11. 通信路符号化法 ― 巡回符号

巡回符号は，ブール多項式の演算を使って体系的に構成された誤り訂正符号である．

11.1 符号の多項式表現

情報ビットや符号語を表す，長さnの符号アルファベットのベクトル

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

に対応する次のGF(2)上の多項式：

$$V(x) = v_{n-1}x^{n-1} + \cdots + v_1x^1 + v_0x^0$$

をvの**多項式表現**と呼ぶ[1]．vが想定している符号の符号語であるときは$V(x)$は**符号多項式**と呼ばれる．GF(2)の多項式は，係数がGF(2)の要素であることを除けば，実数を係数とする多項式と同様に加減乗除が定義される．例えば

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

とすると，

$$G(x) + H(x) = G(x) - H(x) = x^4 + x$$
$$G(x) \cdot H(x) = x^6 + x^4 + x^3 + x^2 + x^4 + x^2 + x + 1 = x^6 + x^3 + x + 1$$
$$G(x) = x^2H(x) + x + 1$$
$$G(x) = x + 1 \mod H(x)$$

ここで最後の除算は図 1 のような組み立て算で求めることができる．あるいは計算に本質的な係数の部分だけ取り出して，図 2 のようにしてもよい．

$G(x)$が$H(x)$を割り切るとき，

$$G(x) \mid H(x)$$

と表記する．

$$G(x) \mid (x^n - 1)$$

となる 最小の正整数nを$G(x)$の**周期**と呼ぶ．例えば，図 3 の計算から，

$$(x^4 + x^2 + x + 1) \mid (x^7 - 1)$$

であり，7 より小さいmに対して，$(x^4 + x^2 + x + 1) \mid (x^m - 1)$とはならないので，$x^4 + x^2 + x + 1$の周期が 7 であることがわかる．

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

図 1. 組み立て算による除算の実行

$$\begin{array}{r|l} & 1\ 0\ 0 \\ \hline 1\ 0\ 1 & 1\ 0\ 1\ 1\ 1 \\ & 1\ 0\ 1 \\ \hline & 1\ 1 \end{array}$$

図 2. 図 1 の組み立て算で係数だけを表示したもの

[1] $v = (v_{n-1}, \cdots, v_1, v_0)$という表記は，通常の表記の逆順であるが，符号多項式との対応関係が直感的にわかりやすいので，巡回符号，BCH 符号の議論ではこの表記を用いることにする．

```
          1 1 0 1
      ┌──────────
1 1 1 0 1 ) 1 0 0 0 0 0 0 1
            1 1 1 0 1
            ─────────
              1 1 0 1 0
              1 1 1 0 1
              ─────────
                  1 1 1 0 1
                  1 1 1 0 1
                  ─────────
                          0
```

図 3．組み立て算によるx^4+x^2+x+1の周期の計算

0,1を係数とするm次の多項式の周期は高々2^m-1である．なぜならば，x^n-1という多項式をm次多項式$a_m x^m+\cdots+a_1 x+a_0$で割り算をする状況を考えると，出現する剰余は，$b_{m-1}x^{m-1}+\cdots+b_1 x+b_0$でという形をしている．これらは高々$2^m-1$通りの異りしか持たない．

例えば，$m=4$に対して，周期が最大になる場合を図 4 に示す．はじめのところで，0001,0010,0100,1000と，4回数えられていることに注意すれば，赤で囲まれたところに$2^4=16$通りのパターンが出尽くしている．周期が2^m-1となるm次多項式を**原始多項式**と呼ぶ．GF(2)の上の原始多項式を求めてみよう．

$m=1$のときは，$x+1$である．

$m=2$のときは，$2^m-1=3$であるので，周期3の2次多項式を探すことになる．x^2+1の周期は2であるが，$(x+1)(x^2+x+1)=x^3+1$であるので，x^2+x+1の周期が3であり，原始多項式であることがわかる．

