m=4$, 情報点$k=5$であるので, $n-k=10 \leqq 4t$より, $t=3$ (tは最小).
- $t=3$なので, α, α^2, α^3, α^4, α^5, α^6を根とする多項式が生成多項式となる.
- これらのうち, α, α^2, α^4を根とする最小多項式$M(X)$は同じとなる($M_1(x)$). 同様に, α^3, α^6を根とする最小多項式は両方とも$M_3(x)$となる.
- 結局, 生成多項式$G(x)$は,

$$G(x)=\mathrm{LCM}(M_1(x), M_3(x), M_5(x)) = M_1(x) M_3(x) M_5(x) = (x^4+x+1)(x^4+x^3+x^2+x+1)(1+x+x^2) = x^{10}+x^8+x^5+x^4+x^2+x+1$$

12.33 重要な巡回符号：BCH符号の最小距離

- BCH符号の符号多項式は生成多項式で割り切れるのだから、
  $\alpha, \alpha^2, \ldots, \alpha^{2t}$
  を根として持たなければならない。従って、BCH符号の検査行列Hは、次のように書ける。

$$H = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \cdots & \alpha^{n-1} \\ \left(\alpha^2\right)^0 & \left(\alpha^2\right)^1 & \left(\alpha^2\right)^2 & \cdots & \left(\alpha^2\right)^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \left(\alpha^{2t}\right)^0 & \left(\alpha^{2t}\right)^1 & \left(\alpha^{2t}\right)^2 & \cdots & \left(\alpha^{2t}\right)^{n-1} \end{bmatrix}$$

  - α：GF（2^m）の原始元（原始多項式の根）とする
  - 行列Hの要素 $(\alpha^i)^j$ はGF（2）上のm次元列ベクトル表現されているとみなす（例えば、α＝（0100），α^2＝（0010）など）
- 符号の最小距離は、「行列Hの一次独立な列の数+1」 に等しいことが言えるので、一時独立な列数を求めればよい

12.33 重要な巡回符号：BCH符号の最小距離

- 行列Hの任意の2t列からなる行列の**行列式**をDとする。即ち、下記の式を計算する。

$$D = \begin{vmatrix} \alpha^{i1} & \alpha^{i2} & \cdots & \alpha^{i_{2t}} \\ \left(\alpha^{2}\right)^{i1} & \left(\alpha^{2}\right)^{i2} & \cdots & \left(\alpha^{2}\right)^{i_{2t}} \\ \vdots & \vdots & \vdots & \vdots \\ \left(\alpha^{2t}\right)^{i1} & \left(\alpha^{2t}\right)^{i2} & \cdots & \left(\alpha^{2t}\right)^{i_{2t}} \end{vmatrix}$$

ここで、

$0 \le i_1 < i_2 < \cdots < i_{2t} \le n-1$

とする。

- 上記Dの第1列から α^{i_1}、第2列から α^{i_2}、等を外に出せば、次のように変形できる。

12.33 重要な巡回符号：BCH符号の最小距離

$$D = \alpha^{i_1+i_2+\cdots+i_{2t}} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ (\alpha)^{i_1} & (\alpha)^{i_2} & \cdots & (\alpha)^{i_{2t}} \\ \vdots & \vdots & \vdots & \vdots \\ (\alpha^{i_1})^{2t-1} & (\alpha^{i_2})^{2t-1} & \cdots & (\alpha^{i_{2t}})^{2t-1} \end{vmatrix}$$

- 上記の行列式は、Van der Monde（ファンデルモンデ）の行列式と呼ばれるもので、$1 \leqq k < l \leqq 2t$となる全てのk, lの組について、$\alpha^{i_l} - \alpha^{i_k}$の積をとったものに等しい。従って、次式のようにかける。

$$D = \alpha^{i_1+i_2+\cdots+i_{2t}} \prod_{1 \leq k < l \leq 2t} (\alpha^{i_l} - \alpha^{i_k})$$

- 上記の $\alpha^{i_l} - \alpha^{i_k}$は、全て異なるので、$D \neq 0$。これは、Hの任意の2t列から成る行列が正則であること、即ちHの任意の2t列が一次独立であること、を意味する。
- これより、最小距離は、2t+1以上となる。

12.33 重要な巡回符号：BCH限界

- 上記の証明を少し修正すれば、巡回符号の**生成多項式が連続した（d−1）個のαのべき乗**、

$$\alpha^{l}, \alpha^{l+1}, \cdots, \alpha^{l+d-2}$$

を根としてもつならば、この巡回符号の最小距離がd以上である、ことが証明できる。

すなわち，生成多項式の根が，原始元αの連続する冪乗数より1つ大きい値が最小距離となる．

- これを**BCH限界**と言う。

12.34 重要なBCH符号：非2元BCH符号

- BCH符号は、一般のガロア体GF (q) 上の非2元符号に拡張できる
- GF (q^m) の原始元をαとし、$\alpha, \alpha^2, \ldots, \alpha^{2t}$を根とする最小次数の多項式を生成多項式とすれば、
  - 符号長：$n=q^m-1$
  - 情報点数：$k \geqq q^m-1-2mt$
  - 検査点数：$n-k \leqq 2mt$
  - 最小距離：$d \geqq 2t+1$

  （式１）

  の巡回符号が得られる。これが非2元BCH符号。
  - （式１）は．BCH符号の，「2→q」に一般化したもの．
- 非2元なので，符号シンボルは{0，1}の2値でなく多値になる．特に，GF (2) のm次拡大体GF (2^m) の元として構成されることが多い．

（参考）非2元符号について

- 非2元符号
  - 符号シンボルが {0,1,2,3...} のように，2以上のアルファベットを含む符号
- 2元符号のブロック化による非2元符号
  - GF (2^m) では，mビットの0,1記号をベクトル表現でGF (2^m) の要素に対応づけることができる．

（例）m=3の場合，3ビットづつのブロック化により，GF (2^3) の8個の元に対応づけることができる．

１００１１１０１１０００１０１

を3ビットづつに区切ると，

１００, １１１, ０１１, ０００, １０１

となる．これを10進数値記号で表せば，4, 7, 3, 0, 5

となるが，GF (2^3) の元に対応させ，原始元αとそのべき乗を用いて，

α^2, α^5, α^3, 0, α^6, となる．

（参考）非2元符号の多項式表現

- 符号多項式 F (x)
  - 符号語($c_{n-1}, c_{n-2}, \ldots, c_0$) に対する多項式は，
  - $F(x) = c_{n-1}X^{n-1} + c_{n-2}X^{n-2} + \cdots + c_0,\ c_i \in GF(q)$
  - 前ページ例の場合，$q=2^3=8$,であり，$n=7$とすると，符号語は(4, 7,3,0,5) または(α^2, α^5, α^3, 0, α^6) であるので，

    $F(x) = 4X^6 + 7X^5 + 3X^4 + 0X^3 + 5X^2$

    $= \alpha^2X^6 + \alpha^5X^5 + \alpha^3X^4 + 0X^3 + \alpha^6x^2$

    となる.
- 生成多項式，パリティ検査多項式
  - 同様に，多項式の係数がGF (q) の要素となる.

12.35 重要なBCH符号：リードソロモン(RS) 符号

- 非2元BCH符号の中で重要なものがリードソロモン (RS) 符号。これは、m=1の非2元BCH符号である。
- GF (q) の原始元αに対して、

$$G(x) = (x - \alpha)(x - \alpha^2)\cdots(x - \alpha^{2t})$$

を生成多項式とする、符号長n=q−1,情報点数k=q−1−2tとなるq元巡回符号。

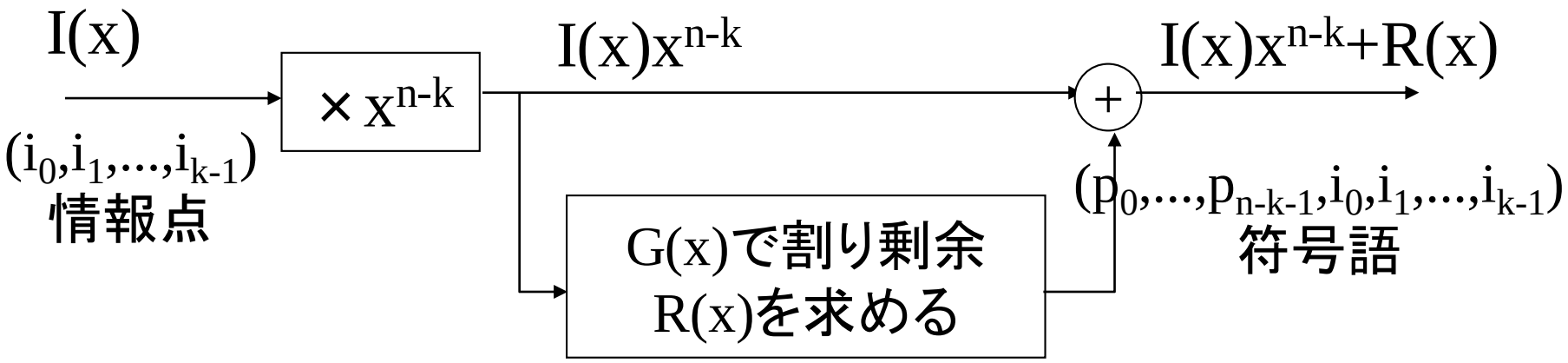
- 生成多項式の項数は2t+1となるので、最小距離はd_{min}=2t+1となる。t重誤り訂正符号。
- RS符号の例：
  - GF (2^4) の元をもつ、次の生成多項式G (x) をもつ符号は、 t=3となり， 3重誤り訂正符号のRS符号となる。

$$G(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4)(x + \alpha^5)(x + \alpha^6)$$
$$= x^6 + \alpha^{10}x^5 + \alpha^{14}x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^9 x + \alpha^6$$

