通信路符号化法 (2)

符号のブール多項式表現

- **ブール体** GF(2)

x	y	$x+y$	$x \cdot y$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

- **符号長nの符号語**

$$v = (v_{n-1}, \cdots, v_1, v_0) \qquad v_i \in \{0,1\}$$

に対して，ブール体GF(2)**の要素**$\{0, 1\}$**を係数とするブール多項式**

$$V(x) = v_{n-1}x^{n-1} + \cdots + v_1 x^1 + v_0$$

をv**の多項式表現と呼ぶ．**$V(x)$**は符号多項式と呼ばれる．**

符号のブール多項式表現

ブール多項式の加減乗除

- 例えば，

$$G(x) = x^4 + x^2 + x + 1,\ H(x) = x^2 + 1$$

とすると，

$$G(x) + H(x) = G(x) - H(x) = x^4 + x$$

$$G(x) \times H(x) = x^6 + x^4 + x^3 + x^2 + x^4 + x^2 + x + 1 = x^6 + x^3 + x + 1$$

$$G(x) = x^2 H(x) + x + 1$$

$$G(x) = x + 1 \mod H(x)$$

また，

$$(0) - 1 = 1$$

符号のブール多項式表現

組み立て算

$$
\begin{array}{rl}
 & x^2 \\
x^2 \quad +1 & \overline{)\,x^4 \quad +x^2+x+1} \\
 & \underline{x^4 \quad +x^2} \\
 & \qquad\qquad x+1
\end{array}
$$

あるいは，係数の部分だけを取り出して，

$$
\begin{array}{rl}
 & 1\ 0\ 0 \\
1\ 0\ 1 & \overline{)\,1\ 0\ 1\ 1\ 1} \\
 & \underline{1\ 0\ 1} \\
 & \qquad 1\ 1
\end{array}
$$

符号のブール多項式表現

- ブール多項式 $G(x)$ が $H(x)$ を割り切るとき，$G(x) \mid H(x)$ と表記する．
- $G(x)$ の周期：$G(x) \mid (x^n - 1)$ となる最少の正整数 n

例：

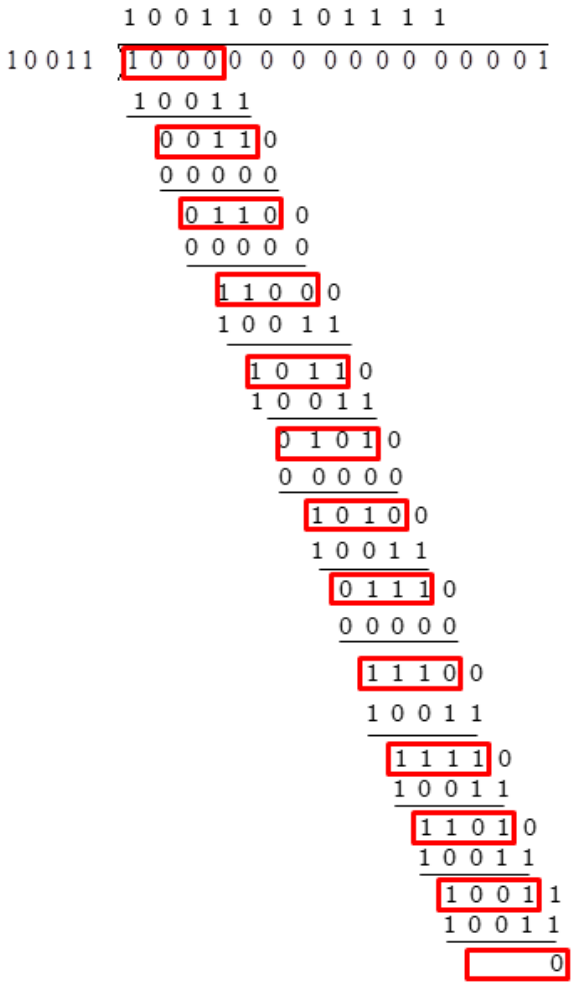
$$
\begin{array}{r}
1\ 1\ 0\ 1 \\
\hline
1\ 1\ 1\ 0\ 1 \;\big)\; 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1 \\
\quad 1\ 1\ 1\ 0\ 1 \\
\hline
\quad\ 1\ 1\ 0\ 1\ 0 \\
\quad\ 1\ 1\ 1\ 0\ 1 \\
\hline
\quad\quad\ 1\ 1\ 1\ 0\ 1 \\
\quad\quad\ 1\ 1\ 1\ 0\ 1 \\
\hline
\quad\quad\quad\ 0
\end{array}
$$

$(x^4 + x^3 + x^2 + 1) \mid (x^7 - 1)$ であり，7より小さな n に対して $(x^4 + x^3 + x^2 + 1) \mid (x^n - 1)$ とならないので，$x^4 + x^3 + x^2 + 1$ の周期は7である．

符号のブール多項式表現

- 0, 1を係数とするm次のブール多項式の周期は高々$2^m - 1$である.