$m=3$のときは，$(x^3+x+1)(x^4+x^2+x+1)=x^7+1$，また，$n<7$なる整数$n$に対して，$x^3+x+1$が$x^n+1$を割り切ることがない（図 5）．

$m=4$のときは，$(x^4+x+1)(x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)=x^{15}+1$，また，$n<15$なる整数$n$に対して，$x^4+x+1$が$x^n+1$を割り切ることはない（図 6）．

m次の原始多項式の例を表 1 に示す．

GF(2)上の多項式$G(x)$の周期がpであれば，$G(x)\mid(x^n-1)$であるための必要十分条件は，$p\mid n$となることである．なぜならば，$p\mid n$でないとすると，$n=ap+b, 0<b<p$と書けるはずである．一方，$G(x)\mid(x^n-1)$かつ$G(x)\mid(x^p-1)$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，$(x^p-1)\mid(x^{ap}-1)$であるので，$x^{ap}-1=(x^p-1)C(x)$と書ける．

$$\begin{aligned}x^n-1&=x^{ap+b}-1\\&=x^b x^{ap}-1\\&=x^b\big((x^p-1)C(x)+1\big)-1\\&=x^b G(x)B(x)C(x)+x^b-1\end{aligned}$$

従って，$G(x)\mid(x^b-1)$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，$p\mid n$でなければならない．

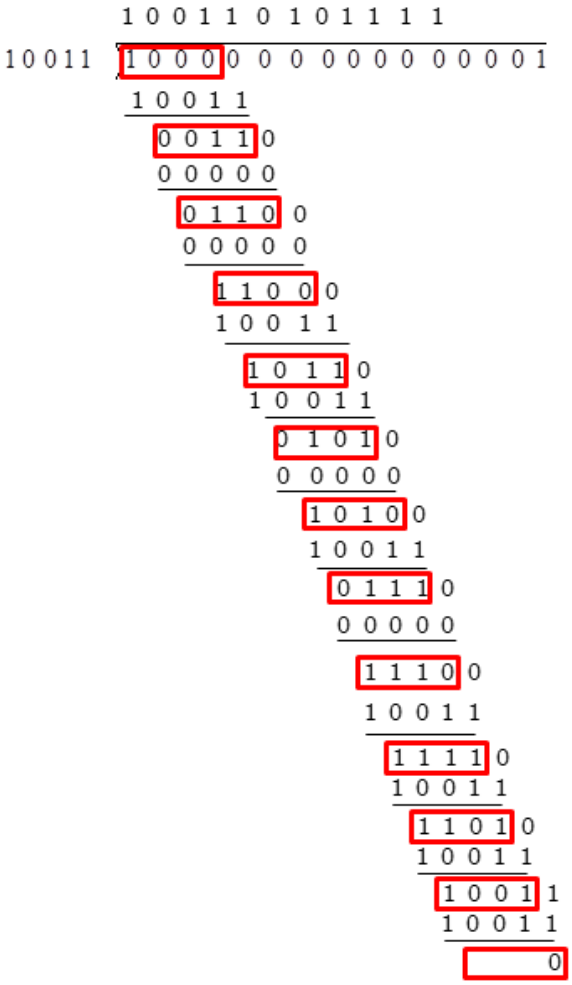

図 4. 周期の計算:原始多項式x^4+x+1の場合

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$F(x)$をGF(2)上の**規約多項式**と呼ぶ．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はそれぞれの周期の最小公倍数である．

証明：$F_1(x)\times\cdots\times F_n(x) \mid (x^n-1)$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．■

```
          1 0 1 1 1
      ------------------
1 0 1 1 ) 1 0 0 0 0 0 1
          1 0 1 1
          -------
            1 1 0 0
            1 0 1 1
            -------
              1 1 1
              1 0 1 1
              -------
                1 0 1 1
                -------
                    0
```

