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

前回は 1 個の誤りを訂正できるハミング符号 $H(7,4)$ について詳しくみた．$H(7,4)$ では，長さ 4 の情報 bit に長さ 3 の検査 bit を付け加えて長さ 7 の符号語として送信する．このとき，符号語は $\mathbf{F}_2=\{0,1\}$ をスカラーとする 7 次元のベクトルとして捉えられる．符号語全体の集合は，2 つの符号語間のハミング距離が 3 以上となるように 7 次元ベクトル空間のなかに等間隔で散りばめられており，受信した語に最も近い符号語が送信されたものであると推定することにより誤りを訂正する．

今回は，BCH 符号と呼ばれる別の誤り訂正符号の仕組みについて詳しくみる．BCH 符号は，実際に衛星通信や移動通信に用いられる実用性の高い符号である．BCH 符号では情報のブロックの長さや誤り訂正能力を目的に応じてカスタマイズできる．

ハミング符号で用いられた $\mathbf{F}_2$ の元を成分とするベクトルを，BCH 符号では $\mathbf{F}_2$ 係数例えば，1011011 という 7 bit のデータは，左端が最高次 6 次の係数，右端が定数項として，

$$\begin{aligned}1101001 \quad\longmapsto\quad & 1\cdot x^6+1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+0\cdot x+1\\ & =x^6+x^5+x^3+1\end{aligned}$$

というように 6 次の多項式で表される．

1 1100101 を多項式として表せ．

有限体 $\mathbf{F}_{2^q}$ を利用する BCH 符号では，(2^q-1)bit の情報を (2^q-2) 次多項式と捉え，そこに送りたいデータ（**情報語**）と誤り訂正用のデータ（**検査語**）を詰め込んだ**符号語**として送受信する．ここでは $\mathbf{F}_8$ を用いた $(7,4)$ 型と呼ばれる最も簡単な BCH 符号について，具体例を用いて詳しく見ることにする．実は，この $\mathbf{F}_8$ を用いた BCH 符号は前回のハミング符号と全く同値なものになるのであるが，誤り訂正の仕組みには有限体の性質が用いらる．$(7,4)$ の 7 は符号語の bit 数，4 は情報語の bit 数を表していて，長さ 7 の符号語を 6 次多項式と見做す．

$\mathbf{F}_8$ は $\mathbf{F}_2$ に $\alpha^3+\alpha+1=0$ をみたす数 α を加えて得られる数の体系であった．$\mathbf{F}_8$ の元はすべて α の 2 次以下の多項式として表され（**加法表示**），0 を除く 7 個の元は α^k（$0\leqq k\leqq 6$）と表せる（**乗法表示**）のであった．まず，加法表示と乗法表示の間の対応を復習しておく．

$\alpha^0=$　　$\alpha^4=$

$\alpha^1=$　　$\alpha^5=$

$\alpha^2=$　　$\alpha^6=$

$\alpha^3=$　　$\alpha^7=$

Mathematica でこの計算を行うには，例えば次のようにすればよい．

```
PolynomialMod[α^5, α^3 + α + 1, Modulus -> 2]  ⇧+↵
```

2 Mathmatica のコマンド **Table** を用いて上の表を作れ．

$(7,4)$ 型 BCH 符号の基本は，6 次多項式 $f(x)$ に対応する長さ 7 の語が符号語であるための必要十分条件が，$f(\alpha)=0$ となることである．これは，すなわち $f(x)$ が $g(x)=x^3+x+1$ で割り切れることに他ならない．この $g(x)$ は「生成多項式」とも呼ばれる．

