HOKKAIDO UNIVERSITY

Title	2005年度　情報理論講義ノート
Author(s)	井上, 純一
Issue Date	2005-11-18T09:19:52Z
Doc URL	http://hdl.handle.net/2115/772
Rights(URL)	http://creativecommons.org/licenses/by-nc-sa/2.1/jp/
Type	learningobject
Note(URL)	http://www005.upp.so-net.ne.jp/j_inoue/index.html; http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/
Additional Information	There are other files related to this item in HUSCAP. Check the above URL.
File Information	InfoTheory05_10.pdf (第10回講義ノート)

Instructions for use

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

情報理論 配布資料 #10

担当：井上 純一 (情報科学研究科棟 8-13)
URL：http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/

平成 17 年 6 月 27 日

目 次

演習問題 9 の解答例

パリティ検査行列として $H = (\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_n)$, 符号語ベクトルを $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ とすれば, パリティ検査方程式：$H\boldsymbol{x}^{'} = 0$ は

$$x_1\boldsymbol{h}_1 + x_2\boldsymbol{h}_2 + \cdots + x_n\boldsymbol{h}_n \quad = \quad 0 \tag{292}$$

と書くことができる. そこで, この符号語ベクトルの成分のうち, 値がゼロでないものを $a_1, a_2, \cdots, a_t$ とすれば, ベクトル $\boldsymbol{x}$ のハミング重みは $w(\boldsymbol{x}) = t$ となるが, $a_1, a_2, \cdots, a_t$ のそれぞれに該当するパリティ検査行列の t 個の列ベクトル $\boldsymbol{h}_{a_1}, \boldsymbol{h}_{a_2}, \cdots, \boldsymbol{h}_{a_t}$ が線形独立であるならば

$$a_1\boldsymbol{h}_{a_1} + a_2\boldsymbol{h}_{a_2} + \cdots + a_t\boldsymbol{h}_{a_t} \quad \neq \quad 0 \tag{293}$$

となるのでパリティ検査方程式を満たさない. 従って, ハミング重みが t であるような符号は存在しない. そこで, $t+1$ 個のベクトルが線形従属であるとし, $a_1, a_2, \cdots, a_t$ に対応する t 個の列ベクトル $\boldsymbol{h}_{a_1}, \boldsymbol{h}_{a_2}, \cdots, \boldsymbol{h}_{a_t}$ が線形独立であるならばベクトル $\boldsymbol{h}_{a_{t+1}}$ は

$$\begin{aligned} \boldsymbol{h}_{a_{t+1}} &= a_1\boldsymbol{h}_{a_1} + a_2\boldsymbol{h}_{a_2} + \cdots + a_t\boldsymbol{h}_{a_t} \\ &= \boldsymbol{h}_{a_1} + \boldsymbol{h}_{a_2} + \cdots + \boldsymbol{h}_{a_t} \end{aligned} \tag{294}$$

となるが, この式を変形し, 2 進数の演算では $\boldsymbol{h}_{a_{t+1}} = -\boldsymbol{h}_{a_{t+1}}$ であることに注意すれば

$$\boldsymbol{h}_{a_1} + \boldsymbol{h}_{a_2} + \cdots + \boldsymbol{h}_{a_t} + \boldsymbol{h}_{a_{t+1}} \quad = \quad 0 \tag{295}$$

であり, これはパリティ検査方程式が満たされていることを意味する. また, このときのハミング重みは $w(\boldsymbol{x}) = t+1$ である. 以上より, パリティ検査行列のどの t 個の列ベクトルも線形独立で, $t+1$ 個の列ベクトルが線形従属であるならば, 符号の最小重み (最小距離) は $t+1$ であることが言える.

7.6 巡回符号

ここからは巡回符号と呼ばれるクラスの線形符号の構成法と符号・復号化の手続きについて詳しく見ていくことにする.