12.36 巡回符号の符号化回路

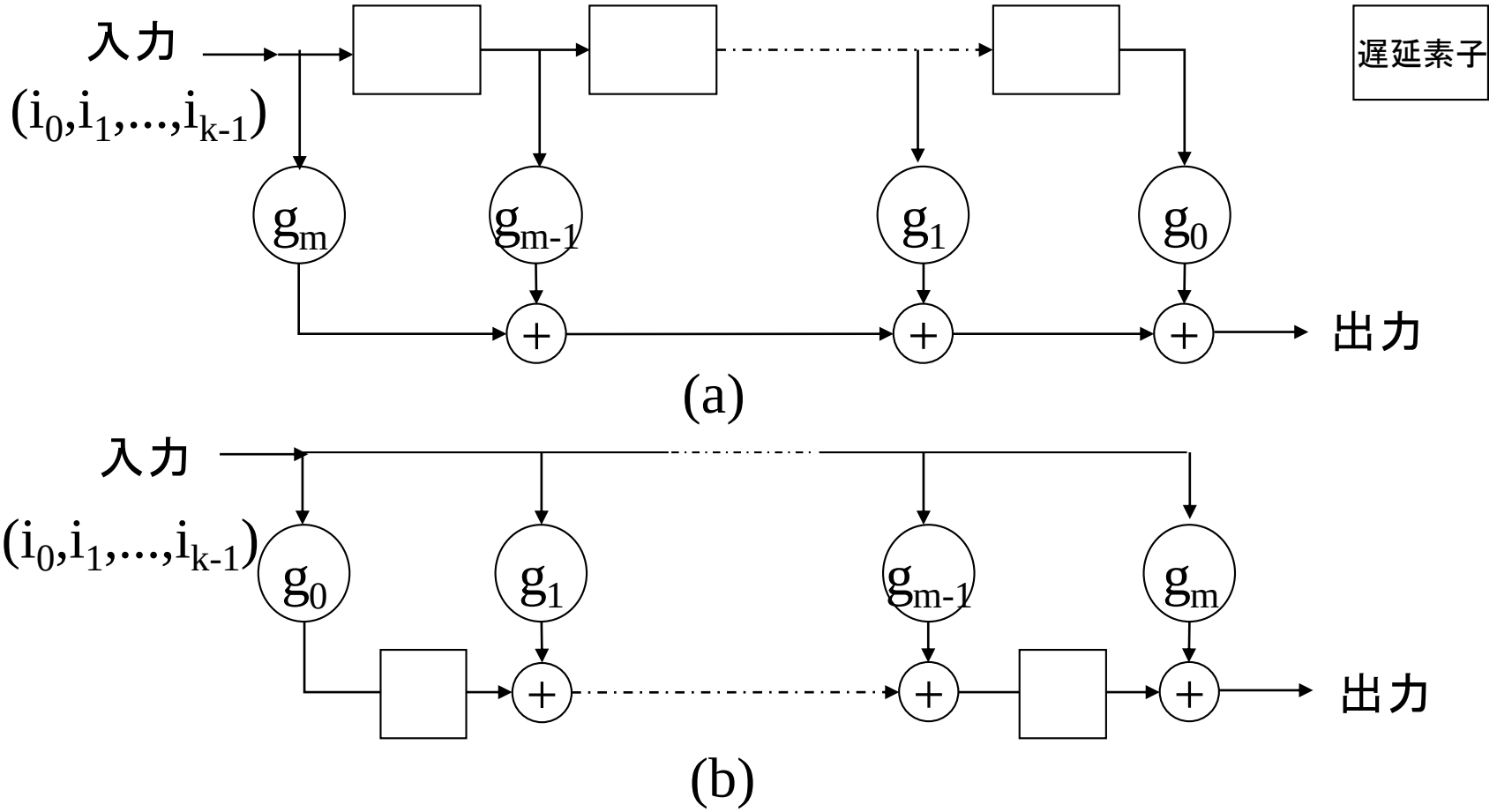
- 巡回符号の特徴の１つは、符号化回路を簡単に構成できること。・・・・符号の評価尺度の1つ
- 前提条件として次の符号を考える：
  - 符号長：n、情報点数：k、検査点数：m=n-k
  - 生成多項式 G(x) から作られる2元巡回符号
    - 巡回符号であるから、G(x) はx^n-1を割り切る。即ち、$x^n-1=G(x)*Q(x)$となる多項式Q(x) が存在する。
    - $G(x)=g_0+g_1x+g_2x^2+\cdots+g_mx^m$、とする（次数=検査点数）。
- m段シフトレジスタによる多項式の乗算回路を用いて、簡単に符号化が行える。

12.36 巡回符号の符号化回路図



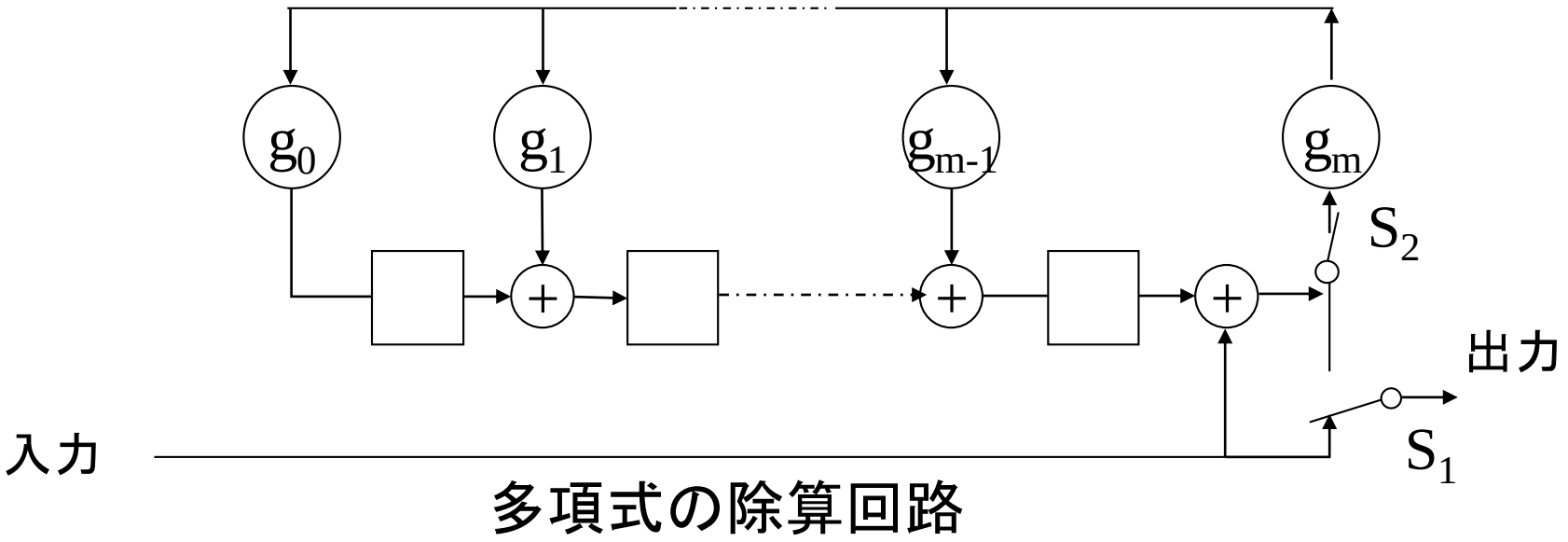
- kビットの情報$i=(i_0,i_1,\ldots,i_{k-1})$は、多項式 $I(x)=i_0+i_1x+\cdots+i_{k-1}x^{k-1}$ で表わされる。$I(x)$にx^mを掛け、それを$G(x)$で割った剰余多項式を $R(x)=p_0+p_1x+\cdots+p_{m-1}x^{m-1}$ で表わす。すなわち、$R(x)$は、 $I(x)x^m=Q(x)G(x)+R(x)$ となるm−1次以下の多項式。
- $X(x)=I(x)x^m-R(x)=I(x)x^m+R(x)$ とおくと、$X(x)=Q(x)G(x)$となるので、$X(x)$は符号多項式となる。$X(x)$をベクトル表現すると、 $x=(p_0,p_1,\ldots,p_{m-1},i_0,i_1,\ldots,i_{k-1})$ となり、右のkビットに情報点、左のmビットに検査点、が現れる構成となる。$(m=n-k)$

12.36 m段シフトレジスタによる符号化回路



- **入力側から順次に情報点を**k**個入れて**$(i_0,i_1,\ldots,i_{k-1})$**、さらにこの回路を**m=n-k**だけシフトさせると、全体で**n**桁の符号語が出力側から取り出せる。**
- **出力系列が**G(x)**で割り切れることが分かる。しかし欠点は、情報点と符号語桁が対応しないこと。**

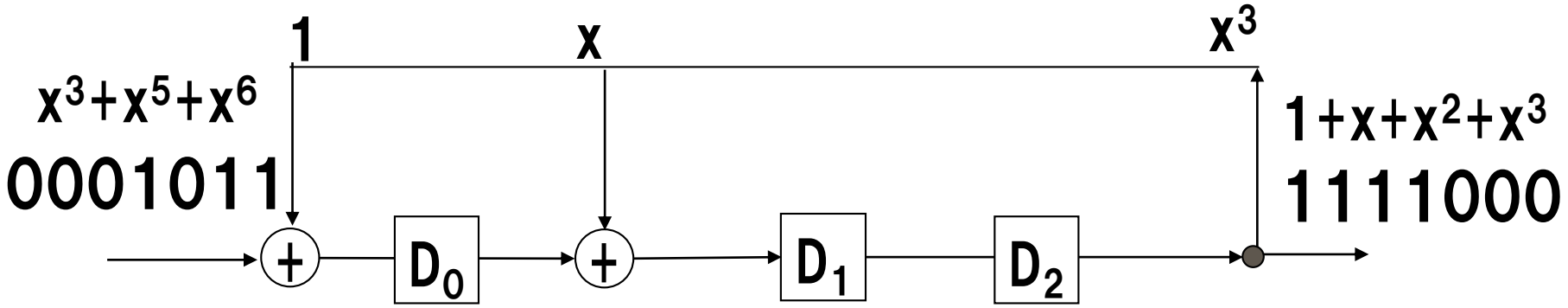
12.36 m段シフトレジスタによる符号化回路(２)



