入学年度		学部	学科		組		番号			検	フリガナ	
		D		1							氏名	

QR コードの一部にはこれまで扱った BCH 符号が使われているのであるが，伝達したいデータを扱う核心部分には **RS 符号**（Reed-Solomon 符号）と呼ばれる BCH 符号をさらに進化させた符号が使われる．RS 符号は密集する誤り (バースト誤り) に対して有効な誤り訂正符号である．

BCH 符号では，0 と 1 の列である情報をブロックに分け，その 1 つ 1 つを 0 と 1 を係数に持つ多項式，すなわち $\mathbb{F}_2[x]$ の元として扱う．RS 符号では，1 つの情報のブロックを細かいブロック分けし，細かいブロックを $\mathbb{F}_{2^q}$ の元とみなし，大きなブロックを $\mathbb{F}_{2^q}[x]$ の元として扱う．例えば，実際の QR コードでは 8bit を 1 つのブロックとし，それを $2^8 = 256$ 個の要素を持つ $\mathbb{F}_{256}$ の元と見做す．一番小さな 1 型の QR コードでは，情報は $\mathbb{F}_{256}$ を係数とする 25 次式一つに詰め込まれている．

ここでは，RS 符号の仕組みが理解しやすいように，もう少し簡単な $\mathbb{F}_{16}$ を係数とする多項式を用いる場合を考察する．

$\mathbb{F}_{16}$ はすでに何度も見たように $\beta^4 + \beta + 1 = 0$ をみたす元 β で生成される．$\mathbb{F}_{16}$ の各要素は乗法表示 β^k $(0 \leqq k \leqq 14)$ と加法表示 $c_3\beta^3 + c_2\beta^2 + c_1\beta + c_0$ の二通りの表示を持つ．それらの間の変換についてはすでに計算されているものとする．

- $RS(15, 9, 7)$

この型の RS 符号では送信語の長さが 15，情報語の長さが 9 であって，2 つの符号の最小距離が $15 - 9 + 1 = 7$ である．従って，送信多項式の次数は 14，情報多項式の次数は 8 であり，$7/2 = 3.5$ だから 3 個の誤りを訂正できる．BCH 符号と同様，ある 0 と 1 の列が符号語であるかどうかは，それに対応する多項式が生成多項式と呼ばれる多項式 $g(x)$ によって割り切れるかどうかで判定される．今の場合，生成多項式は $\mathbb{F}_{16}[x]$ の元で，次数は $14 - 8 = 6$ であり，次のように定義する．

$$\begin{aligned} g(x) &= (x-1)(x-\beta)(x-\beta^2)(x-\beta^3)(x-\beta^4)(x-\beta^5) \\ &= x^6 + \beta^9 x^5 + \beta^{12} x^4 + \beta x^3 + \beta^2 x^2 + \beta^4 x + 1 \end{aligned}$$

この定義により，情報多項式は

$$g(1) = g(\beta) = g(\beta^2) = g(\beta^3) = g(\beta^4) = g(\beta^5) = 0$$

となる．BCH 符号の場合，$g(x) \in \mathbb{F}_2[x]$ でなければならないので、このような性質をもつ多項式の次数はこれより大きくなる．

いま，72bit の情報を 8bit ごとの 9 のブロックにわけ，それを $\mathbb{F}_8$ 係数の 9 次元ベクトルとしたものが

$$\vec{q} = (\beta^{13}, 0, \beta^8, \beta^6, \beta^{10}, \beta^9, \beta^2, 1, \beta^7)$$

であるとする．これを符号多項式 $u(x)$ に直すには

$$u(x) = q(x)x^6 + \big(q(x)x^6 \text{ を } g(x) \text{ で割ったあまり}\big)$$

とする．$u(x)$ は $g(x)$ で割り切れるので，商を $a(x)$ と書くことにすれば，$u(x) = g(x)a(x)$ と書ける．実際に計算し，その係数を並べって $\vec{u}$ を作ると

実際に計算してみると，次のようになる．

$$\vec{u} = (\beta^{13}, 0, \beta^8, \beta^6, \beta^{10}, \beta^9, \beta^2, 1, \beta^7, \beta^3, \beta^{14}, 1, \beta^7, \beta^{11}, \beta)$$

- **復号**

さて，受信語の誤り訂正する方法をみる．いま

$$\vec{r} = (\beta^{13}, 0, \beta^8, \beta^6, \beta^{12}, \beta^9, \beta^2, 1, \beta^7, \beta^4, \beta^{14}, 1, \beta^7, \beta^{12}, \beta) \tag{1}$$

を受信したとしよう．これより，受信多項式 $r(x)$ を

$$\begin{aligned} r(x) = \beta^{13}x^{14} + \beta^8 x^{12} + \beta^6 x^{11} + \beta^{12}x^{10} + \beta^9 x^9 + \beta^2 x^8 + x^7 \\ + \beta^7 x^6 + \beta^4 x^5 + \beta^{14} x^4 + x^3 + \beta^7 x^2 + \beta^{12} x + \beta \end{aligned}$$