7.6.1 既約多項式

$x = \{0,1\}$ に関する多項式 :

$$f(x) \quad = \quad x^3 + x + 1 \tag{296}$$

を考える. $f(1) = f(0) = 1 \neq 0$ であるから, $f(x) = 0$ は $x = 0, 1$ を解として持たない. これは, $f(x)$ が $\{0,1\}$ 上で因数分解できないことを意味する. すなわち, α, β を $\alpha + \beta = 3$ を満たす正の整数としたとき,

$$f(x) \quad = \quad x^\alpha (1-x)^\beta \tag{297}$$

のように $f(x)$ を書き直すことはできない. このとき, $f(x)$ は $\{0,1\}$ 上での**既約多項式**であるという.

ところで, $f(x) = 0$ の解を α とし, $f(\alpha) = \alpha^3 + \alpha + 1 = 0$ を用いて, $\alpha^0, \alpha^1, \alpha^2, \cdots$ を書き直してみると

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha^3 = -(\alpha+1) = \alpha + 1 \\
\alpha^4 &= \alpha^3 \cdot \alpha = (\alpha+1)\cdot\alpha = \alpha^2 + \alpha \\
\alpha^5 &= \alpha^4 \cdot \alpha = (\alpha^2+\alpha)\cdot\alpha = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 \\
\alpha^6 &= \alpha^5 \cdot \alpha = (\alpha^2+\alpha+1)\cdot\alpha = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1 \\
\alpha^7 &= \alpha^6 \cdot \alpha = \alpha^3 + \alpha = \alpha + \alpha + 1 = 1 = \alpha^0
\end{aligned}$$

のようになる. ここで, 上記の計算では全て $\{0,1\}$ 上での演算則にならっているので, $\alpha+\alpha = 2\alpha = 0, -\alpha = \alpha$ 等を用いていることに注意されたい. ここで, $\{0,1\}$ 上での**原始既約多項式**を次のように定義しょう.

原始既約多項式 :
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ が $\{0,1\}$ 上で既約, かつ, $f(x) = 0$ の解を α とすると, $\alpha^0, \alpha, \cdots$ の中に α の $n-1$ 次以下の全ての多項式が含まれるとき, $f(x)$ を原始既約多項式と呼ぶ.

従って, ここで調べていた $f(x) = x^3 + x + 1$ は $f(x) = 0$ の解を α としたとき, $\alpha^0, \alpha, \cdots, \alpha^6$ の中に α^2 以下の全ての多項式 : $1, \alpha, \alpha^2, \alpha+1, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1$ が含まれるので, 原始既約多項式であることになる.

7.6.2　巡回ハミング符号

原始既約多項式 $f(x) = x^3 + x + 1$ に対し, $f(x) = 0$ の解 α のべき乗を次のように書き直してみよう.

$$\begin{aligned}
\alpha^0 &= 1 + 0 \cdot \alpha + 0 \cdot \alpha^2 \\
\alpha^1 &= 0 + 1 \cdot \alpha + 0 \cdot \alpha^2 \\
\alpha^2 &= 0 + 0 \cdot \alpha + 1 \cdot \alpha^2 \\
\alpha^3 &= 1 + 1 \cdot \alpha + 0 \cdot \alpha^2 \\
\alpha^4 &= 0 + 1 \cdot \alpha + 1 \cdot \alpha^2 \\
\alpha^5 &= 1 + 1 \cdot \alpha + 1 \cdot \alpha^2 \\
\alpha^6 &= 1 + 0 \cdot \alpha + 1 \cdot \alpha^2
\end{aligned}$$

のように書ける. この右辺に出てくる多項式の係数は $0, 1$ からなるので, この係数をベクトルとして並べたものと, $\alpha^0, \alpha^1, \cdots, \alpha^6$ の対応関係を明示的に書き出してみると

$$\begin{aligned}
\alpha^0 &\rightarrow (100) \\
\alpha^1 &\rightarrow (010) \\
\alpha^2 &\rightarrow (001) \\
\alpha^3 &\rightarrow (110) \\
\alpha^4 &\rightarrow (011) \\
\alpha^5 &\rightarrow (111) \\
\alpha^6 &\rightarrow (101)
\end{aligned}$$