多項式の除算回路

- 入力から、a_{n-1},a_{n-2},...の順にa_{n-k+1}までスイッチS_1を下に倒し、スイッチS_2を閉じたまま情報点を出力に送り込むと同時に、シフトレジスタの中にも送り込む。
- シフトレジスタの中で割り算が行われ、最後にシフトレジスタには、$x^m(a_{n-k+1}+a_{n-k+2}x+\cdots+a_{n-2}x^{k-2}+a_{n-1}x^{k-1})$を$G(x)$で割った剰余$R(x)$が残る。
- 従って、ここでスイッチS_1を上に倒し、S_2を開いて剰余$R(x)$を送り出せばよい。本方法では、符号語の最初のk桁が情報点を表わす。

12.36 シフトレジスタによる割り算回路(例)



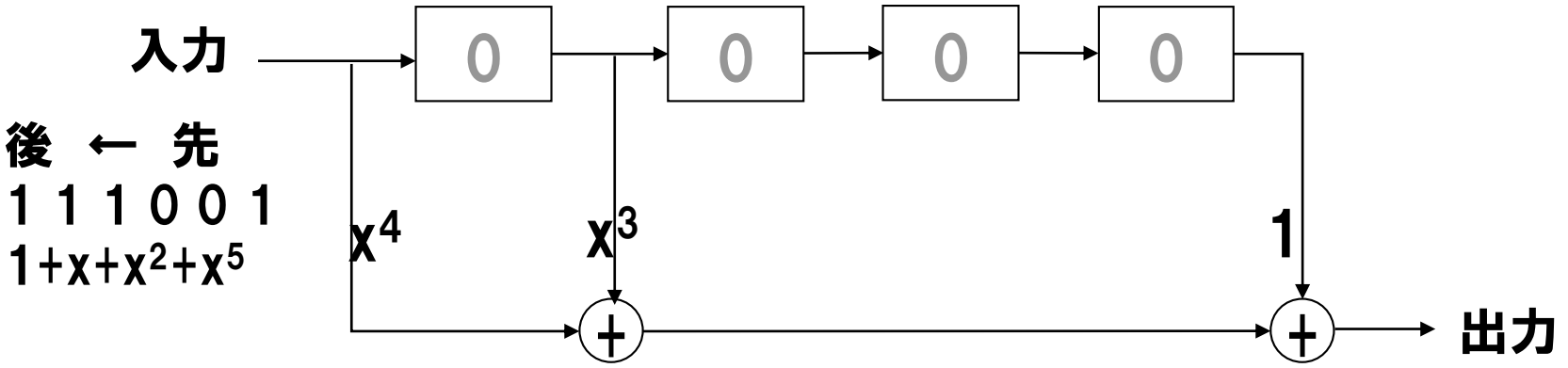
G(x)=1+x+x3で割り算を行う回路

	入力	D_0	D_1	D_2	出力
高次	1	0	0	0	0
	1	1	0	0	0
	0	1	1	0	0
	1	0	1	1	1
	0	0	1	1	1
	0	1	1	1	1
	0	1	0	1	1
t 低次		1	0	0	

割り算過程

```
          1111
1011)1101000
     1011
     01100
      1011
      01110
       1011
       00101
        1011
        00010
         1011
         00001
```

12.36 シフトレジスタによる掛け算回路(例)-1



B(x)=1+x³+x⁴を掛ける掛け算回路

A(x)=1+x+x²+x⁵とB(x)の乗算手順

B(x)

$x^4 \cdot A(x) =$ $x^4+x^5+x^6$ $+x^9$

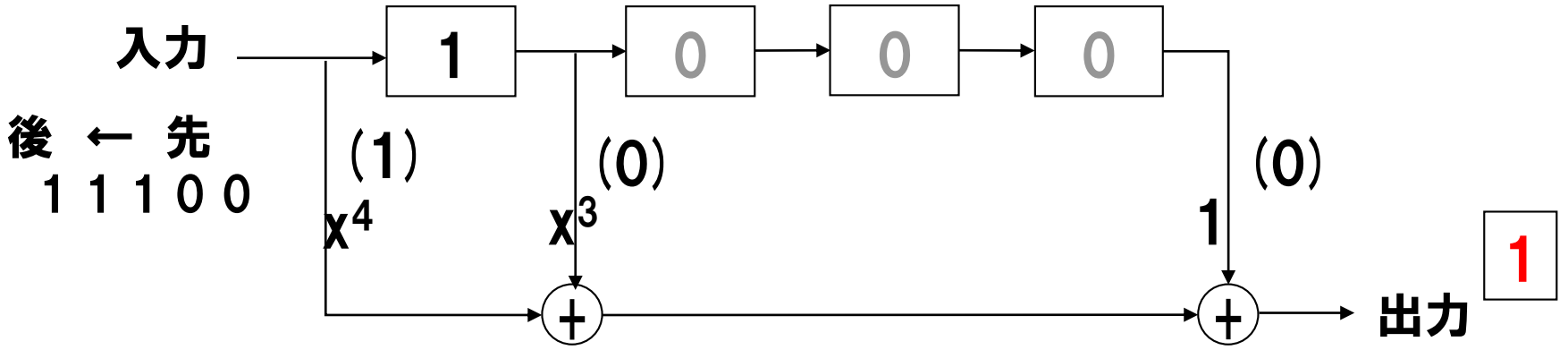
$x^3 \cdot A(x) =$ $x^3+x^4+x^5+$ $+x^8$

$1 \cdot A(x) = 1+x+x^2$ $+x^5$

$B(x) \cdot A(x) = 1+x+x^2+x^3$ $+x^5+x^6$ $+x^8+x^9$

$\Rightarrow$ 1 1 1 10 1 1 0 1 1

12.36 シフトレジスタによる掛け算回路(例)-2



B(x)=1+x³+x⁴を掛ける掛け算回路

A(x)=1+x+x²+x⁵とB(x)の乗算手順

B(x)

x⁴・A(x) = x⁴+x⁵+x⁶ +x⁹

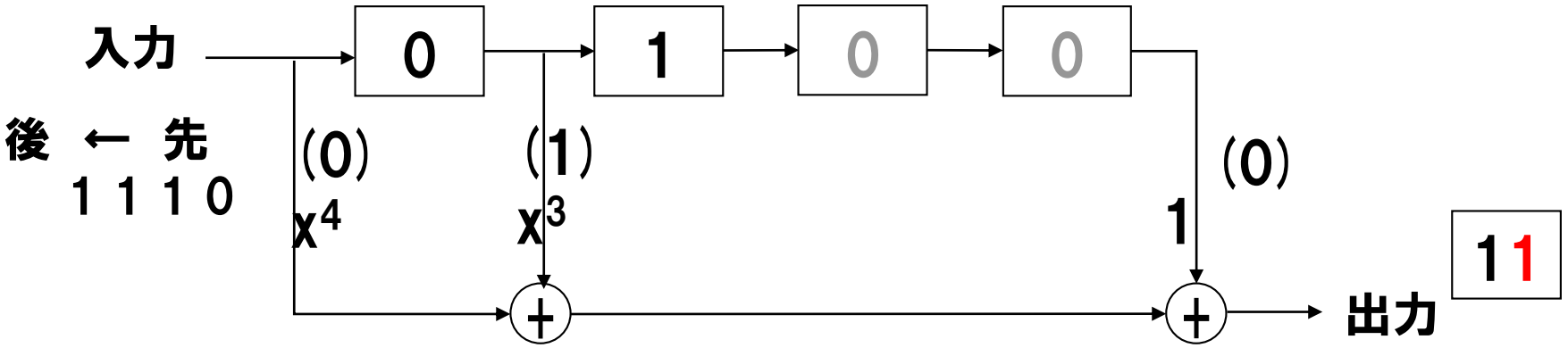
x³・A(x) = x³+x⁴+x⁵+ +x⁸

1・A(x) =1+x+x² +x⁵

B(x)・A(x) =1+x+x²+x³ +x⁵+x⁶ +x⁸+x⁹

⇒ 1 1 1 10 1 1 0 1 1

12.36 シフトレジスタによる掛け算回路(例)-3



B(x)=1+x³+x⁴を掛ける掛け算回路

A(x)=1+x+x²+x⁵とB(x)の乗算手順

B(x)

x⁴・A(x) = x⁴+x⁵+x⁶ +x⁹

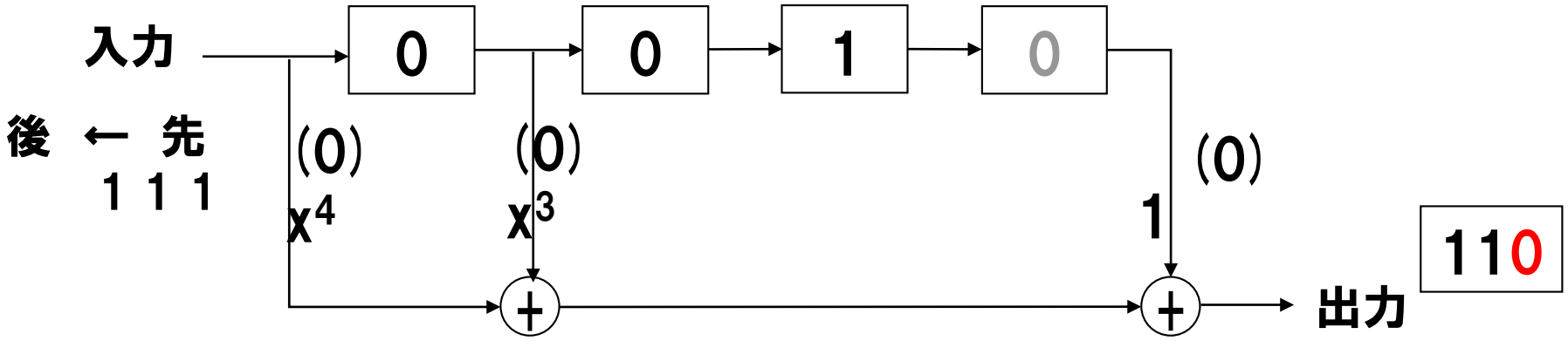
x³・A(x) = x³+x⁴+x⁵+ +x⁸

1・A(x) =1+x+x² +x⁵

B(x)・A(x) =1+x+x²+x³ +x⁵+x⁶ +x⁸+x⁹

⇒ 1 1 1 10 1 1 0 1 1

12.36 シフトレジスタによる掛け算回路(例)-4



B(x)=1+x³+x⁴を掛ける掛け算回路

A(x)=1+x+x²+x⁵とB(x)の乗算手順

B(x)