例えば, m=4のとき …



符号のブール多項式表現

- 原始多項式：周期が $2^m - 1$ となるm次のブール多項式

次数	m次の原始多項式の例
1	$x+1$
2	x^2+x+1
3	x^3+x+1
4	x^4+x+1
5	x^5+x^2+1
6	x^6+x+1
7	x^7+x+1
8	$x^8+x^4+x^3+x^2+1$
9	x^9+x^4+1
10	$x^{10}+x^3+1$

次数	m次の原始多項式の例
11	$x^{11}+x^2+1$
12	$x^{12}+x^6+x^4+x+1$
13	$x^{13}+x^4+x^3+x+1$
14	$x^{14}+x^{10}+x^6+x+1$
15	$x^{15}+x+1$
16	$x^{16}+x^{12}+x^3+x+1$
17	$x^{17}+x^3+1$
18	$x^{18}+x^7+1$
19	$x^{19}+x^5+x^2+x+1$
20	$x^{20}+x^3+1$

符号のブール多項式表現

- GF(2)上の多項式 $G(x)$ の周期が p であるとき，$G(x)\,|\,(x^n - 1)$ であるための必要十分条件は $p\,|\,n$ となることである．

証明　$p\,|\,n$ でないとすると，$n = ap + b,\ 0 < b < p$ と書けるはずである．一方，$G(x)|(x^n - 1), G(x)\,|\,(x^p - 1)$ であるので，

$$x^n - 1 = G(x)A(x),\ x^p - 1 = G(x)B(x)$$

と書ける．また，$(x^p - 1)|(x^{ap} - 1)$ であるので，

$$x^n - 1 = x^{ap+b} - 1 = x^b x^{ap} - 1 = x^b((x^p - 1)C(x) + 1) - 1$$
$$= x^b G(x)B(x)C(x) + x^b - 1$$

と書ける．従って，$G(x)\,|\,(x^b - 1)$ でなければならないが，これは $G(x)$ の周期が p であるという仮定に矛盾する．従って，$p\,|\,n$ でなければならない．　■

符号のブール多項式表現

- GF(2)上の規約多項式：それ以上GF(2)上の非自明な多項式の積に分解できない多項式.

  例えば，x^2+1は$(x+1)(x+1)$と分解できるので，規約多項式ではないが，x^2+x+1 は規約多項式である.

- 異なる規約多項式の積の周期 p はそれぞれの規約多項式の周期の最小公倍数である.

  証明　$F_1(x)$´ L ´ $F_n(x) \mid (x^n - 1)$ であり，かつ，$F_i(x)$ が異なる規約多項式であれば，$F_i(x) \mid (x^n - 1)$でなければならない．$F_i(x)$の周期を p_i とすると $p_i \mid n$ でなければならないので，nは p_i の最小公倍数となる．■

巡回符号 — 符号化

- $G(x) \mid (x^n - 1)$ を満たすm次の生成多項式$G(x)$を用いる.

- $n-m$個の情報ビット $(x_{n-m-1}, \cdots, x_1, x_0)$ の多項式表現として

$$X(x) = x_{n-m-1}x^{n-m-1} + \cdots + x_1 x + x_0$$

が与えられたとする.

- $X(x)$ に x^m を掛けた $X(x)x^m$を $G(x)$ (m次多項式) で割ったときの剰余多項式 ($m-1$次) を

$$C(x) = c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$$

を求める.

