北海道大学
Hokkaido University

情報エレクトロニクス学科共通科目・2年次・夏ターム〔必修科目〕

講義「情報理論」

第13回

第8章 通信路符号化法(3)

8.3 巡回符号

巡回符号

- 巡回符号の特徴
  - 線形符号、符号化・シンドローム計算の装置化が容易
  - 巡回ハミング符号は復号器の装置化も容易
  - 誤り検出能力に優れる
- 巡回符号の定義
  - 符号多項式:符号語の多項式表現

    0, 1 からなる長さn の符号語 $\mathbf{v}=(v_{n-1}, v_{n-2},\cdots, v_1, v_0)$ を

    $$V(x) = v_{n-1}x^{n-1}+v_{n-2}x^{n-2}+\cdots v_1x+v_0$$

    で表す。

    ⇒符号長 n の符号は、$n-1$次以下の多項式の集合として表せる。
  - 巡回符号(cyclic code)

    定数項が 1 の m 次の多項式$G(x)= x^m+g_{m-1}x^{m-1}+\cdots g_1x+1$の

    $n-1$次以下の倍多項式すべての集合C

    $(W(x)=A(x)G(x)$という形の符号多項式)

係数は0か1しか取らない。演算は常に mod 2 であることに注意！

$g_1,\cdots,g_{m-1}$は0か1

$A(x)$は$n-m-1$次以下の任意の多項式

巡回符号の例

- $G(x)=x^4+x^3+x^2+1$によって作られる長さ7の符号C

  表1：符号多項式 $W(x)=w_6x^6+\cdots+w_1x+w_0$ 及び符号語 $\mathbf{w}=(w_6,\cdots,w_1,w_0)$

  表2：$A(x)=x^2+x+1$の場合の $A(x)$ と $G(x)$ の乗算

- 巡回符号Cは$G(x)$によって生成される

  ⇒$G(x)$：Cの**生成多項式**

  （generator polynomial）

任意の二つの符号語の線形和が符号語になる符号

- **巡回符号Cは線形符号**

  $W_1(x)$と$W_2(x)$はCの符号多項式

  ⇒$W_1(x)=A_1(x)G(x)$, $W_2(x)=A_2(x)G(x)$ と書ける

  ⇒$W_1(x)+W_2(x)=[A_1(x)+A_2(x)]G(x)$

  ⇒$W_1(x)+W_2(x)$はCの符号多項式

項が偶数個だと消える

表1 $G(x)=x^4+x^3+x^2+1$ で作られる符号

$A(x)$	$W_1(x)=A_1(x)G(x)$	w
0	0	0000000
1	$x^4+x^3+x^2+1$	0011101
x	$x^5+x^4+x^3+x$	0111010
$x+1$	x^5+x^2+x+1	0100111
x^2	$x^6+x^5+x^4+x^2$	1110100
x^2+1	$x^6+x^5+x^3+1$	1101001
x^2+x	$x^6+x^3+x^2+x$	1001110
x^2+x+1	x^6+x^4+x+1	1010011

表2 0,1を係数とする多項式の乗算

(a)

$$
\begin{array}{rrrrrrrr}
 & & & x^4 & +x^3 & +x^2 & & +1 \\
\times) & & & & & x^2 & +x & +1 \\
\hline
 & & & x^4 & +x^3 & +x^2 & & +1 \\
 & & x^5 & +x^4 & +x^3 & & +x & \\
 & x^6 & +x^5 & +x^4 & & +x^2 & & \\
\hline
 & x^6 & & +x^4 & & & +x & +1
\end{array}
$$

(b)

$$
\begin{array}{rr}
 & 11101 \\
\times) & 111 \\
\hline
 & 11101 \\
 & 11101 \\
 & 11101 \\
\hline
 & 1010011
\end{array}
$$

巡回符号の符号化の仕方

- $n-m$ 個の情報ビット $x_{n-m-1}, \cdots, x_1, x_0$ をCの符号語に符号化する方法

①情報ビットを係数とする多項式

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

に x^m を掛け、それをm次の$G(x)$で割った剰余多項式

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

を計算。$C(x)$ は

$$X(x)\,x^m = A(x)G(x) + C(x) \quad \text{------------}(1)$$

となる $m-1$次以下の多項式。

[$A(x)$は商多項式であり、$n-m-1$次以下]

