これまでに，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 $\mathbb{F}_2 = \{0,1\}$ 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．

ハミング符号では，1011011 という 7 bit のデータは $\mathbb{F}_2$ の元を成分とするベクトル $(1,0,1,1,0,1,1)$ で表されたが，BCH 符号ではこれを $\mathbb{F}_2$ 係数の多項式で表す．例えば，1011011 は，左端が最高次 6 次の係数，右端が定数項として，

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

というように 6 次の多項式で表される．

1 前につくったハミング符号の符号語をそれぞれ多項式に直せ．

10 進法	2 進法	符号語	符号多項式
0	0000	0000000	0
1	0001	0001011	$x^3 + x + 1$
2	0010	0010110	
3	0011	0011101	
4	0100	0100111	
5	0101	0101100	
6	0110	0110001	
7	0111	0111010	
8	1000	1000101	
9	1001	1001110	
10	1010	1010011	
11	1011	1011000	
12	1100	1100010	
13	1101	1101001	$x^6 + x^5 + x^3 + 1$
14	1110	1110100	
15	1111	1111111	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

入学年度	学部	学科	組	番号	検	フリガナ
	B	1				氏名

$\mathbb{F}_8$ を用いた $(7,4)$ 型と呼ばれる最も簡単な BCH 符号では，4bit の情報を 3 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 7bit の**符号語**を作る．これを具体例を用いて詳しく見ることにする．基本的考え方は，「長さ 7 の語が符号語であるための必要十分条件は，それを 6 次多項式 $f(x)$ として表したとき，$f(\alpha) = 0$ となることである.」と定めることにある．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．実際には，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．

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

例えば，$q(x) = x + 1$ ならば，$q(x)x^3 = x^4 + x^3$ として，これを $x^3 + x + 1$ で割った余りを求めると，$x^2 + 1$ となるので，$u(x) = x^4 + x^3 + x^2 + 1$ とする．あるいは，$q(\alpha)\alpha^3 = \alpha^4 + \alpha^3$ として，$\alpha^3 = \alpha + 1$ を用いて $q(\alpha)\alpha^3 = \alpha^4 + \alpha^3$ を α の 2 次以下の式に直し，α を x で置き換えると考えてもよい．

2 次の表を完成させ，先に作った表と比較せよ．

10 進法	情報語	情報多項式	符号多項式
0	0000	0	0
1	0001	1	
2	0010	x	$x^4 + x^2 + x$
3	0011	$x + 1$	
4	0100	x^2	
5	0101	$x^2 + 1$	
6	0110	$x^2 + x$	
7	0111	$x^2 + x + 1$	
8	1000	x^3	
9	1001	$x^3 + 1$	
10	1010	$x^3 + x$	
11	1011	$x^3 + x + 1$	
12	1100	$x^3 + x^2$	
13	1101	$x^3 + x^2 + 1$	
14	1110	$x^3 + x^2 + x$	
15	1111	$x^3 + x^2 + x + 1$	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

【裏に続く】

● 符号化

おもての符号多項式の表を Mathematica™ で作ってみよう．

例えば，5 を 4 桁の 2 進法で表すと 0101 となるが，これを（Mathematica™ の）ベクトル $\{0,1,0,1\}$ に直すには

```
IntegerDigits[5, 2, 4]  ⇧+↵
```

とすればよい．さらにこのベクトルと $\{x^3, x^2, x, 1\}$ との内積をとることにより，

$$0\cdot x^3 + 1\cdot x^2 + 0\cdot x + 1 = x^2 + 1$$

という答を得るには次のようにすればよい．

```
IntegerDigits[5, 2, 4].{x^3, x^2, x, 1}  ⇧+↵
```

（Mathematica™ での表示は答は $1 + x^2$ と昇べきの順になる．）

情報語から符号語を作る方法は，多項式 $q(x)$ に対して $u(x)$ を

$$u(x) = (q(x))x^3 + \big(\, q(x)x^3 \text{ を } x^3 + x + 1 \text{ で割った余り} \,\big)$$

と定義するのであった．Mathemtica™ を用いて上で得た $1 + x^2$ から符号語を作るには，

```
Expand[ (x^2 + 1)*x^3
   + PolynomialMod[(x^2 + 1)*x^3, x^3 + x + 1, Modulus -> 2] ]
```

とすればよい．$x^2 + x^3 + x^5$ という答えが得られるはずである．ここまでの計算を自動化して表にするには，まず上の操作を行う関数 **u** を定義し，それを **Table** を用いて表にすればよい．

```
u[n_] := Expand[
  IntegerDigits[n, 2, 4].{x^3, x^2, x, 1}*x^3
   + PolynomialMod[IntegerDigits[n, 2, 4].{x^3, x^2, x, 1}*x^3,
    x^3 + x + 1, Modulus -> 2]]

Table[u[n], {n, 0, 15}] // TableForm
```

さらに，x の 6 次以下の多項式を 7 次元ベクトルに変えて表示するには次のようにすればよい．

```
Table[Reverse[CoefficientList[u[n], x, 7]], {n, 0, 15}] // TableForm
```

● 復号

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．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)