$x^4 \cdot A(x) =$ $x^4+x^5+x^6+x^9$

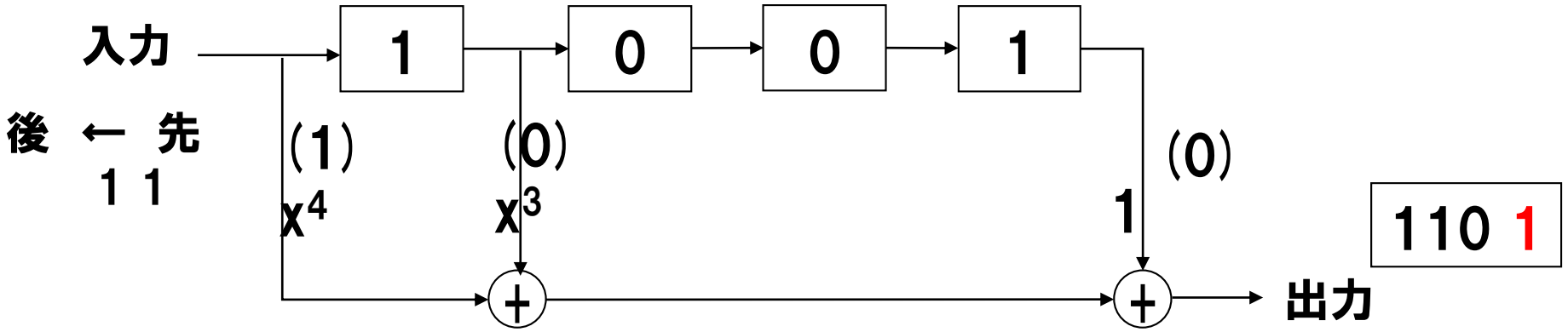
$x^3 \cdot A(x) =$ $x^3+x^4+x^5+x^8$

$1 \cdot A(x) = 1+x+x^2+x^5$

$B(x) \cdot A(x) = 1+x+x^2+x^3+x^5+x^6+x^8+x^9$

⇒1 1 1 10 1 1 0 1 1

12.36 シフトレジスタによる掛け算回路(例)-5



B(x)=1+x³+x⁴を掛ける掛け算回路

A(x)=1+x+x²+x⁵とB(x)の乗算手順

B(x)

$x^4 \cdot A(x) =$ $x^4+x^5+x^6$ $+x^9$

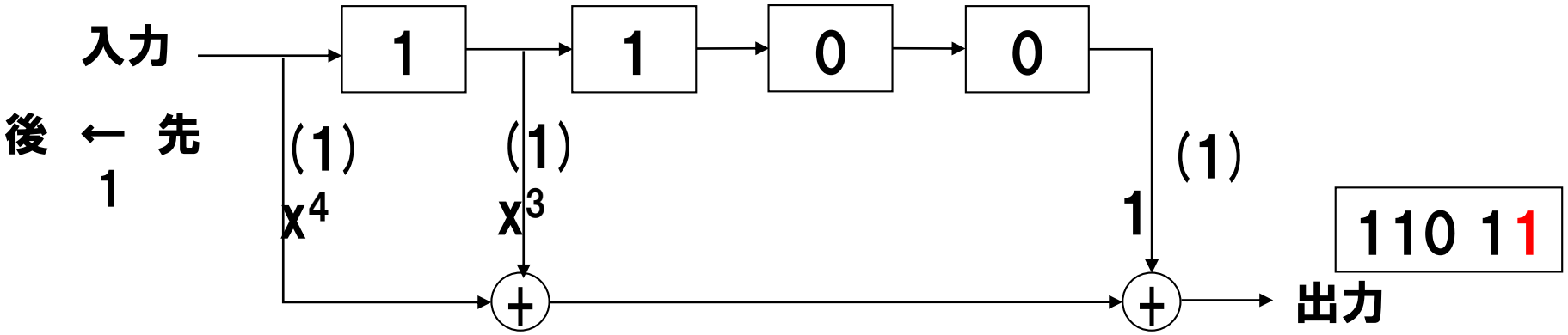
$x^3 \cdot A(x) =$ $x^3+x^4+x^5+$ $+x^8$

$1 \cdot A(x) = 1+x+x^2$ $+x^5$

$B(x) \cdot A(x) = 1+x+x^2+x^3$ $+x^5+x^6$ $+x^8+x^9$

⇒1 1 1 10 1 1 0 1 1

12.36 シフトレジスタによる掛け算回路(例)-6



B(x)=1+x³+x⁴を掛ける掛け算回路

A(x)=1+x+x²+x⁵とB(x)の乗算手順

B(x)

$x^4 \cdot A(x) =$ $x^4+x^5+x^6$ $+x^9$

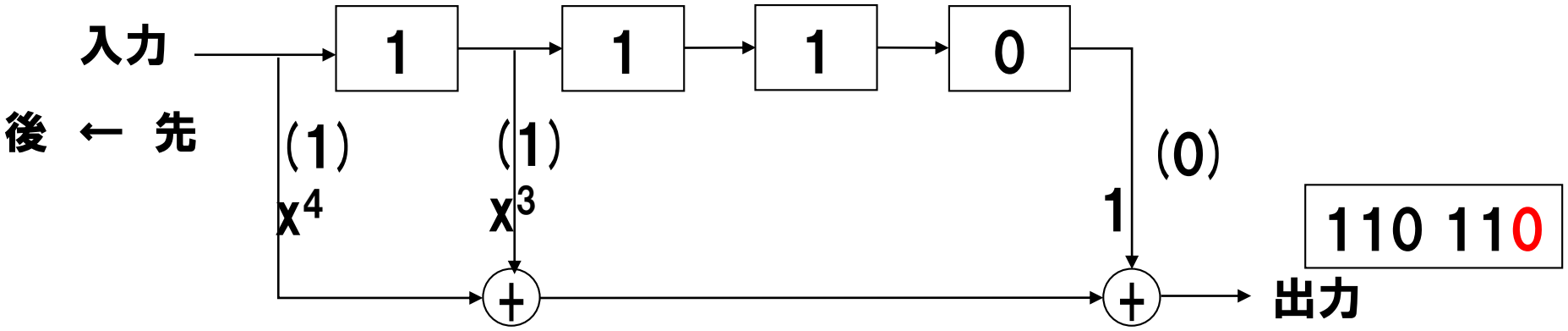
$x^3 \cdot A(x) =$ $x^3+x^4+x^5+$ $+x^8$

$1 \cdot A(x) = 1+x+x^2$ $+x^5$

$B(x) \cdot A(x) = 1+x+x^2+x^3$ $+x^5+x^6+x^8+x^9$

⇒1 1 1 10 1 1 0 1 1

12.36 シフトレジスタによる掛け算回路(例)-7



B(x)=1+x³+x⁴を掛ける掛け算回路

A(x)=1+x+x²+x⁵とB(x)の乗算手順

B(x)

$x^4 \cdot A(x) =$ $x^4+x^5+x^6$ $+x^9$

$x^3 \cdot A(x) =$ $x^3+x^4+x^5+$ $+x^8$

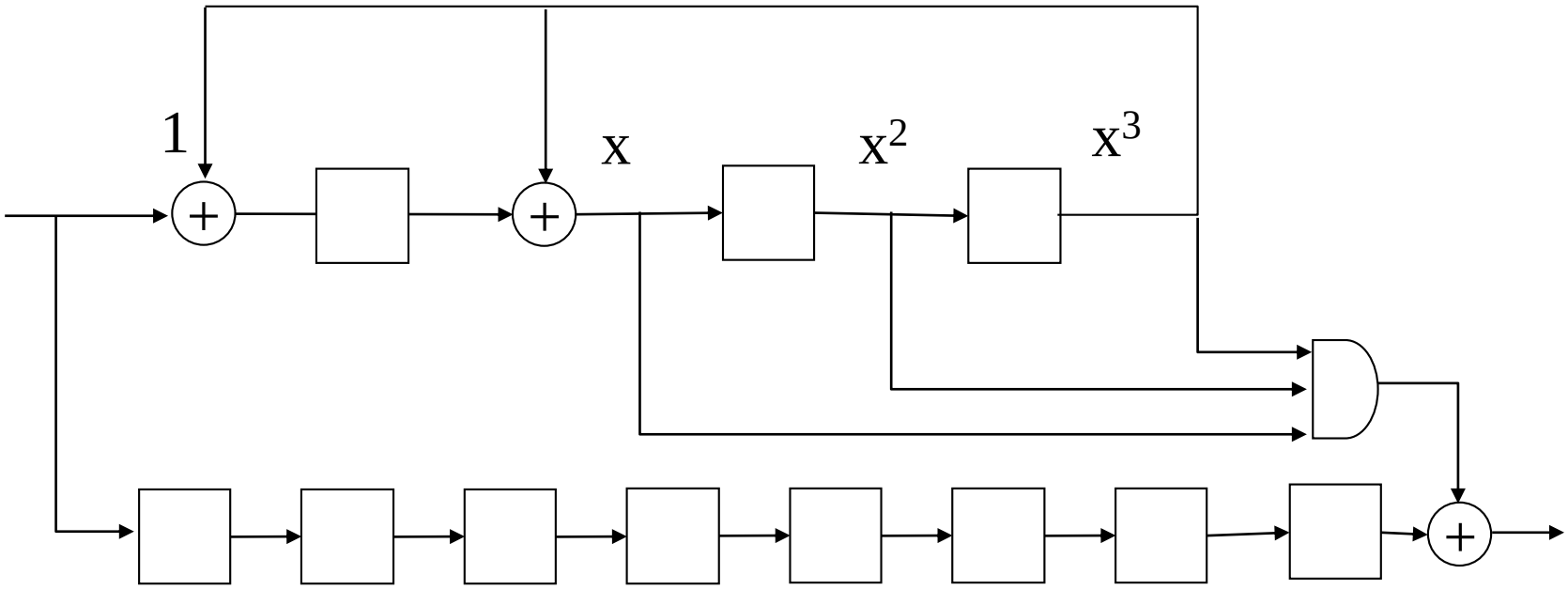
$1 \cdot A(x) = 1+x+x^2$ $+x^5$

$B(x) \cdot A(x) = 1+x+x^2+x^3 +x^5+x^6 +x^8+x^9$

⇒ 1 1 1 1 0 1 1 0 1 1

12.37 巡回ハミング符号の復号器

- 生成多項式$G(x)=1+x+x^3$の巡回ハミング(7,4)の復号器
  - 7ビットの受信語が読みこまれた次の時点から、訂正された符号語が出力される。この間は入力をゼロにする。