②式

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

により$W(x)$を計算。

式(1)から $W(x) = A(x)G(x) \Rightarrow W(x)$ はCの符号多項式

$W(x)$のベクトル表現：

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

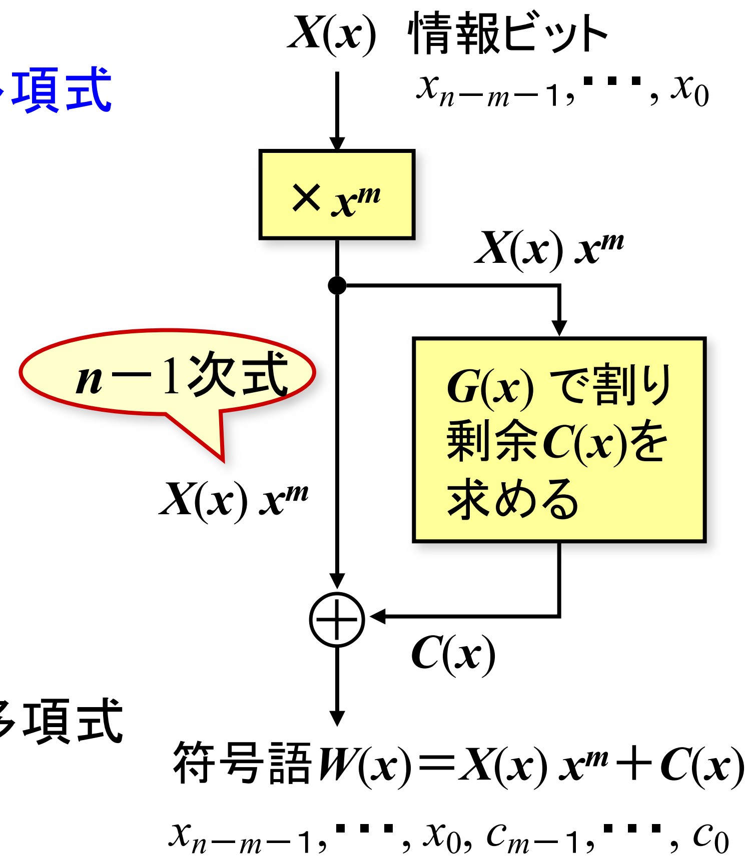


図 巡回符号の符号化

符号化の例

生成多項式: $G(x)=x^4+x^3+x^2+1$ 、

符号長: $n=7$

情報ビット数: $k=3$ (∵生成多項式は4次なので $n-k=4$)

情報ビット 101 の符号化

情報ビットを係数とする多項式: $X(x)=x^2+1$

$x^{n-k}=x^4$ を掛ける: $X(x)\,x^4=x^6+x^4$

$G(x)$ で割った剰余: $C(x)=x+1$

符号多項式: $W(x)=X(x)\,x^4+C(x)=x^6+x^4+x+1$

符号語: (1010011)

表 0,1を係数とする多項式の割り算

(a)

$$
\begin{array}{r|l}
 & x^2+x+1 \\
\hline
x^4+x^3+x^2+1 & x^6+x^4 \\
 & x^6+x^5+x^4+x^2 \\
\cline{2-2}
 & x^5+x^2 \\
 & x^5+x^4+x^3+x \\
\cline{2-2}
 & x^4+x^3+x^2+x \\
 & x^4+x^3+x^2+1 \\
\cline{2-2}
 & x+1
\end{array}
$$

(b)

```
            111
11101 ) 1010000
        11101
        10010
        11101
         11110
         11101
          0011
```

なぜ「巡回」なのか？

- 符号長 n、生成多項式$G(x)$の巡回符号において、$G(x)$が x^n-1を割り切れば

$W(x)=w_{n-1}x^{n-1}+\cdots+w_1x+w_0$ が符号多項式
$\Rightarrow W'(x)=w_{n-2}x^{n-1}+\cdots+w_0x+w_{n-1}$
$\quad=xW(x)-w_{n-1}(x^n-1)$
という多項式もまた符号多項式

この部分が$G(x)$で割り切れる

$\mathbf{w}=(w_{n-1},\cdots,w_1,w_0)$ が符号語
⇒$\mathbf{w}$の成分を巡回置換して得られる$\mathbf{w}'$も符号語

