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

前回は $GF(2^2) = \mathbf{F}_8$ を用いて 1 個の誤りを訂正できる BCH 符号 BCH(7, 4) について見た．今回はさらに複雑な数の体系 $GF(2^4) = \mathbf{F}_{16}$ 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．次第に手計算では手に負えなくなってくるので， Mathematica も利用することにする．

$GF(2^4) = \mathbf{F}_{16}$ は $GF(2) = \mathbf{F}_2$ に $b^4 + b + 1 = 0$ をみたす元 b を加えて得られる数の体系であった．$GF(2^4)$ の元はすべて b の 3 次以下の多項式として表される（加法表示）． b の多項式で表された元は，それを $b^4 + b + 1$ で割った余りと等しい．それを Mathematica で求めるには， “PolynomialMod” というコマンドを用いて次のようにすればよい．

```
PolynomialMod[（b の多項式）, b^4 + b + 1, Modulus -> 2]
```

ここで， “Modulus -> 2” は係数が $\mathbf{F}_2$ の元であること示す．

0 を除く 15 の元は b^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．

$b^0 =$　　$b^8 =$
$b^1 =$　　$b^9 =$
$b^2 =$　　$b^{10} =$
$b^3 =$　　$b^{11} =$
$b^4 =$　　$b^{12} =$
$b^5 =$　　$b^{13} =$
$b^6 =$　　$b^{14} =$
$b^7 =$　　$b^{15} =$

Mathematica でこの表を作るには次のようにすればよい

```
Table[{b^k, "=", PolynomialMod[b^k, b^4 + b + 1, Modulus -> 2]},
  {k, 0, 15}] // TableForm
```

• BCH(15,11)

まず， 1 つの誤りが訂正可能な (15, 11) 型の BCH 符号を見てみる． (15, 11) の 15 は送受信の bit 数，11 は情報語の bit 数を表しており，前回扱った BCH(7, 4) の単純な拡張である．

前回に見たように， BCH 符号は「生成多項式」と呼ばれる多項式を用いて構成される． BCH(7, 4) では $g(x) = x^3 + x + 1$ が用いられたが， BCH(15, 11) では４次の既約多項式 $g(x) = x^4 + x + 1$ を用いる．すぐにわかるように， $g(b) = b^4 + b + 1 = 0$ である．

前回と同様に送りたい情報語を 10 次の情報多項式に変換し，生成多項式 $g(x)$ を用いて，送信多項式 $u(x)$ を前と同様に作る．こうして作られた $u(x)$ は b を代入すると 0 になることに注意する．

情報多項式： $q(x) =$ (10 次多項式),
生成多項式： $g(x) = x^4 + x + 1$,
送信多項式： $u(x) = q(x)x^4 +$ ($q(x)x^4$ を $g(x)$ で割った余り)

1 BCH(15, 11) を用いて情報語 10100111001 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
```

b) 10100111001 を情報多項式 $q(x)$ に直し， Mathematica で定義せよ．

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

c) これより送信多項式 $u(x)$ を次の計算式で計算せよ．

```
u[x_] := Expand[q[x]*x^4] + PolynomialMod[q[x]*x^4,g[x],Modulus->2]
u[x]//TraditionalForm
```

$u(x) =$

d) 送信多項式を 0, 1 の列に直した送信語を求めよ．

2 BCH(15, 11) で 101101101110010 という語を受信したとする．誤りは高々 1 個であると仮定して送信語を求めよう．

a) 受信語 101101101110010 を受信多項式 $r(x)$ に直し， Mathematica で定義せよ．

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

送信多項式 $u(x)$ （未知）は受信多項式 $r(x)$ に誤差多項式 $e(x)$ を加えたものであった．すなわち

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

誤りは高々 1 個であるという仮定より， $e(x)$ は 0 または x^j とい形である．ここで， $u(b) = 0$ であるという性質（$u(x)$ が $g(x)$ で割りきれるという性質と同値）を用いると

$$r(b) = u(b) + e(b) = 0 + e(b) = 0 \text{ または } b^j$$

を得る．そこで $s = r(b)$ とおいて s をシンドロームと呼ぶのであった．

【裏に続く】

b) シンドローム $s = r(b)$ を Mathematica を用いて次のように計算せよ.

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

$s =$

c) シンドローム s を $s = b^j$ の形に表し，誤り位置を求めよ.

d) 情報語を求めよ.

3 前ページの問題１ d) で求めた送信語を一カ所（1bit）だけ変えたものを受信語とし，その誤りを訂正できるか試してみよ．二カ所変更（改竄?）した場合はどうなるか.

次に， 2 つの誤りが訂正可能な $(15, 7)$ 型の BCH 符号について見てみる． BCH$(15, 7)$ の生成多項式を定義するために，まず $\mathbf{F}_2$ 上の 4 次の既約多項式について詳しく調べる.

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

```
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，

```
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 をもとめる． （“=” が 3 回重なることに注意．）

4 これを用いて $g(x)$ を因数分解せよ.

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

5 残りの 2 つの４次既約多項式を $\mathbf{F}_{16}$ 上で因数分解せよ.

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)