となる. この係数ベクトルを各列にとり, 7×3 の行列を作り, それをパリティ検査行列とすることができる. つまり

$$H(\alpha^0 \alpha^1 \cdots \alpha^6) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \tag{298}$$

とする. すると, このパリティ検査行列で与えられる線形符号は**符号長を** n**, 符号語数を** $M = 2^m$**, 最小距離を** d **とする符号を** (n, m, d) **符号と名づける**ことにすれば, $(7, 4, 3)$ 線形符号ということになる.

7.6.3　ハミングの不等式とハミング符号

さて, パリティ検査行列が (298) 式で与えられる $(7, 4, 3)$ 線形符号の最小距離は 3 であることから, この符号が何ビットの誤りまでを訂正できるのかがわかる. t ビットまでの誤りが訂正可能であるためには, 最小ハミング重み (距離) が $2t + 1$ 以上でなければならないので, 今の場合

$$3 \geq 2t + 1 \tag{299}$$

つまり, $t \leq 1$ であり, t は整数であることを考えると, 1 ビットの誤りまでが訂正可能である. このとき, 既に学んだ 1 ビット誤りに対するハミングの不等式 :

$$M \leq \frac{2^n}{n+1} \tag{300}$$

の中に, $n=7, M=2^4$ を代入してみると

$$2^4 \quad \leq \quad \frac{2^7}{7+1} = \frac{2^7}{2^3} = 2^4 \tag{301}$$

となり, ハミングの不等式 (限界式) を等式でぎりぎり満たすことがわかる. この場合, 各符号語を中心とする半径が 1 ビットのハミング球が空間全体 (今の場合, 2^7 個の点からなる) を隙間無く覆っていることになり, このような線形符号を特に**ハミング符号**と呼んでいる.

さて, この行列 (298) に対して符号語ベクトル $\boldsymbol{x}=(x_0,x_1,x_2,x_3,x_4,x_5,x_6)$ を定義し, これが線形符号となるための条件 (**パリティ検査方程式**) : $H\boldsymbol{x}^{'}=0$ を書き出してみると, 直ちに

$$\begin{aligned} x_0+x_3+x_5+x_6 &= 0 \\ x_1+x_3+x_4+x_5 &= 0 \\ x_2+x_4+x_5+x_6 &= 0 \end{aligned}$$

つまり

$$\begin{aligned} x_0 &= x_3+x_5+x_6 \\ x_1 &= x_3+x_4+x_5 \\ x_2 &= x_4+x_5+x_6 \end{aligned}$$

が得られるので, x_3,x_4,x_5,x_6 (情報ビット) を決めれば, x_0,x_1,x_2 (パリティ検査ビット) が定まる. 実際に, x_3,x_4,x_5,x_6 の可能な組み合わせ : $(0000000),(0000001),\cdots,(1111111)$ に対応する $2^4=16$ 個の符号語を書き下してみると

$$\begin{aligned} C \quad = \quad & \{(0000000),(1010001),(1110010),(0100011) \\ , \quad & (0110100),(1100101),(1000110),(0010111) \\ , \quad & (1101000),(0111001),(0011010),(1001011) \\ , \quad & (1011100),(0001101),(0101110),(1111111)\} \end{aligned} \tag{302}$$

が得られる.

7.6.4　なぜ「巡回」符号か ?

