符号理論･暗号理論

- No.10 RS符号 -

渡辺 裕

Coding Theory / Cryptography

- No.10 RS Code -

Hiroshi Watanabe

誤り訂正符号

- RS符号 (Reed-Solomon code)
  - 符号化
    - アービング･リード, ギュスタブ･ソロモン (1960)
  - 復号
    - バーレカンプ, マッシイ (1969)
  - 応用
    - 地上波テレビ放送, 衛星通信, ADSL, CD, DVD, QRコード

Error Correction Code

- RS code (Reed-Solomon code)
  - Coding
    - Irving S. Reed, Gustave Solomon (1960)
  - Decoding
    - Erwyn Berlekamp, James Massey (1969)
  - Application
    - Terrestrial TV broadcasting, Satellite Communication, ADSL, CD, DVD, QR-code

RS符号

- BCH符号は2元[0,1]符号であるが，RS符号は多元符号[0,1,2,...]
- BCH符号がGF(2)の集合上で通報多項式P(x)および生成多項式G(x)を定義するのに対して，RS符号では最初から拡大体GF(2^m)上で通報多項式P(x)および生成多項式G(x)を定義
- 多くの実装では，GF(2^8) (1バイト単位)
- 巡回形BCH符号とみなされる

RS Code

- BCH code is binary element [0,1] code, RS code is multi-element code[0,1,2,...]
- BCH code defines message polynomial P(x) and generator polynomial G(x) on a set of GF(2), where as RS code defines message and generator polynomial on expansion field GF(2^m) from the beginning
- In many implementation, GF(2^8) (1 byte unit) is used
- RS code is viewed as Cyclic BCH code

拡大体

- 有限体GF(2)において系列Fの元{0, 1, α}はαのべき乗で表現される

  $F=\{0, 1, \alpha, \alpha^2, \ldots, \alpha^j, \ldots\}=\{0, \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^j, \ldots\}$

- 拡大体GF(2^m)では元の数は2^mであり，乗算に関して閉じていることが条件となる

- この条件を満たすためには，以下の既約多項式を満たす必要がある

  $\alpha^{(2m-1)}+1=0$

Extension Field

- In finite field GF(2), elements $\{0, 1, \alpha\}$ of series F can be represented by power of α

  $F = \{0, 1, \alpha, \alpha^2, ..., \alpha^j, ...\} = \{0, \alpha^0, \alpha^1, \alpha^2, ..., \alpha^j, ...\}$

- In extension field (2^m), the number of elements is 2^m, it is closed under multiplication

- To construct extension field, the following irreducible polynomial should hold

  $\alpha^{(2m-1)} + 1 = 0$

拡大体 (2)

- なぜなら，既約多項式は

  $\alpha^{(2m-1)} = 1 = \alpha^{0}$

- であるから

  $\alpha^{(2m+n)} = \alpha^{(2m-1)}\alpha^{(n+1)} = \alpha^{0}\alpha^{(n+1)} = \alpha^{(n+1)}$

- となり，系列Fは

  $F = \{0,\ \alpha^{0},\ \alpha^{1},\ \alpha^{2},\ \ldots,\ \alpha^{2m-2},\ \alpha^{2m-1},\ \alpha^{2m},\ \alpha^{2m+1},\ \ldots\}$

  $= \{0,\ \alpha^{0},\ \alpha^{1},\ \alpha^{2},\ \ldots,\ \alpha^{2m-2},\ \alpha^{0},\ \alpha^{1},\ \alpha^{2},\ \ldots\}$

- したがってGF(2^{m})は

  $GF(2^{m}) = \ = \{0,\ \alpha^{0},\ \alpha^{1},\ \alpha^{2},\ \ldots,\ \alpha^{2m-2}\}$

Extension Field (2)

- Because, irreducible polynomial can be written as

  $\alpha^{(2m-1)} = 1 = \alpha^{0}$

- So that

  $\alpha^{(2m+n)} = \alpha^{(2m-1)}\alpha^{(n+1)} = \alpha^{0}\alpha^{(n+1)} = \alpha^{(n+1)}$

- Thus, series F can be expressed as

  $F = \{0, \alpha^{0}, \alpha^{1}, \alpha^{2}, \ldots, \alpha^{2m-2}, \alpha^{2m-1}, \alpha^{2m}, \alpha^{2m+1}, \ldots\}$