12.38 最大長系列符号と復号法

- k次の原始多項式を検査多項式とする符号長$n=2^k-1$の巡回符号を最大長系列符号（M系列符号）という
- 検査多項式の次数＝情報点数なので、この符号は$(2^k-1, k)$巡回符号となる
- 最小距離$d_{min}=2^k-1$ （証明省略）
- 情報速度$R=k/(2^k-1)$は非常に小さい
- 符号語（0以外）は最大長系列（M系列）となる
  - 見かけ上ランダムな周期的系列の1周期となっている
    - k段シフトレジスタ回路で発生する周期が最大(2^k-1)の系列
- 多数決論理による復号が可能

12.39 BCH符号の復号法

- 受信語を表わす多項式

$Y(x)=y_0+y_1x+\cdots+y_{n-1}x^{n-1}$

とする. これに対して、

- $S_i=Y(\alpha^i)$, $i=1,2,\ldots,2t$

なるシンドローム$S_1,S_2,\ldots,S_{2t}$を定義する。これらは、GF(2^m)の元であるが、GF(2)上のm次元ベクトルで表現される.

- 誤りパターンを表わす多項式を$E(x)=e_0+e_1x+\cdots+e_{n-1}x^{n-1}$とすれば、$S_i=E(\alpha^i)$, $i=1,2,\ldots,2t$ となる.
- $Y(x^2)=[Y(x)]^2$であるので、$S_{2i}=(S_i)^2$となる.
  - 偶数番目のシンドロームは他のシンドロームから計算できる.
- 誤りがl個$j_1,j_2,\ldots,j_l$, $(l\leqq t)$の位置に生じたと仮定する.
  - $0\leqq j_1<j_2<\ldots<j_l\leqq n-1$

12.39 BCH符号の復号法

$$S_i = \alpha^{ij_1} + \alpha^{ij_2} + \cdots + \alpha^{ij_L}$$

- **BCH符号の復号は、このシンドロームから誤り位置 $j_1, j_2, \ldots, j_L$ を求めること。直接は困難なので、まず**

$$\sigma(z) = (1 - \alpha^{j_1} z)(1 - \alpha^{j_2} z) \cdots (1 - \alpha^{j_L} z)$$

というGF (2^m) の元を係数とするL次多項式を求める。

$\sigma(z)$ を誤り位置多項式と呼ぶ。

$\sigma(z)$ の根は $\alpha^{-j1}, \alpha^{-j2}, \ldots, \alpha^{-jL}$ となり、これより誤り位置を求められる。

12.39 BCH符号の復号法

下記のように手順がまとめられる。

1. 受信語からシンドローム$S_1, S_2, \ldots, S_{2t}$を求める
2. シンドロームが全て0ならば誤りなしと判定する
3. シンドロームに0でないものがあれば、シンドロームから**誤り位置多項式 σ (z)** を求める
4. σ (z) の根 $\alpha^{-j1}, \alpha^{-j2}, \ldots, \alpha^{-jL}$を求める

   これは σ (z) にGF (2^m) の元を次々と代入して求まる。
5. $\alpha^{-j1}, \alpha^{-j2}, \ldots, \alpha^{-jL}$から$j_1, j_2, \ldots, j_L$を求め、これらの位置の記号を訂正する

12.39 BCH符号の復号法(適用例)

- 原始多項式$1+x+x^4$で生成される2重誤り訂正BCH(15,7)符号の、復号法は以下のとおり
- 受信語y=(100000101000000)とする

多項式表現では$R(x)=1+x^6+x^8$。

(1)シンドロームは$S_1=Y(\alpha)=1+\alpha^6+\alpha^8=\alpha^3$,
$S_3=Y(\alpha^3)=1+\alpha^{18}+\alpha^{24}=\alpha^4$ となる。

ここで、α: 原始多項式の根, $1+\alpha+\alpha^4=0$

(2)$\sigma(z)=1+\alpha^3 z+(\alpha^9+\alpha^4)\,\alpha^{-3}z^2=1+\alpha^3 z+\alpha^{11}z^2$

(3)(4)この根を$z=1,\alpha,\alpha^2,\ldots$を順々に代入して求めると、
$\alpha^8=\alpha^{-7}$, $\alpha^{11}=\alpha^{-4}$であることが分かる。

- 従って、位置4, 7に誤りが生じたと判定される
- 送信符号語は、x=(1000101111000000)

12.39 BCH符号の復号法: 誤り位置多項式

- t=2の場合はシンドロームを用いてσ(z)を簡単な形で表わすことが可能。しかし、tが大きくなると、実際上不可能。⇒シンドロームからσ(z)を効率よく計算する方法を考える必要がある。
- シンドロームを係数とする多項式S(z)を考える:
- $S(z)=S_1+S_2z+\cdots+S_{2t}z^{2t-1}$
- ここで、次の式が成り立つことを用いると、

$$\frac{\alpha^{j_i}}{1-\alpha^{j_i}z}=\alpha^{j_i}+\alpha^{2j_i}z+\alpha^{3j_i}z^2+\alpha^{4j_i}z^3+\cdots$$

12.39 誤り位置多項式の導出

- S(z)は下記のようになる。

$$S(z) \equiv \sum_{i=1}^{l} \frac{\alpha^{j_i}}{1-\alpha^{j_i} z} \bmod z^{2t}$$

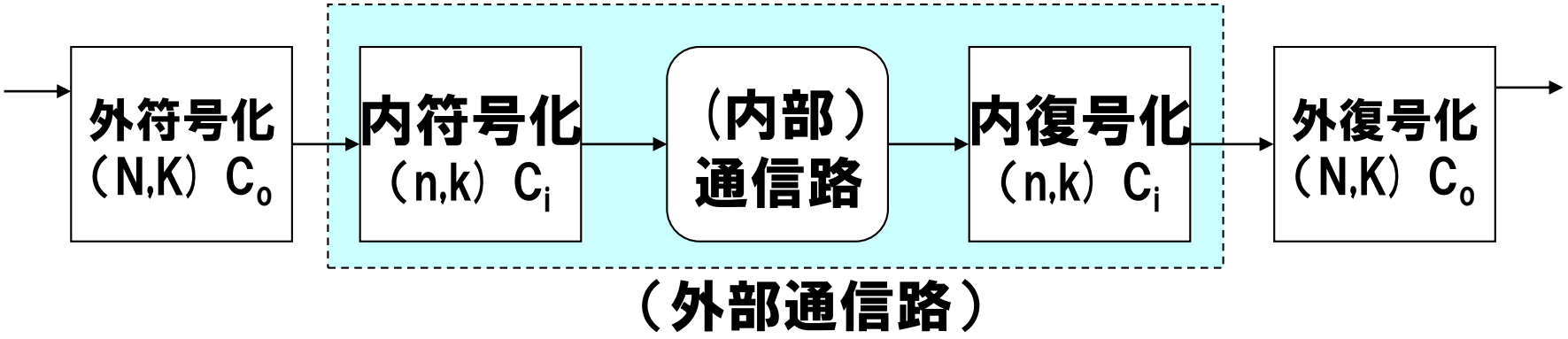
$$\Rightarrow \quad \sigma(z)S(z) \equiv \omega(z) \bmod z^{2t}, \qquad \omega(z) = \sum_{i=1}^{l} \alpha^{j_i} \prod_{k \neq i} (1-\alpha^{j_k} z)$$

- deg ω(z) ＜ deg σ(z)である。また、ω(z)とσ(z)は互いに素である（最大公約数が定数）。
- 上記の式から、適当な多項式A(z)を用いて、
  $A(z)z^{2t} + \sigma(z)S(z) = \omega(z)$ ・・・・・・・・・・・・・・・・・・（１）
  と書き直せる。
- l（誤り個数）≦tとしているから、
  deg ω(z) ＜ deg σ(z) ≦t ・・・・・・・・・・・・・・・・・・（２）
  でなければならない。

12.39 誤り位置多項式の導出

- 上記(１)(２)を満たす互いに素な多項式σ(z)とω(z)は定係数の違いを除き一意的に定まる。(証明略)
- この2つのσ(z)，ω(z)はz^{2t}とS(z)の最大公約多項式を求めるユークリッド互除法により求められる。

12.40 その他の符号：連接符号concatenated code



- **連接符号**とは，２つの符号化を直列につなげたもの．通信路に近い符号を内符号，遠い符号を外符号という．
  - 内符号C_iを (n, k) 符号，外符号を(N, K) 符号とすると，「内符号＋通信路」の部分に対して外符号はkビットを１つの情報シンボルとして符号化を行う．
  - 両方がブロック符号のとき，全体の符号長=nN，情報点数=kK，符号速度(符号化率)=kK/nN
- 通常，内符号=2元ランダム誤り訂正符号，外符号=GF (2k) を元とするシンボル誤り訂正符号，が用いられる．
- 例1：デジタル放送などでは，内符号=畳込み符号，外符号=RS符号
- 例2: 内符号=BCH符号，外符号=RS符号，など．

13. 誤り訂正符号(畳み込み符号)

