入学年度		学部	学 科		組		番　号			検	フリガナ	
											氏 名	

前回に続き，$GF(2^2) = \mathbf{F}_8$ を用いて 2 個の誤りを訂正できる BCH 符号 BCH(15, 7) について，具体例を用いて詳しく見ることにする．前回に見たように，BCH 符号では「生成多項式」と呼ばれる多項式が重要な役割を果たす．前回扱った BCH(15, 11) では生成多項式は $g(x) = x^4 + x + 1$ であった．

まず，Mathematica を用いて多項式 $x^{15} - 1$ を $\mathbf{F}_2$ 上で因数分解してみる．

```
Factor[x^15 - 1, Modulus -> 2]
```

$x^{15} - 1 =$

ここで BCH(15, 11) の生成多項式を $g(x) = x^4 + x + 1$ が上の因数分解に現れるが，$g(b) = 0$ であることから，因数定理により $g(x)$ は $\mathbf{F}_{16}$ 上では $g(x) = (x - b)(x$ の 2 次式) と因数分解される．実は $g(x)$ はさらに因数分解できる．これを見るために，$g(x)$ が $\mathbf{F}_{16}$ の他の元を代入して 0 になるかを見る．$\mathbf{F}_{16}$ の 0 でない元は $b^k, k = 0, \ldots, 14$ の形に書けるので，$g(b^k)$ を計算すれば良い．これは Mathematica で

```
g[x_] := x^4 + x + 1
Table[PolynomialMod[g[b^k], b^4 + b + 1, Modulus -> 2], {k, 0, 14}]
```

とすればよいが，これではどの k で $g(b^k) = 0$ となったのかわかりにくい．そこで，

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

として $g(b^k) = 0$ となる k のリストを作る．（“=” が 3 回重なることに注意．）

1 a) 上の計算結果を用いて $g(x)$ を因数分解せよ．

$g(x) = (x - b)(x-\quad)(x-\quad)(x-\quad)$

b) 同様にして，$x^4 + x^3 + x^2 + x + 1$ と $x^4 + x^3 + 1$ を因数分解せよ．

$x^4 + x^3 + x^2 + x + 1 = (x-\quad)(x-\quad)(x-\quad)(x-\quad)$

$x^4 + x^3 + 1 = (x-\quad)(x-\quad)(x-\quad)(x-\quad)$

• BCH(15,7)

ここで，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．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，$g(b) = g(b^2) = g(b^3) = g(b^4) = 0$ をみたす．

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)

2 情報語 1010011 を送信したい．Mathematica を用いて送信語を求めよ．

a) まず，$g(x)$ を定義する．

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

1010011 を情報多項式 $q(x)$ に直し，Mathematica で定義せよ．

```
q[x_] :=
```

b) これより送信多項式 $u(x)$ を次の計算式で計算し，その結果をその下に転記せよ．

```
u[x_] := Expand[q[x]*x^8] + PolynomialMod[q[x]*x^8,{g[x],2}]
u[x] //TraditionalForm
```

$u(x) =$

c) 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：

さて，ある送信語が通信経路を通って受信されたとする．誤りは2つまであると仮定して，この受信語の誤りを訂正したい．まず，受信語を受信多項式 $r(x)$ に直す．$r(x)$ と送信多項式 $u(x)$ の差は誤差多項式 $e(x)$ とよばれる．すなわち，

$$r(x) = u(x) + e(x)$$

と書ける．いま，送信語と受信語は高々 2 bit しか相違しないという仮定から，誤差多項式 $e(x)$ は次のような形をしているはずである．

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

【裏に続く】

ここで，$u(x)$ は $g(x)$ で割りきれるから，$u(b) = u(b^2) = u(b^3) = u(b^4) = 0$ が成り立つので，上の式に b, b^2, b^3, b^4 を代入して，次が成り立つ．

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

これらすべてが 0 ならば誤りはないので，これらは誤りの特徴を表すと考えられる．そのため，これらはシンドロームと呼ばれ，

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

と名付けらる．

さて，$e(x) = x^i + x^j$ であるとして，すなわち，誤りがちょうど 2 個あると仮定して，誤り位置方程式と呼ばれる 2 次方程式を

$$F(X) = (X - b^i)(X - b^j) = 0$$

と定義する．（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．）　誤り位置方程式は

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

という性質を持つ．$F(X)$ を展開して整理とき

$$F(X) = X^2 + t_1 X + t_2$$

と書けたとすると，$s_k = b^{ki} + b^{kj}$ と $t_1 = -b^i - b^j, t_2 = b^i b^j$ の間には，解と係数の関係の拡張として，次の関係が成り立つ．

$$\begin{cases} s_1 t_2 + s_2 t_1 = -s_3 \\ s_2 t_2 + s_3 t_2 = -s_4 \end{cases} \qquad \begin{pmatrix} s_1 & s_2 \\ s_2 & s_3 \end{pmatrix} \begin{pmatrix} t_2 \\ t_1 \end{pmatrix} = - \begin{pmatrix} s_3 \\ s_4 \end{pmatrix}$$

（右は左の連立一次方程式を「行列」を用いて表示したもの．） Mathematica で，次のようにして連立一次方程式を解くと，$\begin{pmatrix} t_2 \\ t_1 \end{pmatrix} = \begin{pmatrix} b^i b^j \\ -b^i -]b^j \end{pmatrix}$ が解として得られるので，これを見てみよう．

```
s[k_] :=b^(k*i) + b^(k*j)
```

```
LinearSolve[{{s[1], s[2]}, {s[2], s[3]}}, -{s[3], s[4]}] //MatrixForm
```

これより，$F(X) = X^2 + t_1 X + t_2$ が得られるので，この 2 次方程式の解を求め，それらを b^k の形に表せば誤り位置がわかる．これを具体例で見てみよう．

3 いま，100110111000010 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 $s_k = r(b^k)$，$k = 1, \ldots, 4$ 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

```
t[k_]:=LinearSolve[{{s[1], s[2]}, {s[2], s[3]}}, -{s[3], s[4]}][[3-k,1]]
```

```
F[X_]:=X + t[1]*X + t[2]
```

d) $F(1), F(b), F(b^2), \ldots, F(b^{14})$ を順に計算し，誤り位置を求めたい．これを自動でやるには，表でやった因数分解と同様に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) 誤り位置を求めよ．

f) 送信多項式 $u(x)$ を求めよ．

g) 情報語を求めよ．

情報語：

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)