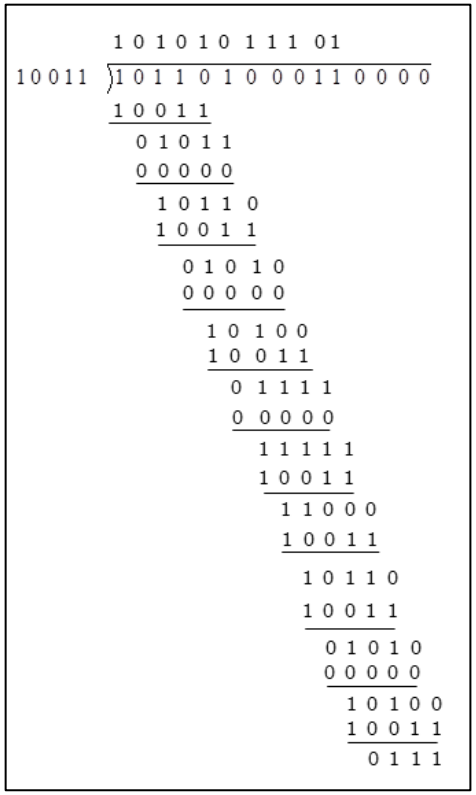
- $X(x)$に対する符号語として,

$$W(x) = X(x)x^m - C(x) = X(x)x^m + C(x)$$

を用いる.

巡回符号 — 符号化

（例） $G(x) = x^4 + x + 1$ は $G(x) \mid (x^{15} - 1)$ を満たすので，$G(x)$ を生成多項式とする，符号長15，情報ビット数11の(15, 11) 巡回符号を構成できる．



例えば，情報ビット

$$(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}) = (1,1,0,0,0,1,0,1,1,0,1)$$

が与えられたとしよう．これに対する多項式は，

$$X(x) = x^{10} + x^8 + x^7 + x^5 + x + 1$$

である．

$$X(x)x^m = x^4(x^{10} + x^8 + x^7 + x^5 + x + 1) = A(x)G(x) + C(x)$$

と置いて，$A(x)$と$C(x)$を求めると，

$$A(x) = x^{10} + x^8 + x^6 + x^4 + x^3 + x^2 + 1, \quad C(x) = x^2 + x + 1$$

であるので，求める符号多項式は，

$$W(x) = x^{14} + x^{12} + x^{11} + x^9 + x^5 + x^4 + x^2 + x + 1$$

であり，符号語は

$$(w_0, w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8, w_9, w_{10}, w_{11}, w_{12}, w_{13}, w_{14}) = (1,1,1,0,1,1,0,0,0,1,0,1,1,0,1)$$

である．

巡回符号 — 性質

- 上のようにして定めた$W(x)$は確かに符号語である.

$$
\begin{aligned}
W(x) &= X(x)x^m + C(x) \\
&= \big(A(x)G(x) + C(x)\big) + C(x) \\
&= A(x)G(x)
\end{aligned}
$$

- $W(x)$のベクトル表現

$$
w = \underbrace{(x_{m-1}, \ldots, x_1, x_0}_{\text{情報ビット}}, \underbrace{c_{n-m-1}, \ldots, c_1, c_0)}_{\text{検査ビット}}
$$

- 巡回符号は線形符号である.

$$
\begin{array}{c}
W_1(x) = A_1(x)G(x) \\
W_2(x) = A_2(x)G(x) \\
\hline
W_1(x) + W_2(x) = \big(A_1(x) + A_2(x)\big)G(x)
\end{array}
$$

巡回符号 — 性質

- $G(x)|(x^n - 1)$ であるとき，$(w_{n-1}, \cdots, w_0)$ が符号語ならば，$(w_{n-2}, \cdots, w_0, w_{n-1})$ も符号語である．

なぜならば，$W(x) = w_{n-1}x^{n-1} + \cdots + w_1 x + w_0$ が符号多項式であれば，

$$W'(x) = w_{n-2}x^{n-1} + \cdots + w_0 x + w_{n-1}$$
$$= xW(x) - w_{n-1}(x^n - 1)$$

において，$W(x) = A(x)G(x)$ も $x^n - 1$ も $G(x)$ で割り切れるので，$W'(x)$ も $G(x)$ で割り切れ，符号多項式である．