図 5. x^3+x+1の周期計算

```
              1 0 0 1 1 0 1 0 1 1 1 1
          ----------------------------
10011 ) 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1
          1 0 0 1 1
          ---------
            0 0 1 1 0
            0 0 0 0 0
            ---------
              0 1 1 0 0
              0 0 0 0 0
              ---------
                1 1 0 0 0
                1 0 0 1 1
                ---------
                  1 0 1 1 0
                  1 0 0 1 1
                  ---------
                    0 1 0 1 0
                    0 0 0 0 0
                    ---------
                      1 0 1 0 0
                      1 0 0 1 1
                      ---------
                        0 1 1 1 0
                        0 0 0 0 0
                        ---------
                          1 1 1 0 0
                          1 0 0 1 1
                          ---------
                            1 1 1 1 0
                            1 0 0 1 1
                            ---------
                              1 1 0 1 0
                              1 0 0 1 1
                              ---------
                                1 0 0 1 1
                                1 0 0 1 1
                                ---------
                                      0
```

図 6. x^4+x+1は，$n<15$なる整数nに対してx^n+1を割り切ることがないが，$x^{15}+1$は割り切る．

表 1. いろいろな次数の原始多項式の例

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	$x^{10}+x^3+1$
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	$x^{20}+x^3+1$

11.2 巡回符号

巡回符号は，$G(x) \mid (x^n-1)$を満たすm次の**生成多項式**$G(x)$を用いて構成される$(n, n-m)$符号である．

【符号化】

1. 与えられた$n-m$個の情報ビット$x_0, x_1, \cdots, x_{n-m-1}$に対応する多項式
$$X(x) = x_{n-m-1}x^{n-m-1} + \cdots + x_1 x + x_0$$
にx^mを掛ける．
2. それを$G(x)$ （m次多項式）で割ったときの剰余多項式を
$$C(x) = c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$$
とする．すなわち，$C(x)$は，
$$X(x)x^m = A(x)G(x) + C(x)$$
となる$m-1$次多項式である．
3. 求める符号多項式は
$$W(x) = X(x)x^m - C(x) = X(x)x^m + C(x)$$
である．

例：$(x^4+x+1) \mid (x^{15}-1)$であるので，$x^4+x+1$を生成多項式とする$(15,11)$巡回符号を構成する．与えられた11個の情報ビット
$$(x_{10}, x_9, x_8, x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0) = (1,0,1,1,0,1,0,0,0,1,1)$$
に対応する多項式は，$X(x) = x^{10}+x^8+x^7+x^5+x+1$である[2]．
$$X(x)x^m = x^4(x^{10}+x^8+x^7+x^5+x+1) = A(x)G(x) + C(x)$$
と置いて，$A(x)$と$C(x)$を求めると，図 7 のようになることから，
$$A(x) = x^{10}+x^8+x^6+x^4+x^3+x^2+1$$
$$C(x) = x^2+x+1$$
であり，求める符号多項式は
$$W(x) = x^{14}+x^{12}+x^{11}+x^9+x^5+x^4+x^2+x+1$$
符号語は
$$(w_{14}, w_{13}, w_{12}, w_{11}, w_{10}, w_9, w_8, w_7, w_6, w_5, w_4, w_3, w_2, w_1, w_0) = (1,0,1,1,0,1,0,0,0,1,1,0,1,1,1)$$
であることがわかる．このように，巡回符号では，チェックビット$w_3, \cdots, w_0$は，情報ビット$w_{14}, \cdots, w_4$の後ろにつながれることなる．

巡回符号の性質

このようにして構成される巡回符号の性質を調べてみよう．

(1) 生成多項式$G(x)$を用いて構成される巡回符号の符号語を$W(x)$とすると，$G(x) \mid W(x)$で

[2] 情報ビットと情報多項式$X(x)$の対応付けについても，便宜上多項式の高次の桁の係数を情報ビットの左に対応付けることにする．これは便宜的なものであり，ブール多項式の演算を主体とする議論の本質にはかかわるものではない．