  $= \{0, \alpha^{0}, \alpha^{1}, \alpha^{2}, \ldots, \alpha^{2m-2}, \alpha^{0}, \alpha^{1}, \alpha^{2}, \ldots\}$

- Therefore, GF(2^m) is constructed

  $GF(2^m) = \ = \{0, \alpha^{0}, \alpha^{1}, \alpha^{2}, \ldots, \alpha^{2m-2}\}$

拡大体 (3)

- 拡大体GF(2^m)における加算は，非零のi乗の元α^iをxの多項式で表現して

$$\alpha^i = \alpha_i(x) = \alpha_{i,0} + \alpha_{i,1}x + \alpha_{i,2}x^2 + \alpha_{i,3}x^3 + \ \dots\ + \alpha_{i,m-1}x^{m-1}$$

- 任意の2項の加算は，多項式の対応する係数の加算(排他的論理和)となる

$$\begin{aligned}\alpha^i + \alpha^j &= \alpha_i(x) + \alpha_j(x) \\ &= (\alpha_{i,0} + \alpha_{j,0}) + (\alpha_{i,1} + \alpha_{j,1})x + (\alpha_{i,2} + \alpha_{j,2})\ x^2 + \ \dots\ + \\ &\quad (\alpha_{i,m-1} + \alpha_{j,m-1})\ x^{m-1}\end{aligned}$$

- したがって，加算に関して閉じている

Extension Field (3)

- Addition in extension field GF(2^m) is based on the following polynomial representation. Non-zero element α^i can be written as

$$\alpha^i = \alpha_i(x) = \alpha_{i,0} + \alpha_{i,1}x + \alpha_{i,2}x^2 + \alpha_{i,3}x^3 + \ \dots \ + \alpha_{i,m-1}x^{m-1}$$

- Addition of two elements can be done by XOR operation of each term of polynomial

$$\alpha^i + \alpha^j = \alpha_i(x) + \alpha_j(x)$$
$$= (\alpha_{i,0} + \alpha_{j,0}) + (\alpha_{i,1} + \alpha_{j,1})x + (\alpha_{i,2} + \alpha_{j,2})\ x^2 + \ \dots \ + (\alpha_{i,m-1} + \alpha_{j,m-1})\ x^{m-1}$$

- Therefore, it is closed under addition

RS符号の構成 (1)

- 8元の場合，シンボル0-7に対して3ビットを単位として誤り訂正，検出を行う (αはx^3+x+1の根)

シンボル	ビット表現	多項式表現	GF(2^m)べき表現
0	000	0	0
1	001	1	1
2	010	α	α
3	011	α^2	α^2
4	100	$1+\alpha$	α^3
5	101	$\alpha+\alpha^2$	α^4
6	110	$1+\alpha+\alpha^2$	α^5
7	111	$1+\alpha^2$	α^6

Structure of RS Code (1)

- For 8 elements, error correction and detection is performed to symbol 0-7 based on 3-bit unit (α is root of x^3+x+1

Symbol	Bit Rep.	Poly. Rep.	GF(2^m) Power Rep.
0	000	0	0
1	001	1	1
2	010	α	α
3	011	α^2	α^2
4	100	$1 + \alpha$	α^3
5	101	$\alpha + \alpha^2$	α^4
6	110	$1 + \alpha + \alpha^2$	α^5
7	111	$1 + \alpha^2$	α^6

RS符号の構成 (2)

- 加算演算 (αはx^3+x+1の根)

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	0	α^3	α^6	α^1	α^5	α^4	α^2
α^1	α^3	0	α^4	α^0	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α^1	α^3	α^0
α^3	α^1	α^0	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α^1	α^6	0	α^0	α^3
α^5	α^4	α^6	α^3	α^2	α^0	0	α^1
α^6	α^2	α^5	α^0	α^4	α^3	α^1	0

Structure of RS Code (2)

- Addition (α is a root of x^3+x+1)

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	0	α^3	α^6	α^1	α^5	α^4	α^2
α^1	α^3	0	α^4	α^0	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α^1	α^3	α^0
α^3	α^1	α^0	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α^1	α^6	0	α^0	α^3
α^5	α^4	α^6	α^3	α^2	α^0	0	α^1
α^6	α^2	α^5	α^0	α^4	α^3	α^1	0