$\Rightarrow$ これが巡回符号という名前の由来である．

巡回符号 — 性質

(例) 生成多項式 $G(x) = x^4 + x + 1$ に対応する符号語を順に右にシフトしたとき

(1,1,0,0,1,0,0,0,0,0,0,0,0,0,0)	$x^4 + x + 1 = G(x)$
(0,1,1,0,0,1,0,0,0,0,0,0,0,0,0)	$x^5 + x^2 + x = xG(x)$
(0,0,1,1,0,0,1,0,0,0,0,0,0,0,0)	$x^6 + x^3 + x^2 = x^2G(x)$
(0,0,0,1,1,0,0,1,0,0,0,0,0,0,0)	$x^7 + x^4 + x^3 = x^3G(x)$
(0,0,0,0,1,1,0,0,1,0,0,0,0,0,0)	$x^8 + x^5 + x^4 = x^4G(x)$
(0,0,0,0,0,1,1,0,0,1,0,0,0,0,0)	$x^9 + x^6 + x^5 = x^5G(x)$
(0,0,0,0,0,0,1,1,0,0,1,0,0,0,0)	$x^{10} + x^7 + x^6 = x^6G(x)$
(0,0,0,0,0,0,0,1,1,0,0,1,0,0,0)	$x^{11} + x^8 + x^7 = x^7G(x)$
(0,0,0,0,0,0,0,0,1,1,0,0,1,0,0)	$x^{12} + x^9 + x^8 = x^8G(x)$
(0,0,0,0,0,0,0,0,0,1,1,0,0,1,0)	$x^{13} + x^{10} + x^9 = x^9G(x)$
(0,0,0,0,0,0,0,0,0,0,1,1,0,0,1)	$x^{14} + x^{11} + x^{10} = x^{10}G(x)$
(1,0,0,0,0,0,0,0,0,0,0,1,1,0,0)	$x^{12} + x^{11} + 1$
(0,1,0,0,0,0,0,0,0,0,0,0,1,1,0)	$x^{13} + x^{12} + x$
(0,0,1,0,0,0,0,0,0,0,0,0,0,1,1)	$x^{14} + x^{13} + x^2$
(1,0,0,1,0,0,0,0,0,0,0,0,0,0,1)	$x^{14} + x^3 + 1$
(1,1,0,0,1,0,0,0,0,0,0,0,0,0,0)	$x^4 + x + 1$

これらが符号語であることは明らか

巡回符号 — 性質

$x^{14}+x^{11}+x^{10}$ が符号語であることを利用すると

$$x^{12}+x^{11}+1 = x(x^{14}+x^{11}+x^{10})+(x^{15}+1)$$
$$= x\times x^{10}\times(x^4+x+1)+(x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)\times(x^4+x+1)$$
$$= (x\times x^{10}+x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)(x^4+x+1)$$
$$= (x^8+x^7+x^5+x^3+x^2+x+1)(x^4+x+1) \quad \Rightarrow \text{符号語}$$

$$x^{13}+x^{12}+x = x(x^{12}+x^{11}+1) \quad \Rightarrow \text{符号語}$$

$$x^{14}+x^{13}+x^2 = x(x^{13}+x^{12}+x) \quad \Rightarrow \text{符号語}$$

$$x^{14}+x^3+1$$
$$= x(x^{14}+x^{13}+x^2)+(x^{15}+1)$$
$$= x\times x^2\times(x^{12}+x^{11}+1)+(x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)\times(x^4+x+1)$$
$$= x\times x^2\times(x^8+x^7+x^5+x^3+x^2+x+1)(x^4+x+1)$$
$$+(x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)\times(x^4+x+1)$$
$$= \left(x\times x^2\times(x^8+x^7+x^5+x^3+x^2+x+1)+(x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)\right)(x^4+x+1)$$
$$= (x^{10}+x^7+x^6+x^4+x^2+x+1)(x^4+x+1) \quad \Rightarrow \text{符号語}$$

巡回符号 — 性質

- $G(x)$で生成される巡回符号 C の符号長 n は，通常$G(x)$ の周期 p 以下に選ばれる．

- なぜならば，Cの符号長が$G(x)$の周期 pよりも大きい $(n>p)$ ならば，$x^p - 1$ (＝ $x^p + 1$)は，n－1次以下の多項式であり，かつ$G(x)$で割り切れるので，$x^p - 1$ も符号多項式となり，Cは重み2の符号語をもつことになる．

- $x^p - 1$ が符号多項式であり，0も符号多項式であるので，

  …010…01　と　…000…00

  の両方が符号語であることになると，両者の間の距離は2になる．つまり最小距離は2以下となり，誤りを訂正できない．

巡回符号 — 性質

- 生成多項式の周期をpとするとき，$n \leq p$ なるnを符号長とする巡回符号の最小距離を$d_{\min}$ とすれば，$d_{\min} \geq 3$ である．

