前回，BCH 符号と呼ばれる誤り訂正符号のうち $\mathbb{F}_8$ を用いて誤りを 1 個だけ訂正できる $(7, 4)$ 型と，$\mathbb{F}_{16}$ を用いてやはり 1 個だけ訂正可能な $(15, 11)$ 型を扱った．今回は，$\mathbb{F}_{16}$ を用い，誤り訂正能力が 2 である $(15, 7)$ 型の BCH 符号について詳しく見ることにする．

有限体 $\mathbb{F}_{2^q}$ を利用する BCH 符号では，$(2^q - 1)$ bit の語を $(2^q - 2)$ 次多項式とみなし，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．BCH(15, 7) は $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ を用い，$15 = (2^4 - 1)$ bit の語を送受信する．そして，7 は情報語の bit 数を表し，7 bit の語をを 6 次多項式で表し，それを 14 次式に変換して送信する．BCH 符号は**生成多項式**と呼ばれる多項式 $g(x)$ を用いて誤り訂正機能を持たせが，$g(x)$ の次数により，この情報語の bit 数を決定する．

$\mathbb{F}_{16}$ の元は $\mathbb{F}_2 = \{0, 1\}$ に $\beta^4 + \beta + 1 = 0$ をみたす “虚数” β を付け加えることにより得られ，すべて β の 3 次以下の多項式として表せる（**加法表示**）．また，0 を除く 15 の元は β^k（$0 \leqq k \leqq 14$）と表せる（**乗法表示**）のであった．加法表示と乗法表示の間の対応が重要になるので，ここで復習しておく．

1 β^k を β の 4 次以下の多項式で表せ．

$\beta^0 =$ $\beta^8 =$

$\beta^1 =$ $\beta^9 =$

$\beta^2 =$ $\beta^{10} =$

$\beta^3 =$ $\beta^{11} =$

$\beta^4 =$ $\beta^{12} =$

$\beta^5 =$ $\beta^{13} =$

$\beta^6 =$ $\beta^{14} =$

$\beta^7 =$ $\beta^{15} =$

2 $f(x) \in \mathbb{F}_2[x]$ を $\mathbb{F}_2$ 係数の多項式とする．$x = a \in \mathbb{F}_{16}$ が $f(x) = 0$ の解であれば，$x = a^2$ も $f(x) = 0$ の解であることを示せ．

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

3 $\mathbb{F}_2$ 係数の 4 次の既約多項式は

$$g_1(x) = x^4 + x + 1, \quad g_2(x) = x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1$$

の 3 つであった．これを $\mathbb{F}_{16}$ 上で因数分解し，$(x - \beta^{k_1}) \cdots (x - \beta^{k_4})$ の形に表せ．

- **BCH 符号** $(15, 7)$

まず，$g(x)$ を次のように定義し，**生成多項式**と呼ぶ．

$$g(x) = g_1(x)g_2(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

$g_1(x)$，$g_2(x)$ の因数分解を考慮すると，

$$g(\beta) = g(\beta^2) = g(\beta^3) = g(\beta^4) = 0$$

が成り立つことがわかる．

4 $g(x)$ を展開せよ．

まず 7bit の情報語を 6 次の情報多項式 $q(x)$ に変換し，それを生成多項式 $g(x)$ を用いて次のようにして 14 次の送信多項式 $u(x)$ を作る．

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

$u(x)$ の構成方法より，$u(x)$ は $g(x)$ で割りきれるので，次が成り立つ．

$$u(\beta) = u(\beta^2) = u(\beta^3) = u(\beta^4) = 0$$

【裏に続く】

さて，$u(x)$ を何らかの伝送経路を通じて送信し，受信者が受信多項式 $r(x)$ それを受け取る．伝送中に誤りが生じなければ $r(x)$ は $u(x)$ と一致するが，一般には誤りが生じるので，$u(x)$ と $r(x)$ の差を誤差多項式 $e(x)$ とおき，

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

と表す．いま，受信多項式 $r(x)$ はちょうど 2 つの誤りを含むと仮定する．すると，

$$e(x) = x^k + x^l, \quad 0 \leqq k < l \leqq 15$$

と書ける．このとき，$u(\beta) = 0$ だから

$$r(\beta) = u(\beta) + e(\beta) = 0 + \beta^k + \beta^l = \beta^k + \beta^l$$

となる．さらに $x = \beta^2$ を $r(x)$ に代入すると

$$r(\beta^2) = u(\beta^2) + e(\beta^2) = 0 + (\beta^2)^k + (\beta^2)^l = \beta^{2k} + \beta^{2l}$$

となる．$x = \beta^3$，$x = \beta^4$ についても同様．ただし，実際に $r(\beta)$ を計算しようとすると，結果は加法表示として 3 次以下の β の多項式として現れ，それを $\beta^k + \beta^l$ の形に表すのは容易ではない．

そこで，$e(x) = x^k + x^l$ の k, l を求めるために，**シンドローム** s_1, s_2, s_3, s_4 を

$$\begin{aligned} s_1 &= r(\beta^1) = \beta^k + \beta^l, \\ s_2 &= r(\beta^2) = \beta^{2k} + \beta^{2l}, \\ s_3 &= r(\beta^3) = \beta^{3k} + \beta^{3l}, \\ s_4 &= r(\beta^4) = \beta^{4k} + \beta^{4l} \end{aligned}$$

と定義する．これらを用いて k, l を求める．

5 受信多項式 $r(x)$ がちょうど 2 つの誤りを含むとし $e(x) = x^k + x^l, (0 \leqq k < l \leqq 15)$ とするとき，

$$\begin{vmatrix} 1 & X & X^2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} = 0$$

で定義される X の 2 次方程式は β^k と β^l を解に持つことを示せ．

6 受信多項式 $r(x)$ が 1 つしか誤りを含まないとし，$e(x) = x^k, (0 \leqq k \leqq 15)$ とする．

a) 行列式 $\begin{vmatrix} 1 & X & X^2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} = 0$ は常に 0 になることを示せ．

b) $\begin{vmatrix} 1 & X \\ s_1 & s_2 \end{vmatrix} = 0$ で定義される 1 次方程式は β^k を解に持つことを示せ．

7 BCH(15, 7) の復号の手順について考えてみよ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)