RS符号の構成 (3)

- 乗算演算 (αはx^3+x+1の根)

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^1	α^1	α^2	α^3	α^4	α^5	α^6	α^0
α^2	α^2	α^3	α^4	α^5	α^6	α^0	α^1
α^3	α^3	α^4	α^5	α^6	α^0	α^1	α^2
α^4	α^4	α^5	α^6	α^0	α^1	α^2	α^3
α^5	α^5	α^6	α^0	α^1	α^2	α^3	α^4
α^6	α^6	α^0	α^1	α^2	α^3	α^4	α^5

Structure of RS Code (3)

- Multiplication (α is a root of x^3+x+1)

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^1	α^1	α^2	α^3	α^4	α^5	α^6	α^0
α^2	α^2	α^3	α^4	α^5	α^6	α^0	α^1
α^3	α^3	α^4	α^5	α^6	α^0	α^1	α^2
α^4	α^4	α^5	α^6	α^0	α^1	α^2	α^3
α^5	α^5	α^6	α^0	α^1	α^2	α^3	α^4
α^6	α^6	α^0	α^1	α^2	α^3	α^4	α^5

RS符号の構成 (4)

- 送信情報の分割とGF(2^3)の割り当て
  - (100111011000000000)
  - (100)(111)(011)(000)(000)(000)
  - α^3, α^6, α^2, *0*, *0*, *0*

- 生成多項式を G(x)=$x+1$ とする

- これらの元を係数とする通報多項式P(x)を作成し，生成多項式の最高次数(この例では1)に相当するx^1を掛ける
  - $P(x) = \alpha^3 + \alpha^6 x + \alpha^2 x^2$
  - $xP(x) = \alpha^3 x + \alpha^6 x^2 + \alpha^2 x^3$

Structure of RS Code (4)

- Division of send message and assign of $GF(2^3)$
  - (100111011000000000)
  - (100)(111)(011)(000)(000)(000)
  - α^3, α^6, α^2, 0, 0, 0
- Generator polynomial $G(x)=x+1$
- Create message polynomial $P(x)$ having these elements as coefficients, multiply x^1 to the maximum degree (in this example, 1) of generator polynomial
  - $P(x)= \alpha^3 + \alpha^6 x + \alpha^2 x^2$
  - $xP(x)= \alpha^3 x + \alpha^6 x^2 + \alpha^2 x^3$

RS符号の構成 (5)

- xP(x)を生成多項式で割り,余りR(x)を求める
  - G(x)の根が$x=1$であるから, 余りR(x)はxP(x)に$x=1$を代入した結果に等しい

    $R(x)=1P(1)=\alpha^3 + \alpha^6 + \alpha^2 = \alpha$

- 符号多項式F(x)は

  $F(x)=xP(x)+R(x) = \alpha + \alpha^3 x + \alpha^6 x^2 + \alpha^2 x^3$

- 符号は

  (010)(100)(111)(011)(000)(000)(000)

Structure of RS Code (5)

- Obtain residual R(x) through dividing xP(x) by generator polynomial
  - root of G(x) is $x=1$, thus residual R(x) is the same polynomial obtained by inserting $x=1$ to xP(x)

    $R(x)=1P(1)= \alpha^3 + \alpha^6 + \alpha^2 = \alpha$

- Code polynomial F(x) is given by

  $F(x)=xP(x)+R(x) = \alpha + \alpha^3 x + \alpha^6 x^2 + \alpha^2 x^3$

- Code

  (010)(100)(111)(011)(000)(000)(000)

原始多項式 (1)

- 多項式$x^{n-1}+1$ $(n=2^m-1)$を割り切る既約多項式のうち，周期が最大のものを原始多項式という

- 最大次数n-1次以下の他の多項式でも既約といなっていれば，原始多項式ではない

- 多項式$x^{15}+1$ $(m=4)$の場合，x^4+x+1は原始多項式であるが，$x^4+x^3+x^2+x+1$は既約多項式であっても原始多項式ではない

  $$x^{15}+1 = (x^4+x+1)(x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)$$

  $$x^{15}+1 = (x^4+x^3+x^2+x+1)(x^{11}+x^{10}+x^6+x^5+x+1)$$

  しかし

  $$x^5+1 = (x^4+x^3+x^2+x+1)(x+1)$$

Primitive Polynomial (1)

