15 BCH 符号 (2)

入学年度		学部	学 科		組		番　号			検	フリガナ	
2	3	B		1							氏 名	

前期の最後に BCH 符号と呼ばれる誤り訂正符号のうち $\mathbf{F}_8$ を用いて誤りを 1 個だけ訂正できるものに付いて詳しくみた．今回は $GF(2^4) = \mathbf{F}_{16}$ を用い，誤り訂正能力が 2 である BCH 符号について，具体例を用いて詳しく見ることにする．$\mathbf{F}_{16}$ の元はすべて β の 3 次以下の多項式として

0 を除く 15 の元は β^k（$0 \leqq k \leqq 14$）と表せる（乗法表示）のであった．もう一度，加法表示と乗法表示の間の対応を付けておく．

1 β^k を β の 4 次以下の多項式で表せ．

$\beta^0 =$　　$\beta^8 =$

$\beta^1 =$　　$\beta^9 =$

$\beta^2 =$　　$\beta^{10} =$

$\beta^3 =$　　$\beta^{11} =$

$\beta^4 =$　　$\beta^{12} =$

$\beta^5 =$　　$\beta^{13} =$

$\beta^6 =$　　$\beta^{14} =$

$\beta^7 =$　　$\beta^{15} =$

これから，2 つの誤りが訂正可能な (15, 7) 型の BCH 符号を詳しく見てみる．(15, 7) の 15 は送受信の bit 数，7 は情報語の bit 数を表しており，情報を 6 次多項式で表し，それを 14 次式に変換して送信する．BCH 符号は**生成多項式**と呼ばれる多項式 $g(x)$ を用いて誤り訂正機能を持たせる．BCH(15, 7) では生成多項式として

$$\begin{aligned} g(x) &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \\ &= x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

を用いる．この $g(x)$ は，$g(\beta) = g(\beta^2) = g(\beta^3) = g(\beta^4) = 0$ をみたすことが確かめられる．

● 符号化

BCH(15, 7) は 7bit の情報語に 8bit の検査 bit を加え 15bit を送受信するので，まず送信したい 7bit の情報語を 6 次の情報多項式 $q(x)$ に変換する．送信多項式 $u(x)$ を作るには，生成多項式 $g(x)$ を用いて次のようにする．

情報多項式：　$q(x) =$ (6 次多項式),
生成多項式：　$g(x) = x^8 + x^7 + x^6 + x^4 + 1$,
送信多項式：　$u(x) = q(x)x^8 +$ ($q(x)x^8$ を $g(x)$ で割った余り)

この定義により，送信される “正しい” 多項式 $u(x)$ は $g(x)$ で割り切れる多項式ということになる．すなわち，$u(x) = g(x)q_0(x)$ の形にかけ，$x = \beta, \ldots, \beta^4$ を代入することにより，

(1)　$$u(\beta) = u(\beta^2) = u(\beta^3) = u(\beta^4) = 0$$

が成り立つことがわかる．$u(x)$ を 0, 1 の列に直したものが**送信語**である．

2 情報語 1100101 を送信したい．

a) 1100101 を情報多項式 $q(x)$ に直せ．

$q(x) =$

b) $q(x)x^8$ を $g(x)$ で割った余りを求めよ．

余り $=$

c) 送信多項式 $u(x)$ を求めよ．

$u(x) = q(x)x^8 +$ (b) の答え)

$=$

d) 送信多項式 $u(x)$ を 0, 1 の列に直した送信語を求めよ．

送信語：

Mathematica を用いて送信語を求めるには次のようにすればよい．

- まず，$g(x)$ を定義する．

```
g[x_] := (x^4 + x + 1) (x^4 + x^3 + x^2 + x + 1)  ⇧+↵
```

- 次に 1010011 を情報多項式 $q(x)$ に直し，Mathematica で定義する．

```
q[x_] :=                                          ⇧+↵
```

- これより送信多項式 $u(x)$ を次の計算式で計算し，それを降べきの順に表示する．

```
u[x_] := Expand[q[x]*x^8] + PolynomialMod[q[x]*x^8, g[x], Modulus -> 2]]
u[x] //TraditionalForm  ⇧+↵
```