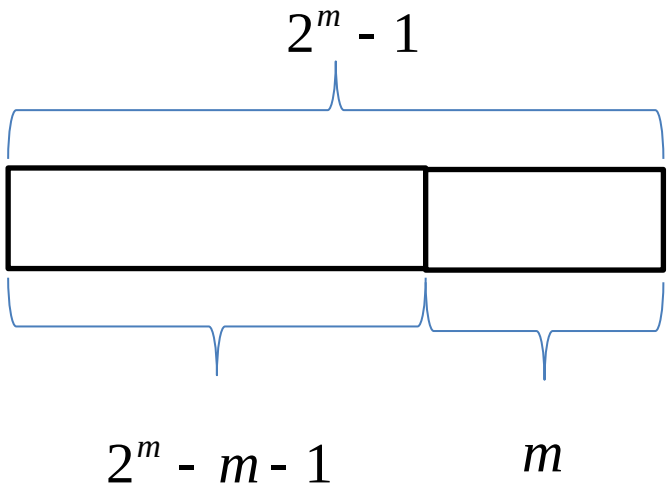
  なぜならば，最小距離を2とすると，$0 \leq i < j < n$ なるi, jに対して，符号語 $W_1(x), W_2(x)$ があり，$W_1(x) - W_2(x) = x^i + x^j$ となるが，巡回符号は線形符号であるので，$W_1(x) - W_2(x)$ も符号語である．従って，$G(x) | (x^i + x^j)$ でありさらに，$G(x) | (x^{j-i} + 1)$ となるが，$0 < j - i < n \leq p$となり，$G(x)$の周期がpであることに矛盾する．■

巡回符号 — 性質

m次の原始多項式を生成多項式とする符号の最小距離 $d_{\min}$ はちょうど3.

(証明)

- まず $d_{\min} \geq 3$ は，生成多項式が原始多項式であることから証明できる．
- m $(m \geqq 3)$次の原始多項式を生成多項式とする巡回ハミング符号



- 符号語の個数 $2^{2^m - m - 1}$
- 各符号語の周りのハミング距離2の語数

$$\frac{(2^m - 1)(2^m - 2)}{2} > \frac{2^m \times 2^m}{2 \times 2} = 2^{2m-2} \quad \text{L} \ (m \geq 3)$$

- 符号語＋その周りのハミング距離2の語数

$$> 2^{2^m - m - 1} \times 2^{2m-2} = 2^{2^m + m - 3} > 2^{2^m - 1}$$

- 従って，長さ $2^m - 1$ の可能な語数を超えることになり，どの語の間もハミング距離2×2を保つことはできない (最小距離は3以下)．

巡回符号 — 性質

- 長さlのバースト誤りの多項式表現を

$$B(x) = x^{l-1} + b_{l-2}x^{l-2} + \cdots + b_1 x + 1$$

とし，多項式表現で のバースト誤り多項式表現を

$$E(x) = x^i B(x) = x^{i+l-1} + b_{l-2}x^{i+l-2} + \cdots + b_1 x^{i+1} + x^i$$

とする．

$G(x)$ を生成多項式とする巡回符号において，$G(x) \mid E(x)$ でなければ，$E(x)$は符号多項式ではないので，検出可能である．しかるに，符号多項式で使われる生成多項式$G(x)$ は x^0 の係数が 1 であり，$0 < j$ なる j に対して x^j を因数として持たないので，$G(x) \mid E(x)$ であることの必要十分条件は，$G(x) \mid B(x)$ であることである．

従って，$G(x)$の次数をmとするとき，$l \leq m$ のときは$G(x) \mid B(x)$ にはなり得ない．

以上から，m次の生成多項式を使った巡回符号では，長さm以下のバースト誤りを検出できる．

巡回符号 — 復号

- 予め，次のようにして，$0 \le i \le n-1$となるすべてのiに対する誤り位置判定表を作成しておく．

誤り位置	シンドローム
…	…
i	x^iを$G(x)$で割ったときの剰余
…	…

- 受信語$(y_0, \cdots, y_{n-1})$の多項式表現は$y_{n-1}x^{n-1} + \cdots + y_0$を生成多項式で割ったときの剰余$R(x) = r_{m-1}x^{m-1} + \cdots + r_0$を計算する．
- $R(x)=0$ならば，誤りなしと判定する．$R(x)\neq 0$の場合は誤り位置判定表に従って該当する位置の情報ビットを訂正する．