このような手続きで求めることのできるハミング符号が「巡回符号」と呼ばれる理由を考えてみよう. $\boldsymbol{x}=(x_0,x_1,\cdots,x_6)$ が条件式 : $H\boldsymbol{x}^{'}=0$ を満たすとすれば一般に $H=(\alpha^0,\alpha,\alpha^2,\cdots,\alpha^6)$ として

$$(\alpha^0,\alpha,\alpha^2,\cdots,\alpha^6)\begin{pmatrix} x_0 \\ x_1 \\ \cdots \\ \cdots \\ x_6 \end{pmatrix} \quad = \quad 0 \tag{303}$$

すなわち

$$0 \quad = \quad x_0\alpha^0+x_1\alpha+\cdots+x_6\alpha^6 \tag{304}$$

であるが, この両辺から α をかけると

$$0 \quad = \quad x_0\alpha^1+x_1\alpha^2+\cdots+x_6\alpha^7 \tag{305}$$

が得られ, $\alpha^7 = \alpha^0$ であったことを思い出せば

$$0 \quad = \quad x_6\alpha^0 + x_0\alpha + x_1\alpha^2 + \cdots + x_5\alpha^6 \tag{306}$$

となるので, $\boldsymbol{x} = (x_6, x_0, x_1, \cdots, x_5)$ も $H\boldsymbol{x}^{'} = 0$ の解であることになる. 従って, この手の手続きを繰り返すことにより, $\boldsymbol{x}$ の巡回ベクトル：$(x_5, x_6, x_0, x_1, \cdots, x_4), (x_4, x_5, x_6, x_0, x_1, \cdots, x_3), \cdots$ は $H\boldsymbol{x}^{'} = 0$ を満たすので, パリティ検査行列 H のハミング符号となっていることがわかる.

7.6.5　巡回符号の多項式表現

符号語 $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n-1}) \in C$ に対し, 多項式：$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ を対応させ, $f(x)$ を符号語と呼ぶことにしょう.

このとき,

$$\begin{aligned} xf(x) &= a_0x + a_1x^2 + \cdots + a_{n-1}x^n \\ &= a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}(x_n - 1) + a_{n-1} \\ &\equiv a_{n-1} + a_0x + \cdots + a_{n-1}x^{n-2} \pmod{(x^n - 1)} \end{aligned} \tag{307}$$

すなわち

$$f(x) \in C \quad \Rightarrow \quad xf(x) \in C \pmod{(x^n - 1)} \tag{308}$$

となり, このとき, 線形符号 C は巡回符号になる.

また, (308) 式より

$$f(x) \in C \quad \Rightarrow \quad xf(x), x^2f(x), \cdots \in C \pmod{(x^n - 1)} \tag{309}$$

であることもわかる. さらに, 線形符号の性質から

$$f_1(x), f_2(x) \in C \quad \Rightarrow \quad f_1(x) + f_2(x) \in C \tag{310}$$

である.

7.6.6　生成多項式

生成多項式を次数の最も小さい符号語 $g(x)$ とする. このとき, 線形符号 C は生成多項式を用いて次のように書ける.

$$C \quad = \quad \{b(x)g(x) \,|\, b(x) \text{ は } \{0,1\} \text{ 上の } k-1 \text{ 次以下の多項式 } \} \tag{311}$$

定理 5・4：
$\{0,1\}$ 上の長さ n の巡回符号の生成多項式を $g(x)$ とすると, $g(x)$ は $x^n - 1$ を割り切る.

(例)
$n = 7$ のとき, $\{0,1\}$ 上で

$$x^7 - 1 \quad = \quad (x^3 + x^2 + 1)(x^3 + x^2 + 1)(x + 1) \tag{312}$$

となる. ここでは $g(x) = x^3 + x^2 + 1$ が生成多項式である.