13.1 畳み込み符号(概要)
13.2 畳み込み符号の定義
13.3 畳み込み符号器
13.4 畳み込み符号の性質
13.5 畳み込み符号の符号器
13.6 畳み込み符号の生成行列
13.7 畳み込み符号の復号法
13.8 自己直交符号
13.9 繰り返し符号と多数決論理復号法
13.10 最尤復号:ビタビアルゴリズム

13.1 畳み込み符号(概要)

- ブロック符号(ハミング符号、巡回符号など)
  - 符号化を一定のブロック単位で行う
  - 前後のブロックで符号化に影響を与えない
- **畳み込み(たたみこみ)符号**
  - 符号化はブロック単位で行う
  - 過去のブッロクが現在のブロックに影響を及ぼす
  - ブロック長はブロック符号に比べて短いことが一般的
- 代数的にきれいに扱うことが困難
- しかし、実用的には通信への応用など広く使われる
- 理由は同じ複雑さであれば、誤り訂正能力が高いため

13.2 畳み込み符号の定義

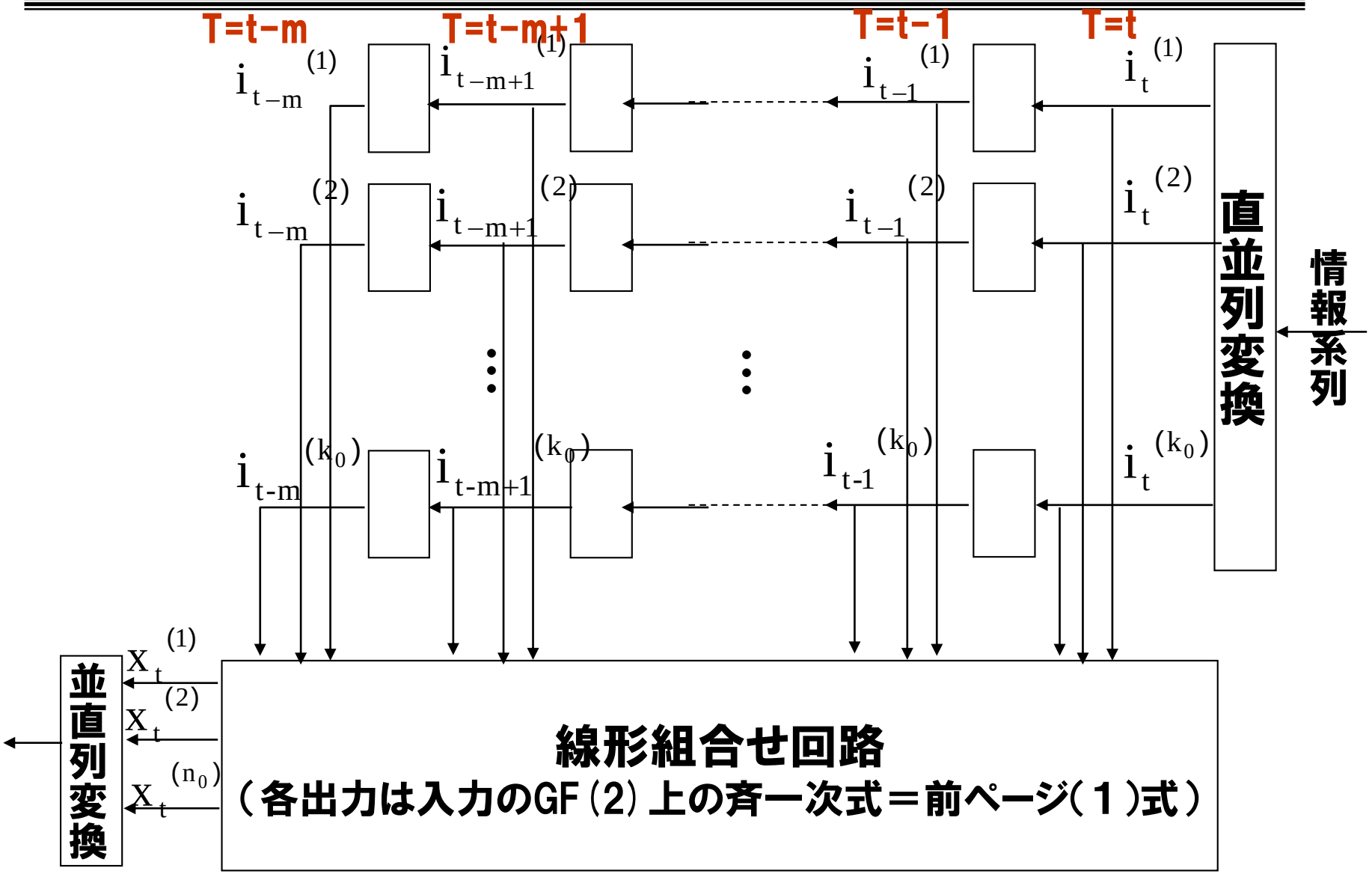
- 情報系列は長さk_0ビットのブロックに分割され、各ブロックのk_0ビットは並列化される。⇒**直並列変換**
- 時刻t (t=0,1,2,...) における並列化された**k_0個の情報ビット**を
  $i_t^{(1)}, i_t^{(2)}, \cdots, i_t^{(k_0)}$ で表わす。
- これら情報ビットは縦続接続されたm個の遅延素子に入力される。各遅延素子の出力および直並列変換の出力が線形組み合わせ回路に入力される。この回路の出力
  $x_t^{(1)}, x_t^{(2)}, \cdots, x_t^{(n_0)}$ は次のとおりに書ける。

$$x_t^{(l)} = \sum_{k=1}^{k_0} \sum_{j=0}^{m} g_j^{(k,l)} i_{t-j}^{(k)}, \quad l = 1,2,...,n_0 \qquad \cdots (1)$$

- $g_j^{(k,l)}$ は0または1であり、式の演算はGF (2) 上で行う。
- **n_0個の出力**は直列に変換され(**並直列変換**)、通信路に送られる。<u>直列化された系列を**畳み込み符号**</u>という。

$$x = (x_0^{(1)}, x_0^{(2)}, \cdots, x_0^{(n_0)}, x_1^{(1)}, x_1^{(2)}, \ldots, x_1^{(n_0)}, x_2^{(1)}, \ldots\ldots,)$$

13.3 畳み込み符号器: Wozencraft形符号器



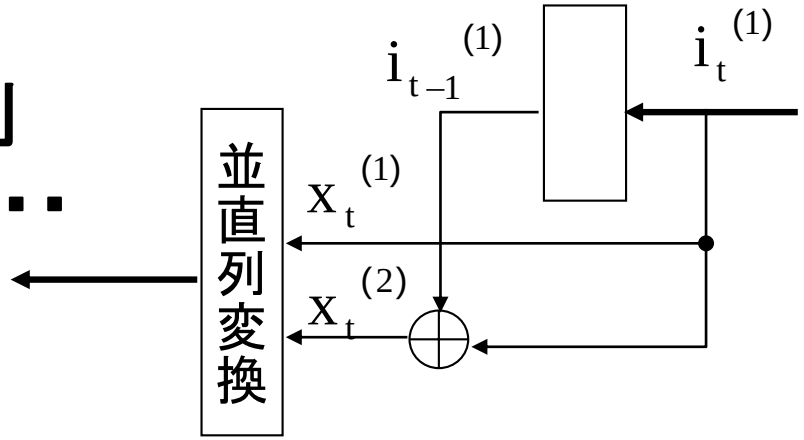
13.4 畳み込み符号の性質

- 情報速度 R= k_0/n_0（bit/記号）
- 拘束長（Constraint length） $n_A=(m+1)n_0$
  - あるブロックの情報ビットが影響が直接及ぶ最大の範囲
  - 直接影響を及ぼしうるブロック数$(m+1)$にn_0（各ブロックの符号長）を掛けた値
  - ブロック符号の符号長(n)に相当する値
    - 同じ程度の拘束長をもつ畳み込み符号と、符号長をもつ巡回符号とは同程度の複雑さ
- 例1：$n_0=2$, $k_0=1$, $m=1$,の畳み込み符号
  - 符号の情報速度は、$R=k_0/n_0=1/2$
  - 拘束長は、$n_A=(m+1)n_0=4$
  - 例えば、情報系列が、（1 0 0・・・）であれば、符号化系列は、（1 1 0 1 0 0 ・・・）、となり、最初の情報ビット 1の影響が$n_A=4$ビットの範囲に及ぶ

13.5 畳み込み符号の符号器

例1: $n_0=2$, $k_0=1$, $m=1$,の畳み込み符号の符号器

符号化系列
1 1 01 0 0・・・



情報系列
1 0 0・・・

- 符号器の構造から、畳み込み符号は線形性をもつ
  - 任意の2つの符号系列の和はまた符号系列となる
- 畳み込み符号にも生成行列を定義できる

13.6 畳み込み符号の生成行列

例1: $n_0=2$, $k_0=1$, $m=1$,の畳み込み符号の生成行列

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

- 行、列ともに無限の行列
- 情報系列をi= $(i_0^{(1)}, i_1^{(1)}, i_2^{(1)}, \ldots)$ とすると、符号化系列はx=i・Gとかける。
  - 例えば、i=（1 1 0 0 ...）とすると、xは第1行＋第2行となり、x=（1 1 1 0 0 1 0 ...）となる。

13.7 畳み込み符号の復号法

- シンドロームパターン検出による復号
  - 帰還復号法(フィードバック・デコーディング)
- 多数決論理復号法
- 最尤復号
  - ビタビ(Viterbi)アルゴリズムによる復号
  - 逐次復号法 (→説明省略)

13.7 シンドロームパターン検出による復号(1)

- シンドローム系列から特定の誤りパターンを検出して，これを訂正する方法
  - 例1: $n_0=2$, $k_0=1$, $m=1$,の畳み込み符号の検査行列

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

第1ブロック　第2ブロック

- 符号系列C= $(C_{11}, C_{12}, C_{21}, C_{22}, \ldots)$
- 誤り系列 e = $(E_{11}, E_{12}, E_{21}, E_{22}, \ldots)$
- シンドロームS=H・(C+e) =H・C+H・e=H・e