$\mathbf{w}=(w_{n-1},w_{n-2},w_{n-3},\cdots,w_1,w_0)$

$\mathbf{w}'=(w_{n-2},w_{n-3},\cdots,w_1,w_0,w_{n-1})$

図 wの成分の巡回置換

- 本来、長さnの巡回符号の生成多項式$G(x)$はx^n-1を割り切らなければならない。
- これが成立しないものを擬巡回符号（pseudo-cyclic code）と呼ぶ。
- $G(x)$ で生成される符号は、$G(x)$がx^n-1を割り切らなくても、ほとんど同様に扱えるため、ここでは擬巡回符号も含めて、単に巡回符号と呼ぶことにする。

$G(x)$の周期

- 多項式$G(x)$ の周期:

  $G(x)$がx^n-1を割り切る最小の正整数 n

- $G(x)$ 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。

  $n>p$ であると、

  x^p-1 は$n-1$次以下の多項式であり$G(x)$ で割り切れる

  ⇒x^p-1 は Cの符号多項式

  ⇒符号の最小ハミング距離が２以下

  （∵x^p-1に対応する符号のハミング重みは 2）

  ⇒誤り訂正できない

  ハミング重み＝ベクトル中の1の個数

- 【例】$G(x)=x^4+x^3+x^2+1$ を生成多項式とする長さ7 の巡回符号

  $G(x)$ の周期は 7（∵$G(x)=x^4+x^3+x^2+1$ は、x^7-1を割り切るが、$x^\ell-1$（$\ell=1, 2, \cdots, 6$）は割り切らない）

  本来の意味の巡回符号となっている。

巡回符号の符号器のための割り算回路

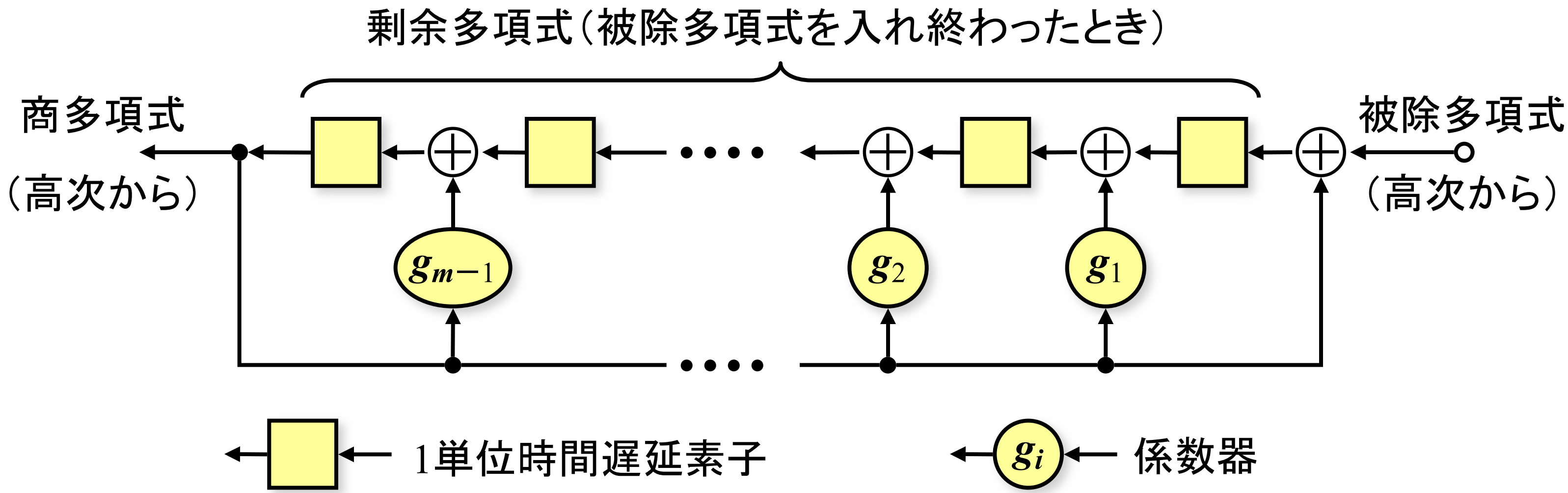


図 割り算回路

この回路で任意の多項式を$G(x)$で割った剰余多項式が求まるので、後は被除多項式と足し合わせるだけでよい

- 図は、生成多項式$G(x)$

$$G(x) = x^m + g_{m-1}x^{m-1} + \cdots g_1 x + 1$$

で割り算を行う回路である。

- このような m個の遅延素子が直列に接続されている回路を、しばしばm段シフトレジスタ回路と呼ぶ。また、この回路にクロックパルスを印加することを、回路をシフトするという。