情報語は次の手順によって符号語に直して送信される．

(1) 送りたい 4bit の情報語を 3 次の情報多項式 $q(x)$ に変換する．

(2) 生成多項式 $g(x)$ を用いて，符号多項式 $u(x)$ を次のように作る．

$$u(x)=q(x)x^3+\big(q(x)x^3 \text{ を } g(x) \text{ で割った余り}\big)$$

このように $u(x)$ を定義すれば，$u(x)$ を $g(x)$ で割った余りが $q(x)x^3$ を $g(x)$ で割った余りの 2 倍になるが，$\mathbf{F}_2$ の演算では $2=0$ なので，$u(x)$ は $g(x)$ で割り切れることになる．したがって，$u(x)=g(x)h(x)$ の形に書けるから，

$$u(x)=g(x)h(x) \quad\Longrightarrow\quad u(\alpha)=g(\alpha)h(\alpha)=0\cdot h(\alpha)=0$$

3 情報語 1101 を送信したい．

a) 1101 を情報多項式 $q(x)$ に直せ．

$q(x)=$

b) $q(x)x^3$ を $g(x)$ で割った余りを求めよ．

$q(x)x^3$ を $g(x)$ で割った余り $=$

c) これより符号多項式 $u(x)$ を作れ．

$u(x)=$

d) 符号多項式を 0, 1 の列に直した符号語を求めよ．

符号語 $=$

Mathematica を用いれば，

```
q[x_]:= ( a) の答え )  ⇧+↵
Expand[q[x] x^{3} + PolynomialMod[q[x],x^3 + x + 1,Modulus -> 2],
  Modulus-> 2]  ⇧+↵
```

4 Mathematica を用いて，16 個ある長さ 4 の情報語をすべて符号化せよ．

【裏に続く】

受信したデータの誤りを訂正して必要な情報を取り出すことを**復号**という．BCH 符号では，復号は次のようになされる．

今，符号語が通信経路を通って受信されたとき，まずそのデータ（受信語）を受信多項式 $r(x)$ に変換する．通信経路で誤りが起こったとするとそれは $r(x)$ と $u(x)$ の差に他ならない．そこで，

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

と置く．この $e(x)$ は**誤差多項式**と呼ばれる．ここで，符号語と受信語は高々 1bit しか相違していないと仮定する．すると，

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

という形をしているはずである．符号多項式 $u(x)$ に α を代入すると $u(\alpha) = 0$ となるのであったから，受信多項式 $r(x)$ に α を代入すると

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

が成り立つ．これより，$r(\alpha)$ を計算することにより誤りがあるかないかが判定できるので，$r(\alpha)$ を「シンドローム」と呼び，s で表す．

シンドローム $s = e(\alpha)$ は，0 または α^k に等しく，

- $s = 0$ なら誤りなし，
- $s \neq 0$ なら，s を情報表示し $s = \alpha^k$ の形にすると，$r(x)$ と $u(x)$ は k 次の項が異なることを示す．すなわち，受信語の右から $k+1$ 番目の bit に誤りがあったことがわかる．

5 いま，$(7,4)$ 型の BCH 符号で 1011011 という語を受信したとする．誤りは高々 1 個であるという仮定の下に符号語を求めたい．

a) 受信多項式 $r(x)$ を求めよ．

$r(x) =$

b) シンドローム $s = r(\alpha)$ を計算せよ．

$s =$

c) シンドローム s を $s = \alpha^k$ の形に表し，誤り位置を求めよ．（最初に求めた，加法表示と乗法表示の対照表を利用するとよい．）

d) 情報語を求めよ．

6 $(7,4)$ 型の BCH 符号で 0101001 という語を受信したとする．誤りは高々 1 個であるという仮定の下に情報語を求めよ．

7 長さ 4 の情報語を (7,4) 型 BCH 符号で符号化したものは，前回のハミング符号による符号化と一致することを示せ．

— ❧❧❧ —

QR コードの中にも BCH 符号が一部使われており，5 bit の情報語を間違いなく送るために 10 bit の検査語を加えて 15 bit とし，3 つまでの誤りを訂正出来るようにしたものである．このため，16 個の元を持つ数の体系 $GF(2^4) = \mathbf{F}_{16}$ を用いる．符号化は，上記と同様に簡単にできるが，復号の仕組みを理解するには連立 1 次方程式の理論（線形代数）が必須となる．これについては，後期のお楽しみ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)