7.6.7　シフトレジスタでの符号器

生成多項式 $g(x) = x^3 + x + 1$ として,　$b(x) = x^2 + x$ の符号器を作ると

$$\begin{aligned} b(x)g(x) &= (x^3 + x + 1)(x^2 + x) \\ &= x^5 + x^3 + x^2 + x^4 + x^2 + x \\ &= x^5 + x^4 + x^3 + x \\ &= 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0 \end{aligned} \tag{313}$$

となる. 図 27 より, 初期設定を $S_0 = S_1 = S_2 = 0$ に選びと

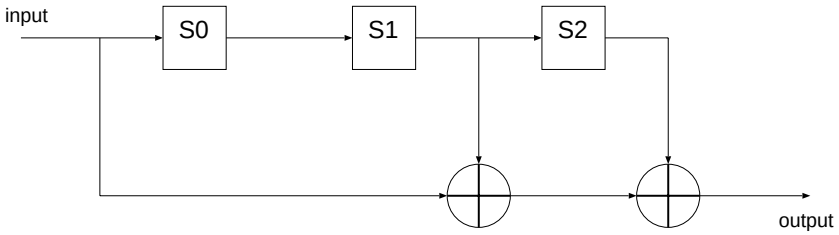

図 27: $g(x) = x^3 + x + 1$ の掛け算回路.

$$\begin{aligned} x_0 &= a_0 + S_1 + S_2 = 1 \ (S_0 = a_0 = 1, S_1 = S_2 = 0) \\ x_1 &= a_1 + S_1 + S_2 = 1 \ (S_0 = a_1 = 1, S_1 = a_0 = 1, S_2 = 0) \\ x_2 &= a_2 + S_1 + S_2 = 1 \ (S_0 = a_2 = 0, S_1 = a_1 = 1, S_2 = a_0 = 1) \\ x_3 &= 0 + S_1 + S_2 = 1 + 1 = 0 \ (S_0 = 0, S_1 = a_2 = 0, S_2 = a_1 = 1) \\ x_4 &= 0 + S_1 + S_2 = 1 \ (S_0 = 0, S_1 = S_0 = 0, S_2 = a_2 = 0) \\ x_5 &= 0 + S_1 + S_2 = 0 \ (S_0 = 0, S_1 = S_0 = 0, S_2 = S_0 = 0) \end{aligned}$$

となるので, 最終的なシフトレジスタ回路の出力は (111010) となる.

7.6.8　2-誤り訂正符号と復号法

多項式を

$$f(x) = a_0 + a_1 x + \cdots + a_n x_n \tag{314}$$

とすると, この自乗は

$$\{f(x)\}^2 = a_0^2 + a_1^2 x^2 + \cdots + a_n^2 x_n^2 = f(x^2) \tag{315}$$

となる. ここで, 自乗する際に現れるクロス・タームは $a_0 + a_0$ のように同じものが必ず 2 回ずつ出てくるので, 2 進数の演算の下では $a_0 + a_0 = 0$ のようになることに注意されたい. 同様に, $\{f(x^2)\}^2 = f(x^4), \{f(x^4)\}^2 = f(x^6), \cdots$ が得られるので, α が $f(x) = 0$ の解であるならば $\alpha^2, \alpha^4, \alpha^8, \cdots$ も $f(x)$ の解であることがわかる.

$\{0,1\}$ 上で $x^{15}-1$ は

$$\begin{aligned} m_1(x) &= x+1 \\ m_2(x) &= x^2+x+1 \\ m_3(x) &= x^4+x^3+x^2+x+1 \\ m_4(x) &= x^4+x+1 \\ m_5(x) &= x^4+x^3+1 \end{aligned}$$

の積で因数分解できる.

今, $g(x)=m_3(x)m_4(x)=1+x^4+x^6+x^7+x^8$ を生成多項式とする長さ 15 の巡回符号 C を考える. そこで, $c(x)=b(x)g(x)$ なる符号語を送信したとき, 3, 8 ビット目に誤りがあるベクトル $e(x)=x^3+x^8$ が加わり,

$$\begin{aligned} \overline{c}(x) &= c(x)+e(x) \\ &= b(x)g(x)+e(x) \\ &\equiv x^3+x^8 \pmod{g(x)} \\ &\equiv 1+x^3+x^4+x^6+x^7 \pmod{g(x)} \end{aligned} \tag{316}$$

であったとすると

$$s(x) = 1+x^3+x^4+x^6+x^7 \tag{317}$$

を**シンドローム多項式**と呼ぶ.