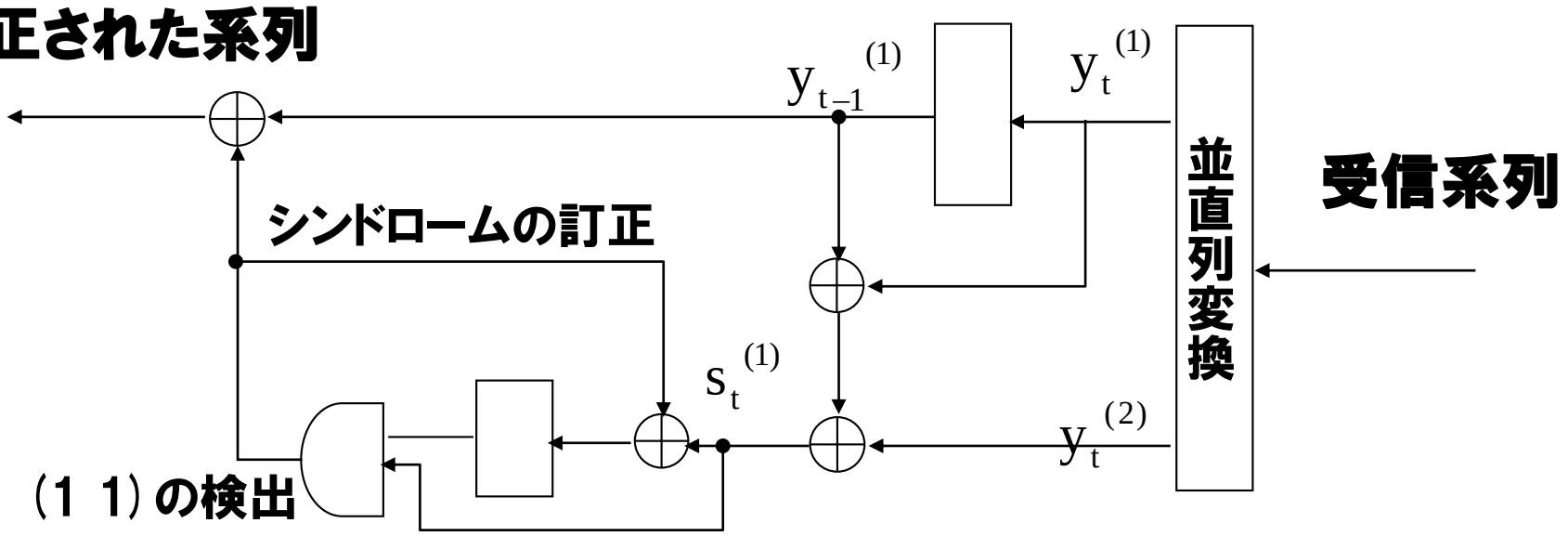
13.7 シンドロームパターン検出による復号(2)

- 誤りパターンの一例の場合
  - 下記の表の規則性より，シンドロームSの最初の2ビットを見て，誤り箇所を推定し復号できる（第1ブロックの訂正規則）.
  - 第2ブロックの訂正も同様に行う．ただし，第1ブロックの誤りの影響を系列から除去する必要あり．（→次ページの復号器）

誤り発生ケース	誤りパターンe	シンドロームS	誤り訂正
第1ブロックの第1ビットに誤りが発生し，第1，第2ブロックはそれ以外誤りなし	10 00 …	1 1 …	第1ブロック第1ビットを訂正
第1ブロックの第2ビット（検査ビット）に誤りが発生し，第1，第2ブロックはそれ以外誤りなし	01 00 …	1 0 …	第1ブロック第2ビットを訂正
第1ブロックに誤りなし	00 xx ….	0 x …	第1ブロック訂正せず

13.7 シンドロームパターン検出による復号(3)

単一誤り訂正畳込み符号の復号器の例



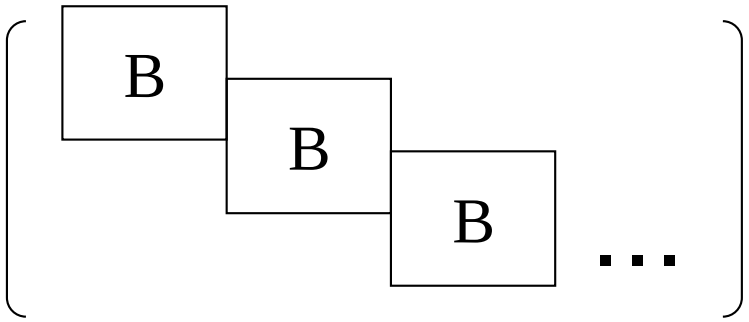
- シンドロームS= (1 1...) の場合，第1ブロックの第1ビットを訂正すると共に，シンドローム系列をS= (0 0 ...) に修正する．このようにすれば，第2ブロック復号も同様に行える．⇒この復号法を，帰還(フィードバック)復号法という．
- この方法の問題点は，一度復号誤りを起こすと誤ったシンドローム修正が行われ，それが後のブロックに伝搬し，後のブロックも復号誤りを起こしやすくなる．⇒誤り伝搬という

13.7 多数決論理復号法

- シンドロームパターン検出による復号法は，ランダム誤りの数が多い場合は複雑になる．
- これを解消する方法が，多数決論理による復号．
  - ただし，この方法が適用できる符号が「直交可能符号」に限られる．直交可能符号は誤り伝搬が無限の可能性があるので，誤り伝搬が有限に限定される「自己直交符号」に適用されることが多い．
  - ブロック符号の繰り返し符号の場合も，多数決論理復号が適用できた（→後述）．　その拡張とみなされる．
- 自己直交符号は，「第1ブロックの情報ビットに対する誤りパターンビット$e_{11},e_{12},..,e_{1k0}$，に対してそれを含むシンドロームビットがそのまま直交するパリティ検査和となる符号」と定義される．（第1ブロックに限ることはない）
- 自己直交符号の例
  - ブロック長$n_0=2$，ブロック内情報点数$k_0=1$，影響ブロック数$m=3$，拘束長$n_A=(m+1)n_0=8$．　→後述．

13.8 自己直交符号の例(1)

- 畳込み符号のパリティ検査行列Hは無限大の大きさになるが，有限次元の検査行列をBを少しづつずらしながら構成される.

- H= 

- B= $\begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}$ の例を考える.

13.8 自己直交符号の例 (2)

- 第1ブロックの復号を考える
  - 受信系列の拘束長までの部分$y_A = (y_{11}, y_{12}, y_{21}, y_{22}, y_{31}, y_{32})$を用いて復号する.
  - $y_A = x_A + e_A$, x_Aは符号系列, e_Aは誤り系列
  - yAからシンドローム系列のはじめの4ビットは完全に定まる:

$$
\begin{aligned}
s_{11} &= e_{11} + e_{12} \\
s_{21} &= e_{11} + e_{21} + e_{22} \\
s_{31} &= e_{21} + e_{31} + e_{32} \\
s_{41} &= e_{11} + e_{31} + e_{41} + e_{42}
\end{aligned}
$$

  - s_{11}, s_{21}, s_{41}はe_{11}に関して直交するパリティ検査和. 従って多数決論理復号が可能.

13.9 繰り返し符号と多数決論理復号法

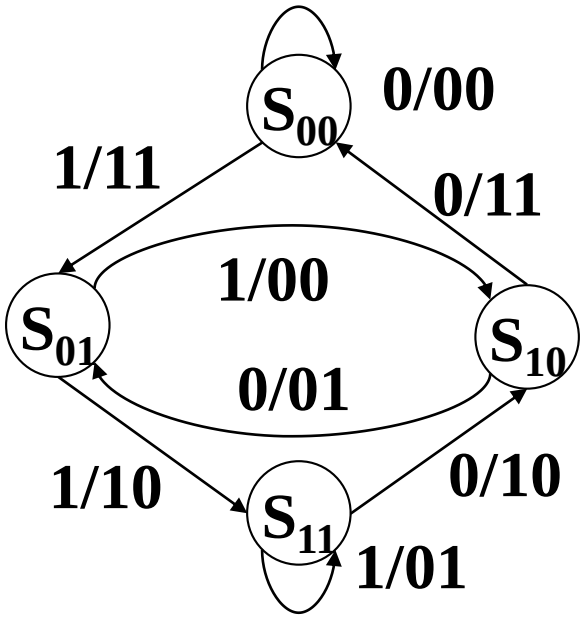
- 0=(0,0,...,0)と1=(1,1,...,1)，(長さはn)の2つの符号語だけから成る符号を(n倍)**繰り返し符号**という.
- [例]符号長n=5の繰り返し符号をCとする.
  - Cの最小距離は5であるので，2個までの誤りを訂正できる．受信系列$y=(y_1,y_2,...,y_5)$の各記号の多数決をとれば誤りが2以下なら送信された符号語が0か1かを推定できる.
  - 符号語$x=(x_1,x_2,x_3,x_4,x_5)$とすれば，$x_1=x_2=\cdots=x_5$なので，
  - $x_1+x_2=0$, $x_1+x_4=0$, $x_1+x_3=0$, $x_1+x_5=0$,(パリティ検査方程式；x_1が情報点，その他が検査点として)が成り立つ.
  - 受信語$y=(y_1,..,y_5)$に対して，$s_1=y_1+y_2$, $s_2=y_1+y_3$, $s_3=y_1+y_4$, $s_4=y_1+y_5$,とおけば，これら$S=(s_1,s_2,s_3,s_4)$は誤りパターン$e=(e_1,e_2,e_3,e_4,e_5)$の関数となる．すなわち，
  - $s_1=e_1+e_2$, $s_2=e_1+e_3$, $s_3=e_1+e_4$, $s_4=e_1+e_5$
  - Sを**パリティ検査和**という．この検査和は，e_1がs_1からs_4全てに含まれるが，他のe_2,e_3,e_4,e_5はs_1からs_4のどれかに1つだけ含まれる．⇔これを「s_1, s_2, s_3, s_4,はe_1**に関して直交する**」，という.