をつく r．BCH 符号の場合と同様に $r(x)$ と $u(x)$ との誤差を $e(x)$ とし，$e(x)$ を求める方法を考える．今考えている $RS(15, 9, 7)$ では，誤りは 3 つまで訂正可能なので，$e(x)$ は

$$e(x) = e_i x^i + e_j x^j + e_k x^k, \quad e_i, e_j, e_k \in \mathbb{F}_{16}$$

という形に書ける．ここで，i, j, k は相異なり，e_i, e_j, e_k は 0 である場合も含める．そして，次のようにシンドロームを定義する．

$$s_0 = r(1), \quad s_1 = r(\beta), \quad s_2 = r(\beta^2) \quad s_3 = r(\beta^3), \quad s_4 = r(\beta^4), \quad s_5 = r(\beta^5)$$

$1, \beta, \beta^2, \beta^3, \beta^4, \beta^5$ はすべて $g(x) = 0$ の解であることに注意すると，$u(x) = g(x)a(x)$ と書けることから，

$$u(\beta^m) = g(\beta^m)a(\beta^m) = 0, \quad m = 0, 1, \ldots, 5.$$

が成り立つ．すると，$r(x) = u(x) + e(x)$ だから，

$$r(\beta^m) = e(\beta^m), \quad m = 0, 1, \ldots, 5.$$

であることがわかる．

ここで，BCH 符号の場合に倣って，次の行列式を考える．

$$F(X) = \begin{vmatrix} 1 & X & X^2 & X^3 \\ s_0 & s_1 & s_2 & s_3 \\ s_1 & s_2 & s_3 & s_4 \\ s_2 & s_3 & s_4 & s_5 \end{vmatrix} \tag{2}$$

BCH 符号の場合と同様に，上の行列式を用いて定義される $F(X)$ は

$$F(\beta^i) = F(\beta^j) = F(\beta^k) = 0$$

をみたす．また，誤りが 2 つ以下の場合（e_i, e_j, e_k いずれかが 0 の場合）$F(X)$ は恒等的に 0 になることも示せる．

【裏に続く】

いま，誤りがちょうど 3 つあると仮定すると，

$$F(X) = (X - \beta^i)(X - \beta^j)(X - \beta^k)$$

が成り立ち，$F(1), F(\beta), F(\beta^2), \ldots, F(\beta^{14})$ を順に計算し，0 となる場所が誤り位置となる．

さて，それぞれの位置での誤り（真の値との差） e_i，e_j，e_k を求めるにはどのようにしたらよいだろうか．このとき，

$$e(\beta^0) = s_0, e(\beta^1) = s_1, e(\beta^2) = s_2$$

が成り立つので，次の連立 1 次方程式が得られる．

$$\left\{ \begin{array}{rcrcrcl} e_i & + & e_j & + & e_k & = & s_0 \\ \beta^i e_i & + & \beta^j e_j & + & \beta^k e_k & = & s_1 \\ (\beta^i)^2 e_i & + & (\beta^j)^2 e_j & + & (\beta^k)^2 e_k & = & s_2 \end{array} \right.$$

これを行列で表せば，

$$\begin{pmatrix} s_0 \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ \beta^i & \beta^j & \beta^k \\ \beta^{2i} & \beta^{2j} & \beta^{2k} \end{pmatrix} \begin{pmatrix} e_i \\ e_j \\ e_k \end{pmatrix}$$

と表せるので，e_i, e_j, e_k を求めるには，逆行列を求めて，

$$\begin{pmatrix} e_i \\ e_j \\ e_k \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ \beta^i & \beta^j & \beta^k \\ \beta^{2i} & \beta^{2j} & \beta^{2k} \end{pmatrix}^{-1} \begin{pmatrix} s_0 \\ s_1 \\ s_2 \end{pmatrix}$$

として計算できることがわかるであろう．

1 a) (2) で定義される 3 次多項式は $F(\beta^i) = F(\beta^j) = F(\beta^k) = 0$ を満たすことを証明せよ．

b) $e_k = 0$ であるとき，$F(X) \equiv 0$ であることを証明せよ．

以下の問題では，Mathematica（あるいは他のソフトウェア）を用いてよい．

2 例 (1) について，

a) 誤り位置を特定せよ．

b) e_i，e_j，e_k を求め，送信された情報語を求めよ．

3 $\vec{r} = (\beta^3, \beta^5, \beta^2, \beta, \beta^{11}, \beta^3, \beta^4, 1, \beta^8, \beta^5, \beta^6, \beta^9, \beta^4, \beta^7, \beta^{10})$ を受信したとする．

a) 誤り位置を特定せよ．

b) 情報語を求めよ．.

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)