従って, 受信ベクトルから, 送信ベクトルを復号するためには, 受信ベクトルに対応する多項式を生成多項式 $g(x)$ で割ればよい.

以上学んだことを確認するために次の例題を見ておこう.

例題 10

$\{0,1\}$ 上の巡回符号に関して, 以下の小問 (1)-(5) に答えよ.

(1) $\{0,1\}$ 上の多項式：$f(x)=x^4+x^3+x^2+x+1$ について, 方程式 $f(x)=0$ の根のべき乗 α^i とその多項式表現を教科書 p.80 表 5.3 にならって求めよ.
(2) (1) の $f(x)$ を生成多項式とする巡回符号のパリティ検査行列を求め, 全ての符号語を列記せよ.
(3) (2) の巡回符号の符号語を作るシフトレジスタによる回路を作成せよ.
(4) $c(x)=(x^2+x)g(x)$ なる符号語を送信したとき, 2 ビット目に誤りを発生させるベクトル $e(x)$ が加わり

$$\overline{c}(x) = c(x)+e(x)$$

を受信したとしょう. このとき, シンドローム多項式 $s(x)$ を求めよ.
(5) (4) でのシンドローム多項式を具体的に求めるためのシフトレジスタによる回路を作成せよ.

(解答例)

(1) $f(x)=0$ の根の冪乗の多項式表現を書き下していってみると

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha^3 \\
\alpha^4 &= \alpha^3+\alpha^2+\alpha+1 \\
\alpha^5 &= \alpha(\alpha^3+\alpha^2+\alpha+1) \\
&= \alpha^4+\alpha^3+\alpha^2+\alpha \\
&- (\alpha^3+\alpha^2+\alpha+1)+\alpha^3+\alpha^2+\alpha = 2\alpha^3+2\alpha^2+2\alpha+1 = 1
\end{aligned}$$

となるから周期 5 であり, 教科書 p.80 表 5.3 にならって表にすると

i	α^3	α^2	α	1
0	0	0	0	1
1	0	0	1	0
2	0	1	0	0
3	1	0	0	0
4	1	1	1	1

となる.

(2) 前問 (1) の結果から, パリティ検査行列 $\boldsymbol{H}$ は

$$\boldsymbol{H} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \tag{318}$$

で与えられるから, $\boldsymbol{x} \equiv (x_1, x_2, x_3, x_4, x_5)$ とおけば, ベクトル $\boldsymbol{x}$ は次のパリティ検査方程式を満たす.

$$\boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{0} \tag{319}$$

つまり

$$\begin{aligned}
x_1 &= x_5 \\
x_2 &= x_5 \\
x_3 &= x_5 \\
x_4 &= x_5
\end{aligned}$$

が満たされるべきである. 従って, 求めるべき符号語は全部で $2^1=2$ つであり, (11111), 及び, (00000) である.

(3) まず, 求めるシフトレジスタ回路を図 28 に示す. このシフトレジスタ回路の動作を実際に確認してみよう.
まずは試しに $b(x)=x^3+x^2$ と選んで $b(x)f(x)$ を $\{0,1\}$ 上において予め手で計算しておくと

$$b(x)f(x) = (x^3+x^2)(x^4+x^3+x^2+x+1) = x^7+x^2 \tag{320}$$

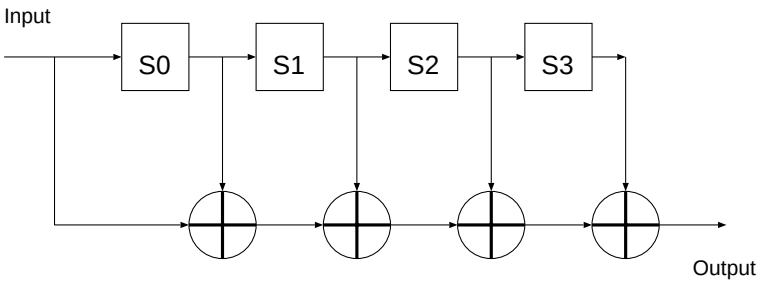

図 28: 任意の符号語 $b(x)f(x) = b(x)(x^4 + x^3 + x^2 + x + 1)$ を作るシフトレジスタ回路.