- こうして得られた送信多項式 $u(x)$ を 0, 1 の列に直した送信語を求めればよい．これを Mathematica で行うには次のようにすればよい．

```
Table[Coefficient[u[x], x, 14 - k], {k, 0, 14}]
```

● 復号化

さて，ある送信語が通信経路を通って受信されたとする．BCH(15, 7) では，誤りは２つまで訂正できる．そこで，送られて来た**受信語**の誤りは 2 つ以下であると仮定して，それを訂正する方法を示す．

まず，受信語を**受信多項式** $r(x)$ に直す．$r(x)$ と送信多項式 $u(x)$ の差を**誤差多項式** $e(x)$ と呼ぶ．すなわち，$r(x)$ は次のように表せる．

(2)　$$r(x) = u(x) + e(x)$$

【裏に続く】

送信語と受信語は高々 2bit しか相違しないという仮定から，誤差多項式 $e(x)$ は次の形をしている．

$$e(x) = 0 \quad \text{または，} \quad x^k \quad \text{または，} \quad x^k + x^l$$

ここで，(1) により，$u(\beta) = u(\beta^2) = u(\beta^3) = u(\beta^4) = 0$ が成り立つので，(2)式に $\beta, \beta^2, \beta^3, \beta^4$ を代入して，次が成り立つ．

$$r(\beta) = e(\beta), \qquad r(\beta^2) = e(\beta^2), \qquad r(\beta^3) = e(\beta^3), \qquad r(\beta^4) = e(\beta^4).$$

もし受信語に誤りがなければ，これらすべてが 0 になるので，これらは “誤りの一連の症状” を表しており，シンドローム（syndrome）と呼ばれ，s_1, s_2, s_3, s_4 で表される．すなわち，

$$s_1 = r(\beta), \qquad s_2 = r(\beta^2), \qquad s_3 = r(\beta^3), \qquad s_4 = r(\beta^4).$$

さて，いま誤りがちょうど 2 個あると仮定し，$e(x) = x^k + x^l$ であるする．そして，行列式を用いて定義される次の 2 次式 $F(X)$ を考える．

$$F(X) = \begin{vmatrix} 1 & s_1 & s_2 \\ X & s_2 & s_3 \\ X^2 & s_3 & s_4 \end{vmatrix} = \begin{vmatrix} 1 & \beta^k + \beta^l & \beta^{2k} + \beta^{2l} \\ X & \beta^{2k} + \beta^{2l} & \beta^{3k} + \beta^{3l} \\ X^2 & \beta^{3k} + \beta^{3l} & \beta^{4k} + \beta^{4l} \end{vmatrix} \tag{3}$$

前回見たように，2 次方程式 $F(X) = 0$ は β^k と β^l を解に持ち，

$$x^k \text{ の位置が誤り} \quad \Longleftrightarrow \quad F(\beta^k) = 0 \quad \Longleftrightarrow \quad \beta^k \text{ が } F(X) = 0 \text{ の解}$$

が成り立つ．2 次方程式 $F(X) = 0$ は**誤り位置方程式**と呼ばれる．

（誤りがない場合，1 個しかない場合の処理については少し煩雑になるので、ここでは扱わないことにする．）これを具体例で見てみよう．

4 いま，100010111001010 という語を受信したとする．

a) 受信語を受信多項式 $r(x)$ に直し，Mathematica で定義せよ．

```
r[x_] :=
```

⇧+↵

b) シンドローム $s_k = r(\beta^k)$，$k = 1, \ldots, 4$ を Mathematica でそれぞれ計算せよ．

```
s[k_] := PolynomialMod[r[b^k], b^4 + b + 1, Modulus -> 2]
```

⇧+↵

c) 誤り位置方程式 $F(X)$ を定義せよ．

```
F[X_]:=Det[{{1, s[1], s[2]}, {X, s[2], s[3]}, {X^2, s[3], s[4]}}]
```

⇧+↵

d) $F(1), F(\beta), F(\beta^2), \ldots, F(\beta^{14})$ を順に計算し，誤り位置を求めよ．これを自動でやるには，次のようにすればよい．

```
Table[If[PolynomialMod[F[b^k], b^4 + b + 1, Modulus -> 2] === 0,
  k, Nothing], {k, 0, 14}]
```

⇧+↵

e) 送信多項式 $u(x)$ を求めよ．

f) 情報語を求めよ．

情報語：□□□□□□□

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)