割り算回路の動作例

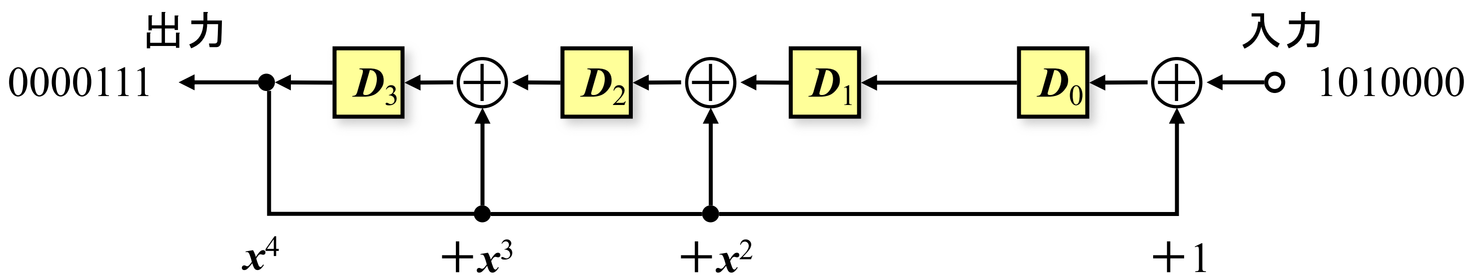


図 $x^4+x^3+x^2+1$ による割り算回路

- 図は、$G(x)=x^4+x^3+x^2+1$ で割り算を行う回路である。
- 表は、被除数多項式が x^6+x^4 であるときの遅延素子 D_3, D_2, D_1, D_0 の状態の推移を示す。

(a)

$$
\begin{array}{r|l}
 & x^2+x+1 \\
\hline
x^4+x^3+x^2+1 & x^6 \quad +x^4 \\
 & x^6+x^5+x^4 \quad +x^2 \\
\hline
 & x^5 \quad +x^2 \\
 & x^5+x^4+x^3 \quad +x \\
\hline
 & x^4+x^3+x^2+x \\
 & x^4+x^3+x^2 \quad +1 \\
\hline
 & x+1
\end{array}
$$

(b)

$$
\begin{array}{r|r}
 & 111 \\
\hline
11101 & \boxed{1010}000 \\
 & 11101 \\
\hline
 & \boxed{10010} \\
 & 11101 \\
\hline
 & \boxed{11110} \\
 & 11101 \\
\hline
 & \boxed{0011}
\end{array}
$$

表 割り算回路の動作

出力	状態 D_3	D_2	D_1	D_0	入力
	0	0	0	0	
0					1
	0	0	0	1	
0					0
	0	0	1	0	
0					1
	0	1	0	1	
0					0
	1	0	1	0	
1					0
	1	0	0	1	
1					0
	1	1	1	1	
1					0
	0	0	1	1	

巡回符号による誤りの検出

- 誤りの検出：受信語 y が符号語になるかどうかを調べる
- $n-1$次以下の多項式$Y(x)$が長さn,生成多項式$G(x)$の巡回符号の符号多項式
  ⇔$Y(x)$が$G(x)$で割り切れる
- CRC（cyclic redundancy check）方式

受信語 $\mathbf{y}=(y_{n-1},\cdots,y_1,y_0)$ を表す多項式
$Y(x)=y_{n-1}x^{n-1}+\cdots+y_1x+y_0$が$G(x)$で割り切れない ⇒誤りがある

‖

受信語を$G(x)$で割る割り算回路に読み込ませて、剰余が 0 にならない

- このCRC方式には、CCITT（国際電信電話諮問委員会）でCRC-16-CCITTとして標準化された

$$G(x)=x^{16}+x^{12}+x^5+1$$

という生成多項式がよく用いられる。

CRC−16−CCITT($G(x)=x^{16}+x^{12}+x^5+1$)の特性 1

- $G(x)=x^{16}+x^{12}+x^5+1$ を因数分解すると、

$$G(x)=(x+1)(x^{15}+x^{14}+x^{13}+x^{12}+x^4+x^3+x^2+x+1)$$

となる。それぞれの因数は既約多項式(irreducible polynomial)。

- $G(x)$の周期: $p=32767$

異なる既約多項式の積の周期は、それぞれの周期の最小公倍数

$x+1$の周期: 1

$x^{15}+x^{14}+x^{13}+x^{12}+x^4+x^3+x^2+x+1$ の周期: $2^{15}-1=32767$

- G(x)を生成多項式とする符号の最小距離$d_{\min}$:

符号長n: $n>p$だと$d_{\min}\leqq 2$となるので$n\leqq p$とする

$d_{\min}=2 \Rightarrow W(x)=x^i+x^j=x^j(x^{i-j}+1)$ ($0\leqq j<i<n$)

という形の符号多項式が存在(∵ハミング重み2の符号が存在)

$\Rightarrow$ $W(x)$ は$G(x)$ で割り切れるから $x^{i-j}+1$は$G(x)$で割り切れる

$\Rightarrow$G(x)の周期は$i-j$以下

$\Rightarrow 0<i-j<n\leqq p$ なので、$G(x)$の周期がp であることと矛盾

$\Rightarrow d_{\min}\neq 2$

$d_{\min}\neq 1$ であることは簡単に確かめられるので、$d_{\min}\geqq 3$

CRC-16-CCITT($G(x)=x^{16}+x^{12}+x^5+1$)の特性 2

- G(x)を生成多項式とする符号の最小距離$d_{\min}$（つづき）:
  符号語の重みは偶数
  ∵$G(x)$ の項数は4であり偶数

  $\Rightarrow W(x) = (x^{16}+x^{12}+x^5+1)A(x)$と書ける

  $\Rightarrow W(1) = w_{n-1}+\cdots+w_1+w_0$

  $=(1^{16}+1^{12}+1^5+1)A(1)$

  $= 0$

  ここが 0

  ⇒W(x)は偶数個の項からなる

  以上から、$d_{\min}\geqq 4$ 。

  $A(x)=1$ の場合を考えよ
- 生成多項式$G(x)=x^{16}+x^{12}+x^5+1$ は、それ自身符号多項式
  ⇒ハミング重み4の符号語が存在⇒$d_{\min}\leqq 4$
- この生成多項式で生成される符号長32767 以下の符号は$d_{\min}=4$であるので、
  3個以下の任意の誤りを検出できる。