巡回符号 — 復号

- 伝送した符号に対応する符号多項式 $W(x) = w_{n-1}x^{n-1} + \mathrm{L} + w_0$ に対して，誤り x' が加わると，受信語に対応する多項式表現は

$$Y(x) = y_{n-1}x^{n-1} + \mathrm{L} + y_0 = w_{n-1}x^{n-1} + \mathrm{L} + (1 + w_{i+1})x^i + \mathrm{L} + w_0$$

となるが，

$$W(x) = A(x)G(x)$$

であるので，

$$Y(x) = W(x) + x^i = A(x)G(x) + x^i$$

となり，$Y(x)$ を $G(x)$ で割ったときの剰余は x' を $G(x)$ で割ったときの剰余に等しく，それが皆違っていると，i が特定できる．

巡回符号 — 復号

例： $(x^4+x+1)\,|\,(x^{15}-1)$ **を満たす** x^4+x+1 **を生成多項式とする**(15,11)**巡回符号に対する誤り位置判定表**：

誤り位置	シンドローム
0	1
1	x
2	x^2
3	x^3
4	$x+1$
5	x^2+x
6	x^3+x^2
7	x^3+x+1
8	x^2+1
9	x^3+x
10	x^2+x+1
11	x^3+x^2+1
12	x^3+x^2+x+1
13	x^3+x^2+1
14	x^3+1

巡回符号 — 生成行列と検査行列

x'を$G(x)$で割ったときの剰余を$P_j(x)$,$P_j(x)$における x' の係数を $P_{i,j}$ とする.
すなわち,

$$P_j(x) = x^j \mod G(x)$$

$$P_j(x) = p_{m,j}x^m + \cdots + p_{0,j}$$

とする. 検査行列は,

$$H = \begin{bmatrix} p_{0,0} & \cdots & p_{0,n-1} \\ \vdots & \ddots & \vdots \\ p_{m-1,0} & \cdots & p_{m,m-1} \end{bmatrix} \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix} \vdots \begin{bmatrix} p_{0,m} & \cdots & p_{0,n-1} \\ \vdots & \ddots & \vdots \\ p_{m-1,m} & \cdots & p_{m-1,n-1} \end{bmatrix} = [I_m \vdots P_c]$$

となる. ここで,

$$P_c = \begin{bmatrix} p_{0,m} & \cdots & p_{0,n-1} \\ \vdots & \ddots & \vdots \\ p_{m-1,m} & \cdots & p_{m-1,n-1} \end{bmatrix}$$

巡回符号 — 生成行列と検査行列

生成行列は，

$$G = [P_c^{\mathrm{T}} \vdots I_{n-m}]$$

に従って構成する．ここで，

$$G = \left[\begin{array}{ccc:ccc} p_{0,m} & & p_{m-1,m} & 1 & & \\ & \mathrm{O} & & & \mathrm{O} & \\ p_{0,n-1} & & p_{m,n-1} & & & 1 \end{array}\right]$$

巡回符号 — 生成行列と検査行列

生成行列は，

$$G = [P_c^{\mathrm{T}} \vdots I_{n-m}]$$

に従って構成する．ここで，

$$G = \left[\begin{array}{ccc:ccc} p_{0,m} & & p_{m-1,m} & 1 & & \\ & \mathrm{O} & & & \mathrm{O} & \\ p_{0,n-1} & & p_{m,n-1} & & & 1 \end{array}\right]$$

巡回符号 — 生成行列と検査行列

例: $(x^4+x+1)\,|\,(x^{15}-1)$ **を満たす** x^4+x+1 **を生成多項式とする**(15,11)**巡回符号**

検査行列:

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

生成行列:

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

巡回ハミング符号

$G(x)$が原始多項式のときは，$G(x)$を生成多項式とする巡回符号は

符号長： $n = 2^m - 1$

情報ビット長： $k = 2^m - 1 - m$

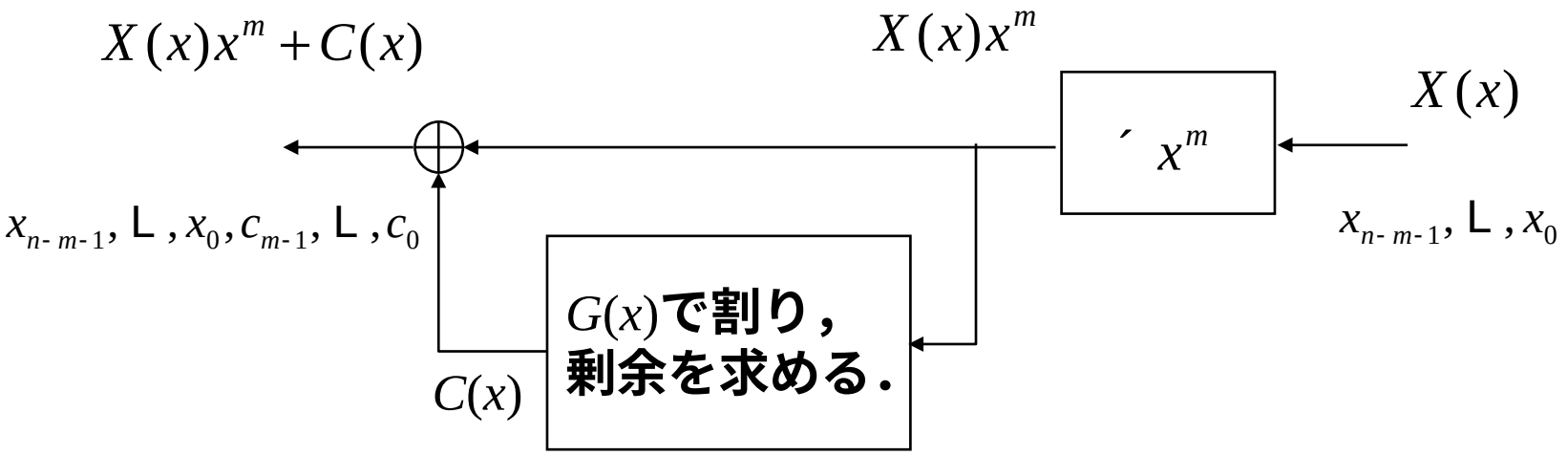
検査ビット長： m

の単一誤り訂正符号となる．

⇒ 巡回ハミング符号と呼ばれる．

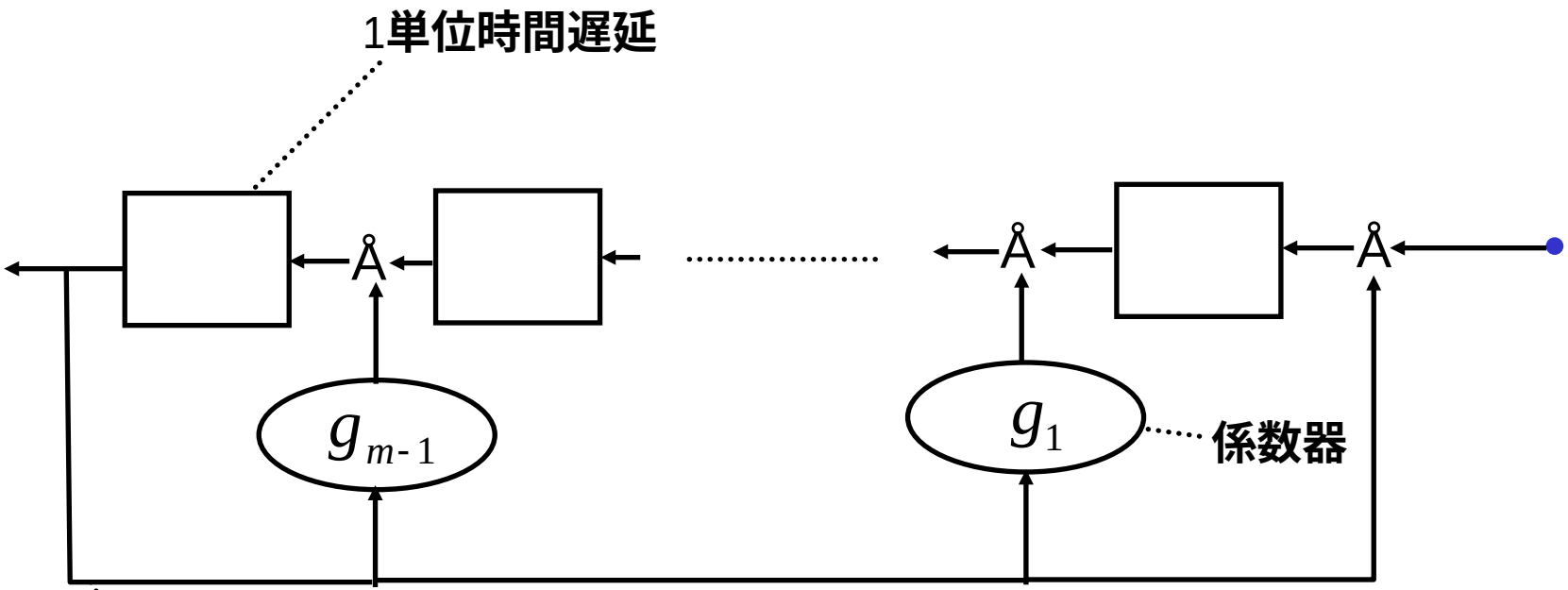
符号器

- 符号化の中心は，生成多項式 $G(x) = x^m + g_{m-1}x^{m-1} + \cdots + g_1 x + 1$ による割り算である．