である．この結果と図 28 に描いたシフトレジスタ回路の出力結果を比較する．$b(x)f(x) = X_0x^7 + X_1x^6 + X_2x^5 + X_3x^4 + X_4x^3 + X_5x^2 + X_6x + X_7$ とおけば, 図 28 に描かれたシフトレジスタ回路の出力 $X_0, X_1, \cdots$ としては

$$(X_0X_1X_2X_3X_4X_5X_6X_7) \quad = \quad (10000100) \tag{321}$$

となればよい. $b(x) = a_0x^3 + a_1x^2 + a_2$, $(a_0a_1a_2) = (110)$ を逐次, このシフトレジスタ回路に入力してみると (各レジスタの初期値は $S_0 = S_1 = S_2 = S_3 = 0$ とする．また, 以下の括弧内はその出力時点でのレジスタの内容を表す).

- $a_0 = 1$

$$\begin{aligned} X_0 &= a_0 + S_0 + S_1 + S_2 + S_3 \\ &= 1 + 0 + 0 + 0 + 0 = 1, \quad (S_0 = 1, S_1 = S_2 = S_3 = 0) \end{aligned}$$

- $a_1 = 1$

$$\begin{aligned} X_1 &= a_1 + S_0 + S_1 + S_2 + S_3 \\ &= 1 + 1 + 0 + 0 + 0 = 0, \quad (S_0 = 1, S_1 = 1, S_2 = S_3 = 0) \end{aligned}$$

- $a_2 = 0$

$$\begin{aligned} X_2 &= a_2 + S_0 + S_1 + S_2 + S_3 \\ &= 0 + 1 + 1 + 0 + 0 = 0, \quad (S_0 = 0, S_1 = 1, S_2 = 1, S_3 = 0) \end{aligned}$$

- 入力ゼロ (i)

$$\begin{aligned} X_3 &= 0 + S_0 + S_1 + S_2 + S_3 \\ &= 0 + 0 + 1 + 1 + 0 = 0, \quad (S_0 = 0, S_1 = 0, S_2 = 1, S_3 = 1) \end{aligned}$$

- 入力ゼロ (ii)

$$\begin{aligned} X_4 &= 0 + S_0 + S_1 + S_2 + S_3 \\ &= 0 + 0 + 0 + 1 + 1 = 0, \quad (S_0 = S_1 = S_2 = 0, S_3 = 1) \end{aligned}$$

- 入力ゼロ (iii)

$$\begin{aligned} X_5 &= 0 + S_0 + S_1 + S_2 + S_3 \\ &= 0 + 0 + 0 + 0 + 1 = 1, \quad (S_0 = S_1 = S_2 = S_3 = 0) \end{aligned}$$

- 入力ゼロ (iv)

$$X_6 = 0, \quad (S_0 = S_1 = S_2 = S_3 = 0)$$

- 入力ゼロ (v)

$$X_7 = 0, \quad (S_0 = S_1 = S_2 = S_3 = 0)$$

となる. 従って, 結局, このシフトレジスタ回路の出力は

$$(X_0X_1X_2X_3X_4X_5X_6X_7) = (10000100) \tag{322}$$

となり, これは先に確認した「手計算」の結果と一致する. ちなみに, 入力, 及び, 各シフトレジスタから $\{0,1\}$ 上の加算器への入力線がこの図 28 では 5 本あるが, これはこの問題の生成多項式が

$$f(x) = 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1 \tag{323}$$

であり, 4 次以下のすべての x 冪がふくまれているので, 計 5 本の入力線が存在し, 左から, $x^4, x^3, \cdots$ に対応している. 教科書 p. 83 の図 5.2 は生成多項式

$$g(x) = \quad 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1 \tag{324}$$

に対応するシフトレジスタ回路であるが, x^2 の係数がゼロ (x^2 が含まれない) なので, s_0, s_1 間の信号の加算器への入力線は存在しない (教科書にはこの点も含めたシフトレジスタによる掛け算回路の構成法が書かれていないので各自がここで確認しておくこと).