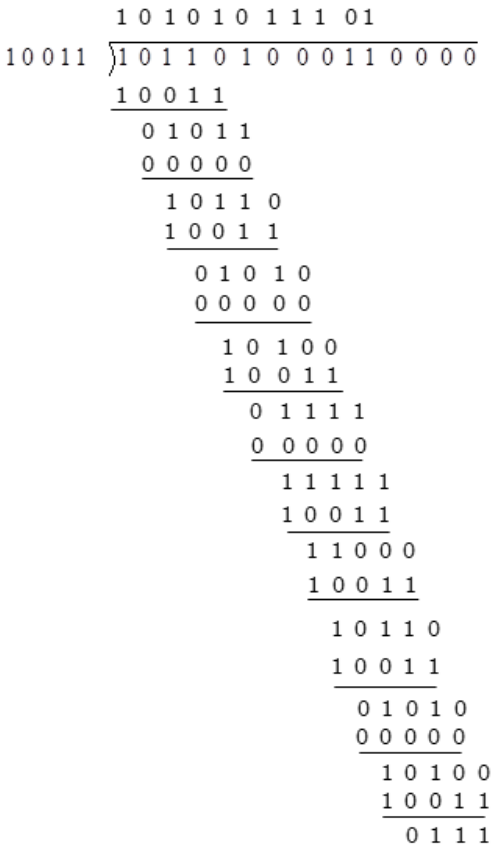

図 7.　$x^4(x^{10}+x^8+x^7+x^5+x+1)=A(x)G(x)+C(x)$ と置いて，$A(x)$と$C(x)$を求める．ただし，$G(x)=x^4+x+1$.

ある．なぜならば，巡回符号の構成法により，ある多項式$G(x)$，$C(x)$に対して，$A(x)$と$W(x)$は

$$X(x)x^m=A(x)G(x)+C(x)$$
$$W(x)=X(x)x^m+C(x)$$

と表されるので，

$$X(x)x^m=A(x)G(x)+C(x)$$
$$W(x)=X(x)x^m+C(x)=A(x)G(x)+C(x)+C(x)=A(x)G(x)$$

が導ける．

逆に，$G(x)\mid(x^n-1)$を満たすm次の**生成多項式**$G(x)$を用いて構成される$(n,n-m)$巡回符号が与えられたとき，$G(x)V(x)$を満たす$n-1$次以下の任意の多項式

$$v_{n-1}x^{n-1}+v_{n-2}x^{n-2}+\cdots+v_mx^m+v_{m-1}x^{m-1}+\cdots+v_1x+v_0$$

が，情報ビット$(v_{n-1},v_{n-2},\cdots,v_m)$に対する符号多項式

$$v_{n-1}x^{n-1}+v_{n-2}x^{n-2}+\cdots+v_mx^m$$

になっていることも容易にわかる．

(2) 線形符号

検査記号が情報記号の線形式

$$c = a_1x_1 + \cdots + a_kx_k$$

で与えられる符号は**線形符号**と呼ばれる.

GF(2)の要素から構成される2元符号Cが線形符号であるための必要十分条件は，Cの任意の2つの符号語の和がCの符号語になっていることである.

【問題】　このことを証明せよ.

任意の符号語を$W_1(x), W_2(x)$とすると，ある$A_1(x), A_2(x)$に対して

$$W_1(x) = A_1(x)G(x)$$
$$W_2(x) = A_2(x)G(x)$$

となるので,

$$W_1(x) + W_2(x) = \big(A_1(x) + A_2(x)\big) \cdot G(x)$$

すなわち,

$$A_1(x) + A_2(x) \mid W_1(x) + W_2(x)$$

であるので，前項に述べたように，$W_1(x)$と$W_2(x)$の和もまたCの符号語になっており，巡回符号は線形符号であることがわかる.

線形符号において，$(0,\cdots,0)$に一番近い符号wと$(0,\cdots,0)$との距離をdとすれば，符号の最小距離（すべての符号語の間の距離の最小値）はdである．$3 \le d$であることが少なくとも1誤り訂正可能であるための必要条件となる.

