

入学年度	学部	学科	組	番号	検	フリガナ
2	3	B	1			氏名

QR コードには **RS 符号** (Reed-Solomon 符号) と呼ばれる符号が使われる。これは、BCH 符号をさらに進化させたものであり、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。

数学的モデルとしては、 $GF(2^q) = \mathbf{F}_{2^q}$ の要素を係数とする多項式を送受信すると考える。実際には $GF(2^q)$ の要素を q bit の 0 と 1 の列のブロックとし、そのブロックの列を送受信することにより通信を行う。

QR コードでは 256 個の要素を持つ $GF(2^8) = \mathbf{F}_{256}$ を係数とする多項式を用いる。例えば、一番小さな 1 型の QR コードでは、 $GF(2^8)$ を係数とする 25 次式一つに情報を詰め込んで、これを送受信する。ここでは、その仕組みが理解しやすいように、もう少し簡単な $GF(2^4) = \mathbf{F}_{16}$ を係数とする多項式を用いる場合を考察する。

$GF(2^4)$ 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。 $GF(2^4)$ の各要素は乗法表示 β^k ($0 \leq k \leq 14$) 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 RS 符号では送信ベクトルの次元が 15 であり、情報ベクトルの次元が 9 である。言い換えると、送信多項式の次数は 14、情報多項式の次数は 8 であり、したがって生成多項式の次数は $14 - 8 = 6$ となる。最後の 7 は二つの符号語の最小距離であり、 $7/2 = 3.5$ なので 3 個の誤りを訂正できる。生成多項式は

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

を用いる。いま、9 次元情報ベクトル

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

を送ることを考える。これを符号多項式 $u(x)$ に直すには BCH 符号と同様にして、

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

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、 $u(x) = q(x)a(x)$ と書ける。

1 情報ベクトル \vec{q} を Mathematica を用いて符号化し、送信語を求めたい。

(入力を簡単にするために β の代わりに b を用いることにする。)

a) \vec{q} を情報多項式 $q(x)$ に直し、Mathematica で定義せよ。

$$q[x_] := \quad \uparrow + \downarrow$$

b) $g(x)$ を Mathematica で定義せよ。

$$g[x_] := (x-1)(x-b)(x-b^2)(x-b^3)(x-b^4)(x-b^5) \quad \uparrow + \downarrow$$

c) 送信多項式 $u(x)$ を次のように計算する。

Collect[PolynomialMod[

$$\begin{aligned} & q[x]*x^6 + \text{PolynomialRemainder}[q[x]*x^6, g[x], x, \text{Modulus} \rightarrow 2], \\ & b^4 + b + 1, \text{Modulus} \rightarrow 2], x] \end{aligned}$$

こうして得られた送信多項式 $u(x)$ の係数をすべて乗法表示し、並べてベクトルにしたものが送信語である。送信語 \vec{u} を求めよ。

$$\vec{u} = (\beta^{13}, 0, \beta^8, \quad \quad \quad)$$

• 復号化

次に、受信語の誤り訂正する方法をみる。いま

$$\vec{r} = (\beta^{13}, 0, \beta^8, \beta^6, \beta^{12}, \beta^9, \beta^2, 1, \beta^7, \beta^4, \beta^{14}, 1, \beta^7, \beta^{12}, \beta^5)$$

を受信したとしよう。これより、受信多項式 $r(x)$ を

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

と定義する。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。今の場合、誤りは 3 つまで訂正可能なので、 $e(x)$ は係数を乗法表示して

$$e(x) = e_i x^i + e_j x^j + e_k x^k$$

という形に書ける。まず、次のようにシンドロームを計算する。

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

$1, \beta, \beta^2, \beta^3, \beta^4, \beta^5$ はすべて $g(x) = 0$ の解であることに注意する。すると、 $r(x) = u(x) + e(x)$ だから、

$$r(\beta^k) = e(\beta^k), \quad k = 0, 1, \dots, 5.$$

であることがわかる。

2 a) \vec{r} を情報多項式 $g(x)$ に直し、Mathematica で定義せよ。

$$r[x_] := \quad \uparrow + \downarrow$$

b) シンドロームを次のように定義せよ。

$$s[k_] := \text{PolynomialMod}[r[b^k], b^4 + b + 1, \text{Modulus} \rightarrow 2] \quad \uparrow + \downarrow$$

c) 次の行列式 $S(X) = \begin{vmatrix} 1 & s_0 & s_1 & s_2 \\ X & s_1 & s_2 & s_3 \\ X^2 & s_2 & s_3 & s_4 \\ X^3 & s_3 & s_4 & s_5 \end{vmatrix}$ を Mathematica で計算せよ

```
S[X_] := Det[{{1, s[0], s[1], s[2]},
             {X, s[1], s[2], s[3]},
             {X^2, s[2], s[3], s[4]},
             {X^3, s[3], s[4], s[5]}}
```

d) $S(X) = 0$ の解を $X = \beta^{14}, \beta^{13}, \dots, \beta^2, \beta, 1$ を順次代入することによって求めよ.

```
Table[PolynomialMod[S[b^(14 - k)], b^4 + b + 1, Modulus -> 2],
      {k, 0, 14}]
```

さて、それぞれの位置での誤り（真の値との差）を e_i, e_j, e_k とする。すなわち、 $e(x) = e_i x^i + e^j x^j + e_k x^k$ であるとする。このとき、 e_i, e_j, e_k は次の連立1次方程式をみたす。

$$\begin{cases} e_i + e_j + e_k = s_0 \\ \beta^i e_i + \beta^j e_j + \beta^k e_k = s_1 \\ (\beta^i)^2 e_i + (\beta^j)^2 e_j + (\beta^k)^2 e_k = s_2 \end{cases}$$

Mathematica でこれを求めることは、少々面倒になるので、ここでは割愛する。

e) [チャレンジ問題] 上の例で、 e_i, e_j, e_k を求め、送信された情報多項式を推定せよ。

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) [チャレンジ問題] 情報多項式を推定せよ。