- Among irreducible polynomials which can divide polynomial $x^{n-1}+1$ $(n=2^m-1)$, the one which has the largest period is called primitive polynomial

- If a polynomial is also irreducible to other lower order (Max. n-1) polynomial, it is not primitive polynomial

- For polynomial $x^{15}+1$ $(m=4)$, x^4+x+1 is primitive polynomial, but $x^4+x^3+x^2+x+1$ is only irreducible

  $$x^{15}+1 = (x^4+x+1)(x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)$$

  $$x^{15}+1 = (x^4+x^3+x^2+x+1)(x^{11}+x^{10}+x^6+x^5+x+1)$$

  but

  $$x^5+1 = (x^4+x^3+x^2+x+1)(x+1)$$

原始多項式 (2)

- 幾つかのmに対する原始多項式

m	原始多項式	m	原始多項式
3	$1+x+x^3$	14	$1+x+x^6+x^{10}+x^{14}$
4	$1+x+x^4$	15	$1+x+x^{15}$
5	$1+x^2+x^5$	16	$1+x+x^3+x^{12}+x^{16}$
6	$1+x+x^6$	17	$1+x^3+x^{17}$
7	$1+x^3+x^7$	18	$1+x^7+x^{18}$
8	$1+x^2+x^3+x^4+x^8$	19	$1+x+x^2+x^5+x^{19}$
9	$1+x^4+x^9$	20	$1+x^3+x^{20}$
10	$1+x^3+x^{10}$	21	$1+x^2+x^{21}$
11	$1+x^2+x^{11}$	22	$1+x+x^{22}$
12	$1+x+x^4+x^6+x^{12}$	23	$1+x^5+x^{23}$
13	$1+x+x^3+x^4+x^{13}$	24	$1+x+x^2+x^7+x^{24}$

Primitive Polynomial (2)

- Primitive polynomials for some m

m	Primitive polynomial	m	Primitive polynomial
3	$1+x+x^3$	14	$1+x+x^6+x^{10}+x^{14}$
4	$1+x+x^4$	15	$1+x+x^{15}$
5	$1+x^2+x^5$	16	$1+x+x^3+x^{12}+x^{16}$
6	$1+x+x^6$	17	$1+x^3+x^{17}$
7	$1+x^3+x^7$	18	$1+x^7+x^{18}$
8	$1+x^2+x^3+x^4+x^8$	19	$1+x+x^2+x^5+x^{19}$
9	$1+x^4+x^9$	20	$1+x^3+x^{20}$
10	$1+x^3+x^{10}$	21	$1+x^2+x^{21}$
11	$1+x^2+x^{11}$	22	$1+x+x^{22}$
12	$1+x+x^4+x^6+x^{12}$	23	$1+x^5+x^{23}$
13	$1+x+x^3+x^4+x^{13}$	24	$1+x+x^2+x^7+x^{24}$

RS符号の構成2 (1)

- 符号シンボル数n，情報シンボル数k，検査シンボル数$2t$

  $RS(n, k) = RS(2^m-1, 2^m-1-2t)$

- 生成多項式

  $G(x)=g_0+g_1x+g_2x^2+ \ldots + g_{2t-1}x^{2t-1} + x^{2t}$

- G(x)の根を$\alpha, \alpha^2, \ldots, \alpha^{2t}$とすると，$t=2$のとき

$$
\begin{aligned}
G(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) \\
&= (x^2-(\alpha+\alpha^2)x+\alpha^3)(x^2-(\alpha^3+\alpha^4)x+\alpha^7) \\
&= x^4-\alpha^3x^3+\alpha^0x^2-\alpha^1x+\alpha^3 \\
&= \alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3+x^4
\end{aligned}
$$

Structure of RS Code-2 (1)