(3) 巡回性

$G(x) \mid (x^n - 1)$を満たす生成多項式$G(x)$を用いて構成される巡回符号において，$(w_{n-1}, w_{n-2}, \cdots, w_0)$が符号語ならば，これを左に一桁巡回させた$(w_{n-2}, \cdots, w_0, w_{n-1})$も符号語である.

なぜならば，$(w_{n-1}, w_{n-2}, \cdots, w_0)$が符号語であることは,

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

が符号多項式であることを意味するが，そのとき，$(w_{n-2}, \cdots, w_0, w_{n-1})$に対する多項式$W'(x)$は,

$$W'(x) = w_{n-2}x^{n-1} + \cdots + w_0x + w_{n-1}$$
$$= xW(x) - w_{n-1}(x^n - 1)$$

となる．$G(x) \mid W(x)$も$G(x) \mid (x^n - 1)$であるので，$G(x) \mid W'(x)$，つまり，$W'(x)$が符号多項式であることが示される.

このように，$w = (w_{n-1}, w_{n-2}, \cdots, w_0)$が符号語であれば，それを巡回シフトした語

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

は，すべて符号語である.

例：$x^4 + x + 1 \mid x^{15} - 1$を満たす$x^4 + x + 1$を生成多項式とする(15,11)巡回符号について考

えてみよう．情報ビット

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

に対応する多項式$X(x)$に対する符号多項式は$x^4 + x + 1$であり，その符号ビットは，$(0,0,0,0,0,0,0,0,0,0,1,0,0,1,1)$となる．これを順に10回まで左に巡回シフトして得られる全部で10個の符号ビットに対応する多項式は$x^k(x^4 + x + 1)$　$(1 \le k \le 10)$という形をしており，すべて符号多項式であることは明らかである．しかし，さらに4回シフトして順に得られる

$(0,0,1,1,0,0,0,0,0,0,0,0,0,1)$　…多項式表現：$x^{12} + x^{11} + 1$

$(0,1,1,0,0,0,0,0,0,0,0,0,1,0)$　…多項式表現：$x^{13} + x^{12} + x$

$(1,1,0,0,0,0,0,0,0,0,0,1,0,0)$　…多項式表現：$x^{14} + x^{13} + x^2$

$(1,0,0,0,0,0,0,0,0,0,1,0,0,1)$　…多項式表現：$x^{14} + x^3 + 1$

については，それらが符号語であることが次のようにして順次確かめられる．

$x^{14} + x^{11} + x^{10}$が符号多項式であることを利用すると，

$$\begin{aligned} x^{12} + x^{11} + 1 &= x(x^{14} + x^{11} + x^{10}) + (x^{15} + 1) \\ &= x \cdot x^{10} \cdot (x^4 + x + 1) \\ &\quad + (x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) \cdot (x^4 + x + 1) \\ &= (x \cdot x^{10} + x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) \cdot (x^4 + x + 1) \\ &= (x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) \cdot (x^4 + x + 1) \end{aligned}$$

…

$$\begin{aligned} x^{14} + x^3 + 1 &= x(x^{14} + x^{11} + x^2) + (x^{15} + 1) \\ &= x \cdot x^2 \cdot (x^{12} + x^{11} + 1) \\ &\quad + (x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) \cdot (x^4 + x + 1) \\ &= x \cdot x^2 \cdot (x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) \cdot (x^4 + x + 1) \\ &\quad + (x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) \cdot (x^4 + x + 1) \\ &= (x \cdot x^2 \cdot (x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) \\ &\quad + (x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1)) \\ &\quad \cdot (x^4 + x + 1) \\ &= (x^{10} + x^7 + x^6 + x^4 + x^2 + x + 1) \cdot (x^4 + x + 1) \end{aligned}$$

