16 ❦ 行列式と BCH 符号 (15, 7)

２０２５年度　総合教育科目演習 I（水曜２限）

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

有限体 $\mathbb{F}_{2^q}$ 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．前期に 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 $(7,4)$ 型ものに付いて詳しくみた．ここでは，$\mathbb{F}_{16}$ 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．$(15,7)$ の 15 は送受信の bit 数，7 は情報語の bit 数を表しており，情報を 6 次多項式で表し，それを 14 次式に変換して送信する．

$\mathbb{F}_{16}$ 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．

[2] β^k を β の 4 次以下の多項式で表せ．

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

[3] いま，$\mathbb{F}_2$ 係数の多項式 $g(x)$ を次のように定義する．

$$g(x)=g_1(x)g_2(x),\quad \text{ただし}\quad g_1(x)=x^4+x+1,\quad g_2(x)=x^4+x^3+x^2+x+1$$

一般に $\mathbb{F}_2$ 係数の式の計算では $(a+b)^2=a^2+b^2$ が成り立つので，$x=\alpha$ が方程式 $f(x)=0$ の解であれば，$x=\alpha^2$ も解になることが示される．

a) $g_1(\beta)=g_1(\beta^2)=g_1(\beta^4)=0$ であることを示し，$g_1(x)$ を因数分解せよ．

b) 同様に，$g_2(\beta^3)=g_2(\beta^6)=g_2(\beta^{12})=g_2(\beta^9)=0$ であることを示し，$g_2(x)$ を因数分解せよ．

• BCH 符号

BCH(15, 7) では，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

$$g(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)=x^8+x^7+x^6+x^4+1$$

を用いて次のようにして 14 次の送信多項式 $u(x)$ を作る．

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

前問で示したとおり，$g(\beta)=g(\beta^2)=g(\beta^3)=g(\beta^4)=0$ が成り立つが，$u(x)$ 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．

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

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．すなわち

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

と書けたとする．このとき，例えば $x=\beta^2$ 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．ただし，実際に $r(\beta^2)$ を計算しようとすると，結果は加法表示として 14 次以下の β の多項式として現れ，それを $\beta^{2k}+\beta^{2l}$ の形に表すのは容易ではない．そのために，**シンドローム** s_1,s_2,s_3,s_4 を

$$s_1=r(\beta^1),\quad s_2=r(\beta^2),\quad s_3=r(\beta^3)\quad s_4=r(\beta^4)$$

と定義する．これらを用いて k,l を求める．

[4] 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，
$\begin{vmatrix} 1 & s_1 & s_2 \\ x & s_2 & s_3 \\ x^2 & s_3 & s_4 \end{vmatrix}=0$ で定義される 2 次方程式は β^k と β^l を解に持つことを示せ．

$\boxed{5}$ 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 $\begin{vmatrix} 1 & s_1 & s_2 \\ x & s_2 & s_3 \\ x^2 & s_3 & s_4 \end{vmatrix}$ は常に 0 になることを示せ.

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

$\boxed{6}$ 行列式 $\begin{vmatrix} 1 & s_1 & s_2 \\ x & s_2 & s_3 \\ x^2 & s_3 & s_4 \end{vmatrix}$ をサラスの公式を用いて展開し，x について整理せよ.

$\boxed{7}$ BCH(15, 7) の復号の手順について説明せよ.

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)