- Code symbol number n, information symbol number k, parity symbol number $2t$

  $$RS(n, k) = RS(2^m-1, 2^m-1-2t)$$

- Generation polynomial

  $$G(x)=g_0+g_1x+g_2x^2+ \ldots + g_{2t-1}x^{2t-1} + x^{2t}$$

- Let roots of G(x) be $\alpha, \alpha^2, \ldots, \alpha^{2t}$. When $t=2$,

  $$\begin{aligned} G(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) \\ &= (x^2-(\alpha+\alpha^2)x+\alpha^3)(x^2-(\alpha^3+\alpha^4)x+\alpha^7) \\ &= x^4-\alpha^3x^3+\alpha^0x^2-\alpha^1x+\alpha^3 \\ &= \alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3+x^4 \end{aligned}$$

RS符号の構成2 (2)

- 通報多項式を検査シンボル数だけシフトして得られた多項式を，生成多項式で割った余りが検査シンボル系列となる

  $X^{n-k}P(x)=G(x)Q(x)+R(x)$

- すなわち剰余R(x)は

  $R(x)=X^{n-k}P(x) \quad modulo\ G(x)$

- 符号多項式F(X)は

  $F(x)= X^{n-k}P(x)+R(x)$

Structure of RS Code-2 (2)

- First, shift input polynomial by the number of parity length. This polynomial is divided by generator polynomial. Residual corresponds to parity data.

  $$X^{n-k}P(x)=G(x)Q(x)+R(x)$$

- Thus, residual is obtained by

  $$R(x)=X^{n-k}P(x) \quad modulo\ G(x)$$

- Code polynomial F(X) is given by

  $$F(x)= X^{n-k}P(x)+R(x)$$

RS符号の構成2 (3)

- (7,3)RS符号の例として情報シンボルが以下の場合の通報多項式を求める

  [010 110 111] = [α^1 α^3 α^5]

  $P(x)=\alpha^1+\alpha^3x+\alpha^5x^2$

- 生成多項式

  $G(x)=\alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3+x^4$

- 通報多項式を$n-k=4$よりx^4だけシフトし，生成多項式で割る

  $X^4P(x)=x^4\ (\alpha^1+\alpha^3x+\alpha^5x^2)=\alpha^1x^4+\alpha^3x^5+\alpha^5x^6$

  $=(\alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3+x^4)(\alpha^4+\alpha^0x+\alpha^5x^2)$

  $+(\alpha^0+\alpha^2x+\alpha^4x^2+\alpha^6x^3)$

Structure of RS Code-2 (3)

- An example of (7,3)RS code. Lets obtain message polynomial when input information is the following.

  [010 110 111] = [α^1 α^3 α^5]

  $P(x)=\alpha^1+\alpha^3x+\alpha^5x^2$

- Generator polynomial

  $G(x)=\alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3+x^4$

- Shift message polynomial as x^4 since $n\text{-}k=4$, divide by generator polynomial

  $X^4P(x)=x^4\ (\alpha^1+\alpha^3x+\alpha^5x^2)=\alpha^1x^4+\alpha^3x^5+\alpha^5x^6$

  $=(\alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3+x^4)(\alpha^4+\alpha^0x+\alpha^5x^2)$

  $+(\alpha^0+\alpha^2x+\alpha^4x^2+\alpha^6x^3)$

RS符号の構成2 (4)

- 符号多項式F(x)はシフトした通報多項式に剰余(検査シンボル)を加える

$$F(x)=R(x)+X^4P(x)$$
$$= (\alpha^0+\alpha^2x+\alpha^4x^2+\alpha^6x^3) +(\alpha^1x^4+\alpha^3x^5+\alpha^5x^6)$$

- シンボルをバイナリに復号

$$[\ \alpha^0\ \alpha^2\ \alpha^4\ \alpha^6\ \alpha^1\ \alpha^3\ \alpha^5\ ]$$

=[001 100 110 101 010 010 111]

検査ビット　　情報ビット

Structure of RS Code-2 (4)

- Code polynomial is created by adding residual (parity symbols) to the shifted message polynomial

  $F(x) = R(x) + X^4 P(x)$

  $= (\alpha^0 + \alpha^2 x + \alpha^4 x^2 + \alpha^6 x^3) + (\alpha^1 x^4 + \alpha^3 x^5 + \alpha^5 x^6)$

- Convert symbols to binary data

  $[\ \alpha^0\ \alpha^2\ \alpha^4\ \alpha^6\ \alpha^1\ \alpha^3\ \alpha^5\ ]$

  $= [\ 001\ 100\ 110\ 101\ 010\ 010\ 111]$

  Parity bit　　Information bit