一方，情報ビット

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

の多項式表現$X(x) = x + 1$に対する符号多項式は$x^5 + x^4 + x^2 + 1$であり，その符号ビットは，$(0,0,0,0,0,0,0,0,0,1,1,0,1,0,1)$となる．これを順に左に巡回シフトして得られる符号ビットに対応する符号多項式は，全部で15個あるが，それらはどれも$X(x) = 1$に対する符号多項式とは異なる多項式になっている．

(4) 巡回符号の符号長の選び方

$G(x)$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，$G(x) \mid (x^p+1)$であるので，$p<n$とすれば，x^p+1は符号語多項式となり，対応する$(\cdots,0,\cdots,1,\cdots,0,\cdots,1)$が$C$の符号語となるが，この符号語の重みは2であるので，符号語$(0,\cdots,0)$との距離が2となり，1誤りの訂正ができなくなるからである．

(5) 生成多項式の周期をpとするとき，$n \le p$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，$d_{\min} \ge 3$である．なぜならば，最小距離を2とすると，$0 \le i < j < n$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，$W_1(x)-W_2(x)=x^i+x^j$も符号語である．従って，$G(x) \mid (x^i+x^j)$でありさらに，$G(x) \mid (x^{j-i}+1)$となるが，$0<j-i<n \le p$となり，$G(x)$の周期がpであることに矛盾する．

(6) m次の原始多項式を生成多項式とし，符号長nが$n \le 2^m-1$を満足する巡回符号の最小距離$d_{\min}$はちょうど3である．
【証明】生成多項式が原始多項式であるので，$d_{\min} \ge 3$である．
m $(m \ge 3)$次の原始多項式を生成多項式とする$(2^m-1, 2^m-m-1)$巡回符号については，

- 符号語の個数は2^{2^m-m-1}である．
- 各符号語の周りにハミング距離1の語は2^m-1個ある．
- 符号語とその周りのハミング距離1の語（これらは重なりがない）の総数を N とすると
$$N = 2^{2^m-m-1} \cdot (1+2^m-1) = 2^{2^m-m+m-1} = 2^{2^m-1}$$
である．
- このように符号語とその周りのハミング距離1の語を全部集めると，ちょうど長さ2^m-1の語によって表現可能な表現の数2^{2^m-1}になり，それ以外の語はないので，どの語もちょうど距離3だけ離れていることになる．

(7) 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$x^i \sim x^{i+l-1}$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，$l \le m$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．

【復号】

予め，$0 \le i \le n-1$となるすべてのiに対する誤り位置判定表（図 8）を作成しておく．

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

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
…	…

図 8．$0 \le i \le n-1$となるすべてのiに対する誤り位置判定表の作成

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．

【例】$x^4 + x + 1 \mid x^{15} - 1$

$x^4 + x + 1 \mid x^{15} - 1$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は表 2 のようになる．

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

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

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^i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．

以上に述べたことを生成行列と検査行列という形にまとめてみよう．

【生成行列と検査行列】

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

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

とする．検査行列は，

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

となる．ここで，

表 2.　$x^4+x+1 \mid x^{15}-1$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+x
12	x^3+x^2+x+1
13	x^3+x^2+1
14	x^3+1

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

である.

生成行列は，$G=[{P_c}^{\mathrm{T}} \quad I_{n-m}]$に従って構成する.

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

【例】　$x^4+x+1 \mid x^{15}-1$を満たすx^4+x+1を生成多項式とする(15,11)巡回符号に対する検査行列は次のようになる.

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

生成行列は,

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

となる.

このように$G(x)$が原始多項式のときは,

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．これを，**巡回ハミング符号**と呼ばれる.

【問題】

生成多項式

$$G(x)=x^{16}+x^{12}+x^5+1=(x+1)(x^{15}+x^{14}+x^{13}+x^{12}+x^4+x^3+x^2+x+1)$$

を用いて構成される巡回符号について次のことを示せ.

(1) この符号の重みは偶数である.

(2) この符号の最小距離$d_{\min}$は$d_{\min}\geq 4$を満たすので，1誤り訂正可能，3誤り検出可能である.

(3) この符号のバースト誤り検出能力は16である.