13.10 最尤復号:ビタビアルゴリズム(1)

- 最尤復号
  - ブロック符号では，2元対称通信路(BSC)を仮定した場合，受信系列とハミング距離が最も近い系列を送信系列と推定するものが最尤復号(最小距離復号).
- 最小自由距離
  - ブロック符号の最小距離に相当するものが，畳込み符号の「最小自由距離」
  - 畳込み符号の最小自由距離の定義
    - 実際に使う畳込み符号は，符号系列が有限長になるよう終結させる．終結させるには，ある程度の長さの0ビット系列を最後に入れる．すなわち，mブロックのk_0×m個の情報ビットを0とする.
    - これは符号器の遅延素子の状態を全部0にするために必要な長さ.
    - このようにして終結させた長さNの系列を考えると，符号長がNよりある値(=d)より大きいと，畳込み符号の最小ハミング距離はNによっては変わらないことがいえる．この最小距離dを最小自由距離という.

13.10 最尤復号:ビタビアルゴリズム (2)

- 畳込み符号の状態図
  - 畳込み符号は，符号器の遅延素子に入るビットの値により，出力される符号が影響される．すなわち，符号器の状態が存在する．
  - 遅延素子の数をdとすると状態数は2^dとなる．
  - 状態の推移により出力の状況を示すものが状態図．
  - 下の図で表される畳込み符号を考える:

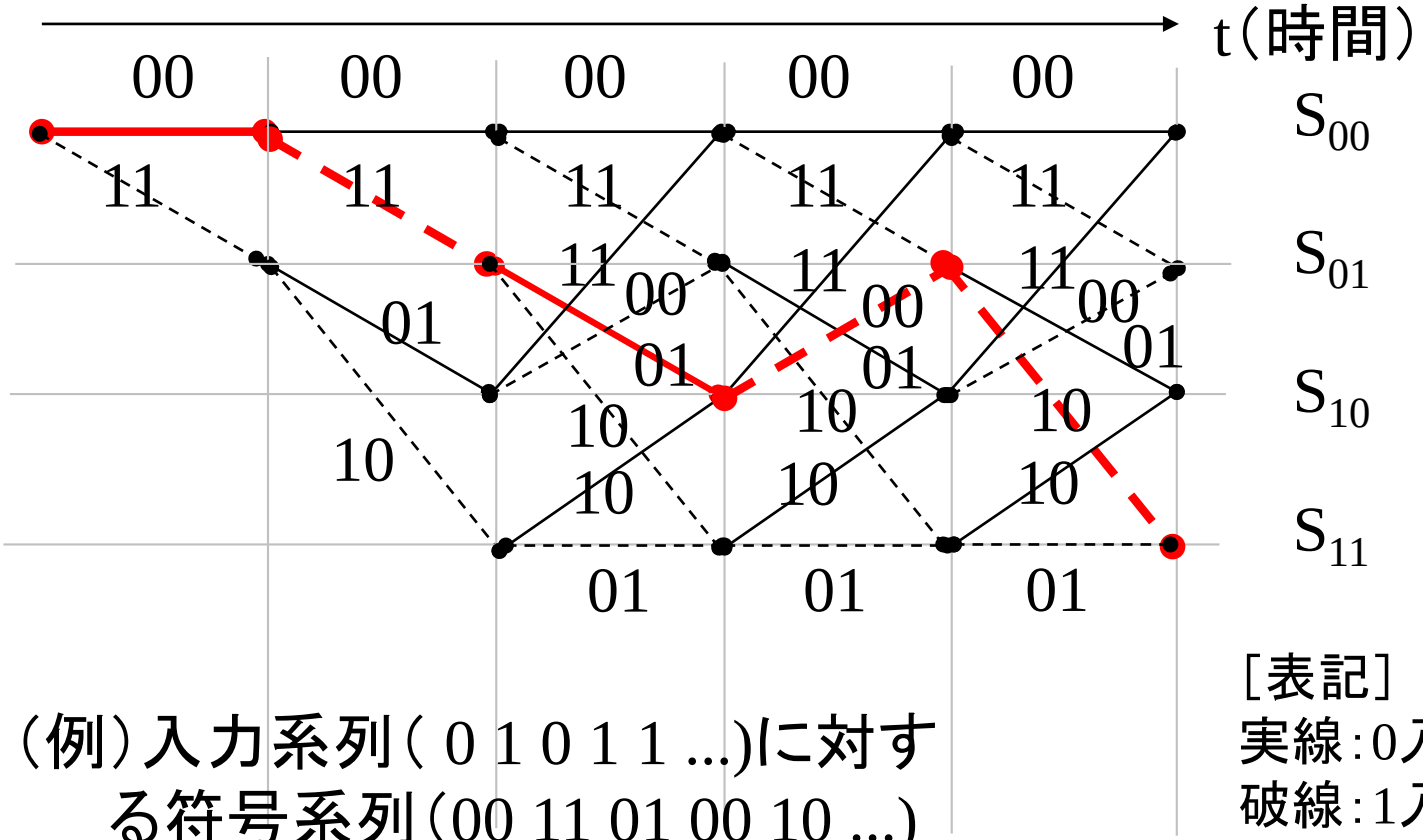


［表記法］

x/z_1z_2:
入力xが入ると，状態遷移し，
出力z_1z_2を出す

13.10 最尤復号:ビタビアルゴリズム (3)

- 畳込み符号の格子状表現(トレリス線図)
  - 状態の遷移と出力を，時間軸を横にとり表したもの.



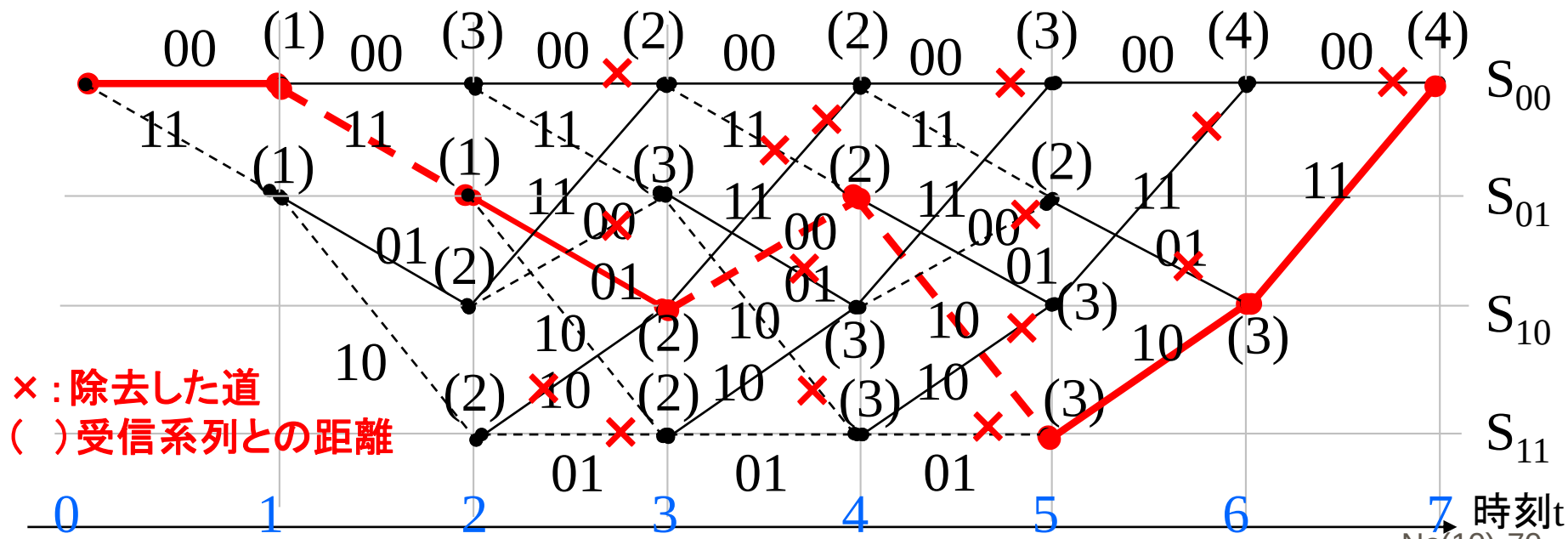
(例)入力系列(0 1 0 1 1 ...)に対する符号系列(00 11 01 00 10 ...)は太線で示すもの.

[表記]
実線:0入力
破線:1入力
線分上:出力

13.10 最尤復号:ビタビアルゴリズム(4)

- 受信系列にハミング距離が最も近い道を探索する「最尤復号法」. 可能性のない道を捨てていく方針をとる.

情報系列	0	1	0	1	1	0	0
符号系列	00	11	01	00	10	10	11
誤り系列	01	00	10	00	01	00	10
受信系列	01	11	11	00	11	10	01



13.10 最尤復号:ビタビアルゴリズム(5)

（仮定）

- 情報(01011)を送り，終結させるため0を2つ送る．→情報系列(0101100)
- これに対する符号系列は(00 11 01 00 10　10 11)．
- 誤り系列e=(01 00 10 00 01 00 10)が加わり，系列y=(01 11 11 00 11 10 01)を受信したとする．

（アルゴリズム）

- 受信系列に最も距離が近い道を選ぶ．
- 時刻3において，
  - 状態S_{00}に合流する2つの道，(00-00-00)と(11-01-11)と受信系列を比較する．ハミング距離は各々5と2であるので，前者(00-00-00)は可能性がないと判断し除去する．（前図で×）
  - 同様にして，S_{01}，S_{10},S_{11}についても合流する2つの道のうち，受信系列に近いほうを選ぶ．
- 時刻4において，

13.10 最尤復号：ビタビアルゴリズム (6)

- 状態S_{00}に合流する2つの生き残り道，(00-11-01-11)と(11-01-11-00)と受信系列を比較する．ハミング距離は各々4と2であるので，前者(00-11-01-11)を除去する．(前図で×)
- 他の状態についても同様．

- 以下，時刻7 (系列を終結させた長さN=14)まで同様の判定を行い，最後まで生き残った道を受信系列に最も近い系列として復号する．