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

前回に引き続き，$GF(2^2) = \mathbf{F}_8$ 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のであった． 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 $g(x)$ について， $g(b) = g(b^2) = g(b^3) = g(b^4) = 0$ が成り立つ（b は $b^4 + b + 1 = 0$ をみたす “虚数”）．

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． 7bit の情報語を送信するには，まずそれをを 6 次の情報多項式 $q(x)$ に変換，次のようにして送信多項式 $u(x)$ を作るのであった．

情報多項式： $q(x) = (6\text{ 次多項式})$,

生成多項式： $g(x) = x^8 + x^7 + x^6 + x^4 + 1$,

送信多項式： $u(x) = q(x)x^8 + \big(q(x)x^8 \text{ を } g(x) \text{ で割った余り}\big)$

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．

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

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

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

と書く．誤りを訂正はこの t_1, t_2 を求めればよいことになる．そのために「シンドローム」と呼ばれる，誤りの特徴を表す数を次のように定義する．

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

$u(x)$ は $g(x)$ で割りきれるから，送信多項式 $u(x)$ に b, b^2, b^3, b^4 を代入するとすべて 0 になるので，受信多項式 $r(x)$ も誤りがなければシンドロームはすべて 0 になるはずである．

さて，シンドローム s_1, s_2, s_3, s_4 から t_1, t_2 を求めるには，連立 1 次方程式を解けばよいことが知られている．連立 1 次方程式 $\begin{cases} ax + by = p \\ cx + dy = q \end{cases}$ は線形代数の理論では「行列」を用いてい

$$\begin{pmatrix} a & b \\ c & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}$$

と表される． Mathematica ではこれを次のコマンドで解くことができる．（Mathematica で行列を入力するには，「パレット」メニューの「基本数学アシスタント」の項目などからできる．）

LinearSolve$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} p \\ q \end{pmatrix}\right]$ **//MatrixForm** ⇧+↵

1 連立 1 次方程式 $\begin{cases} 2x - y = 1 \\ x + 3y = 2 \end{cases}$ をまず手計算で解き，それを Mathematica で解いて答え合わせせよ．

シンドローム $s_k = b^{ki} + b^{kj}$ と誤差方程式の係数 $t_1 = -b^i - b^j, t_2 = b^i b^j$ 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ことが知られている．

$$\begin{cases} s_1 t_2 + s_2 t_1 = -s_3 \\ s_2 t_2 + s_3 t_2 = -s_4 \end{cases} \qquad \begin{pmatrix} s_1 & s_2 \\ s_2 & s_3 \end{pmatrix} \begin{pmatrix} t_2 \\ t_1 \end{pmatrix} = \begin{pmatrix} -s_3 \\ -s_4 \end{pmatrix} \tag{1}$$

2 Mathematica で，次のようにして連立一次方程式 $\begin{pmatrix} s_1 & s_2 \\ s_2 & s_3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -s_3 \\ -s_4 \end{pmatrix}$ を解いてみよ．

```
s[k_] :=b^(k*i) + b^(k*j)
```
⇧+↵

LinearSolve$\left[\begin{pmatrix} \mathtt{s[1]} & \mathtt{s[2]} \\ \mathtt{s[2]} & \mathtt{s[3]} \end{pmatrix}, \begin{pmatrix} -\mathtt{s[3]} \\ -\mathtt{s[4]} \end{pmatrix}\right]$ **//MatrixForm** ⇧+↵

Mathematica による答えは $\begin{pmatrix} b^i b^j \\ -b^i - b^j \end{pmatrix}$ となるはずで，これより， $t_2 = b^i b^j$， $t_1 = -b^i - b^j$ が (1) の方程式をみたすことが確かめられる．

これより， $F(X) = X^2 + t_1 X + t_2$ がシンドローム $s_1, \ldots, s_4$ から上の方法で求められ，さらに，この 2 次方程式の解を求めることにより，誤り位置がわかるという道筋である．これを具体例で見てみよう．

【裏に続く】

3 いま， 110010110110111 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 でそれぞれ定義せよ.

```
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^2 + 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，前回の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)