(4) まずは 2 ビット目に誤りを生じさせる多項式 $e(x)$ は $e(x) = x^2$ であるから, 受信多項式 $\overline{c}(x)$ は

$$\begin{aligned} \overline{c}(x) &= (x^2 + x)(x^4 + x^3 + x^2 + x + 1) + x^2 \\ &= x^6 + x^2 + x \\ &\equiv x^2 \pmod{g(x)} \end{aligned} \tag{325}$$

従って, シンドローム多項式は $s(x) = x^2$ である.

(5) 受信多項式 $\overline{c}(x)$ を生成多項式 $g(x) = x^4 + x^3 + x^2 + x + 1$ で割るためのシフトレジスタ回路は図 29 のようになる. このシフトレジスタ回路の動作を確認するために, $\overline{c}(x) = x^6 + x^2 + x$ に対して, $a_0x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x + a_6$, とおき, この回路に逐次 $(a_0a_1a_2a_3a_4a_5a_6) = (1000110)$ を代入していく. シフトレジスタの内容は初期値として $S_0 = S_1 = S_2 = S_3 = 0$ とする.

- $(a_0 = 1)$ $S_0 = 1, S_1 = S_2 = S_3 = 0, X_0 = 0$
- $(a_1 = 0)$ $S_0 = 0, S_1 = 1, S_2 = 0, S_3 = 0, X_1 = 0$
- $(a_2 = 0)$ $S_0 = 0, S_1 = 0, S_2 = 1, S_3 = 0, X_2 = 0$

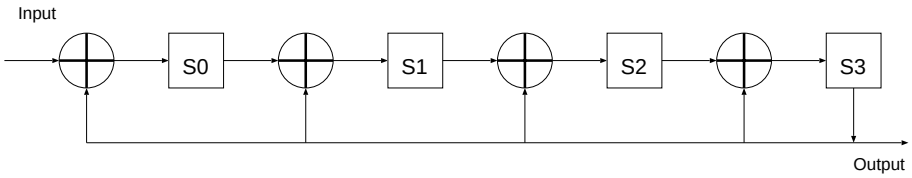

図 29: 受信多項式 $\overline{c}(x)$ を生成多項式 $g(x) = f(x) = x^4 + x^3 + x^2 + x + 1$ で割るシフトレジスタ回路.

- $(a_3 = 0)$ $S_0 = 0, S_1 = 0, S_2 = 0, S_3 = 1, X_3 = 1$
- $(a_4 = 1)$ $S_0 = 0, S_1 = 1, S_2 = 1, S_3 = 1, X_4 = 1$
- $(a_5 = 1)$ $S_0 = 0, S_1 = 1, S_2 = 0, S_3 = 0, X_5 = 0$

となる. この時点での出力の列 : $(X_0X_1X_2X_3X_4X_5) = (000110)$ が商 $X_0x^5 + X_1x^4 + X_2x^3 + X_3x^2 + X_4x + X_5$ を表しているので, この場合の商は $x^2 + x$ である. また, シフトレジスタの内容 $(S_0S_1S_2S_3) = (0100)$ がシンドローム多項式 $S_0x^3 + S_1x^2 + S_2x + S_3$ を表しているので, この場合には x^2 となり, いずれも手計算の結果と合っている.

演習問題 10

$g(x) = x^3 + x^2 + 1$ を生成多項式とする $(7, 4, 3)$ 線形符号が巡回符号になることを示せ.