- 情報ビットに対応する多項式に x^m を乗じること，その後，$G(x)$による割り算の実行過程がシフトレジスタと加算器で表現されている．



除算器

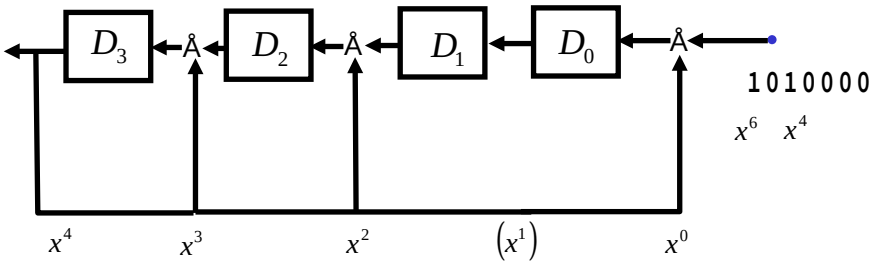
$g_{m-1}x_{m-1} + \mathrm{L} + 1$ による除算器⇒m段シフトレジスタ回路で構成

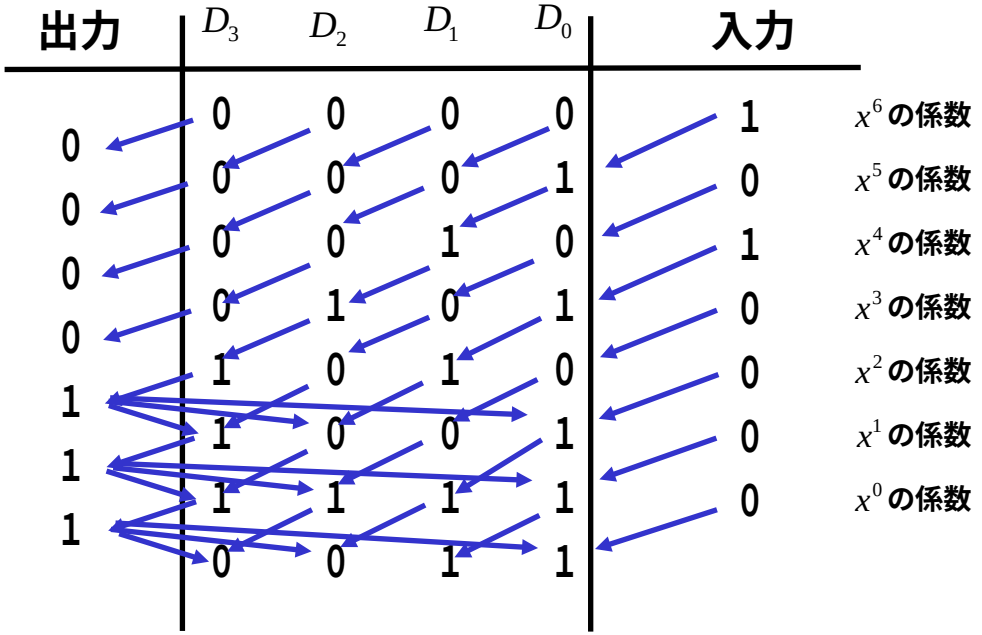


ここに1が立つときは $g_{m-1}x^{m-1} + \mathrm{L} + 1$ が足される（＝引かれる）

割り算回路

(例)　$G(x) = x^4 + x^3 + x^2 + 1$ による割り算回路とその動き.





商が1のとき，x^3, x^2, x^0 に対応するビットに1が加えられる