CRC-16-CCITT($G(x)=x^{16}+x^{12}+x^5+1$)の特性 3

- 長さ16以下のバースト誤りの検出も可能

図のような長さℓのバースト誤りパターンを多項式で表せば、

$$E(x)=x^i B(x)$$

となる。ここに、$B(x)$ は

$$B(x)=x^{\ell-1}+b_{\ell-2}x^{\ell-1}+\cdots+b_1x+1$$

という$\ell-1$次の多項式である。

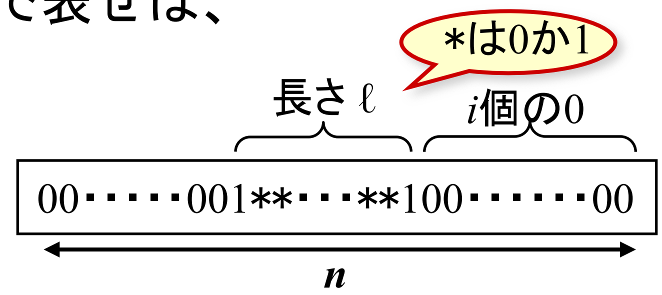


図　長さℓのバースト誤りの誤りパターン

バースト誤りE(x)がCRC方式で検出できる

⇔任意の符号語$W(x)$に対し$W(x)+E(x)$が符号語とはならない

⇔$E(x)$ が $G(x)$ で割り切れない

⇔$B(x)$ が $G(x)$で割り切れない（$\because G(x)$ は x を因数として含まない）

$G(x)=x^{16}+x^{12}+x^5+1$ の場合、次数は 16 であるので、

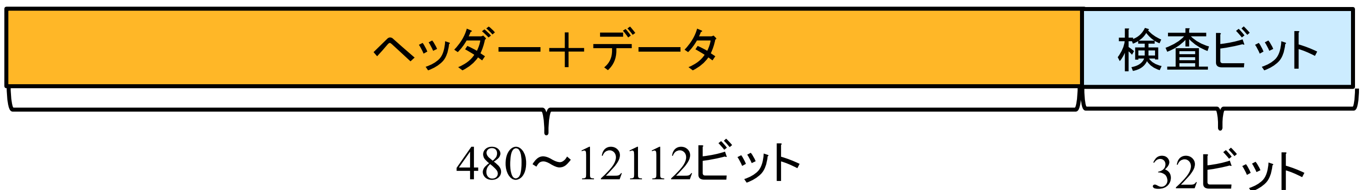
$B(x)$ が15次以下の多項式ならばG(x)で割り切れることはない

⇒長さ16以下の任意のバースト誤りは検出可能

長さ17以上のバースト誤りの大部分は検出可能であることがわかっている

イーサーネットの規格(IEEE 802.3)で使われているCRC方式

- イーサーネット(IEEE 802.3)のパケット構成



- 生成多項式

$$G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

- 符号の最小距離=4 (パケット長の範囲内)
  ３重誤りまではすべて検出可能
- 長さ32までの連続区間内で発生した多重誤りを全て検出可能

巡回ハミング符号

- 0,1 を係数とする m次の多項式の周期≦2^m-1
- 原始多項式(primitive polynomial)

  周期がちょうど2^m-1 となるm次の多項式

  各次数について原始多項式の存在することが証明されている。
- 巡回ハミング符号

  m次の原始多項式を生成多項式とする

  符号長 $n=2^m-1$ の符号

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

最小距離: $d_{\min}=3$ ⇒単一誤り訂正符号

∵符号長＝周期

⇒最小距離$d_{\min}$≧3以上

ちょうど3になることも確認できる。

ハミング符号！

表 20次までの原始多項式の例

次数	原始多項式	次数	原始多項式
1	$x+1$	11	$x^{11}+x^2+1$
2	x^2+x+1	12	$x^{12}+x^6+x^4+x+1$
3	x^3+x+1	13	$x^{13}+x^4+x^3+x+1$
4	x^4+x+1	14	$x^{14}+x^{10}+x^6+x+1$
5	x^5+x^2+1	15	$x^{15}+x+1$
6	x^6+x+1	16	$x^{16}+x^{12}+x^3+x+1$
7	x^7+x+1	17	$x^{17}+x^3+1$
8	$x^8+x^4+x^3+x^2+1$	18	$x^{18}+x^7+1$
9	x^9+x^4+1	19	$x^{19}+x^5+x^2+x+1$
10	$x^{10}+x^3+1$	20	$x^{20}+x^3+1$

巡回ハミング符号の例

- $G(x)=x^3+x+1$を生成多項式とする長さ7の巡回ハミング符号
  この符号の検査行列を求める。
- $R_i(x):x^i(i=0, 1,\cdots, 6)$を $G(x)$ で割った剰余多項式
  これを実際に計算すると表のようになる。
- $W(x) = w_{n-1}x^{n-1}+\cdots+w_1x+w_0$ が $G(x)$ で割り切れる
  $\Leftrightarrow w_ix^i$ を $G(x)$で割った剰余多項式の和が 0
  $\Leftrightarrow \sum_{i=0}^{6} w_iR_i(x) = 0$.
  この式の左辺を x の2, 1, 0次の項の係数ごとに書けば

$$\left.\begin{array}{l} w_6+w_5+w_4+w_2=0 \\ w_5+w_4+w_3+w_1=0 \\ w_6+w_5+w_3+w_0=0 \end{array}\right\}$$

となる。この係数行列は

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

Hは(7,4)ハミング符号の検査行列!

表 x^iを$G(x)=x^3+x+1$ で割った剰余多項式$R_i(x)$

i	$R_i(x)$
0	1
1	x
2	x^2
3	$x+1$
4	x^2+x
5	x^2+x+1
6	x^2+1

多重誤り訂正が可能な巡回符号

- BCH符号(Bose-Chaudhuri-Hocquenghem code)
  符号長: $=2^m - 1$
  情報ビット数: $\geqq 2^m - 1 - m(d - 1)$
  最小距離: $\geqq d$
- リード・ソロモン符号(Reed-Solomon code)
  q元BCH符号
  符号長: $=q - 1$
  情報ビット数: $=q - d$
  最小距離: $=d$

音楽CD, DVD, ２次元バーコード, QRコード, 衛星放送,
地上波デジタル放送等で利用されている！