符号理論･暗号理論

- No.9 BCH符号 -

渡辺　裕

Coding Theory / Cryptography

- No.9 BCH Code -

Hiroshi Watanabe

誤り訂正符号

- BCH符号(Bose-Chaudhuri-Hocquenghem code)
  - 符号
    - オッケンジェム, 1959
    - ボーズ, チョードリ, 1960
  - 復号
    - ピーターソン, 1961
    - バーレカンプ, 1968, マッシイ, 1969
    - チェン, 1964

Error Correction Code

- BCH code(Bose-Chaudhuri-Hocquenghem code)
  - Coding
    - Hocquenghem, 1959
    - Bose & Chaudhuri, 1960
  - Decoding
    - Peterson, 1961
    - Berlekamp, 1968 & Massey, 1969
    - Chien, 1964

BCH符号

- 有限体 GF(2^m) の原始元をαとし, α^1, α^2, … ,α^{2t} の全てを根として持つ最小次数の多項式を生成多項式とする符号長 $n=2^m-1$ の巡回符号をBCH符号という
- $d=2t+1 < 2^m-1$
- 符号長: 2^m-1
  情報ビット数: $k>= 2^m-1-mt$
  誤り訂正能力: $t_o>=t$

BCH Code

- Let the primitive element of Finite Field GF(2^m) be α. BCH code is a cyclic code having generator polynomial with code length $n=2^m-1$. This is the minimum degree polynomial that has all root α^1, α^2, … ,α^{2t}
- $d=2t+1 < 2^m-1$
- code length: 2^m-1
  information bits: $k>= 2^m-1-mt$
  error correction capability: $t_o>=t$

有限体

- 有限体とは？
  - 加算と乗算の結果が有限個の元からなる
  - ガロア体とも呼ぶ
  - GF(q)で表す
  - qを位数を呼ぶ
  - 有限体は位数qが素数あるいはそのべき乗のときに成り立つ

Finite Field

- What is finite field？
  - Addition and multiplication result in finite number of element
  - Finite field is also called "Galois field"
  - Represented by GF(q)
  - "q" is called "order"
  - Finite field exists when order q is prime number or its power

有限体 (2)

- 有限体の例
  - GF(3)　mod3 の演算，逆元の存在が必要

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	-x
0	0
1	2
2	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

x	x^{-1}
0	-
1	1
2	2

Finite Field (2)

- Example of finite field
  - GF(3)　mod3 operation, needs existence of inverse element

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	-x
0	0
1	2
2	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

x	x^{-1}
0	-
1	1
2	2

拡大体

- 拡大体とは
  - 有限体 GF(P) を拡大したもの
  - GF(2) に対して $GF(2^m)$ は拡大体
  - 拡大体では，元は整数だけではなく，m次既約多項式の根を付加
- 拡大体の例
  - $GF(2^2)=GF(4)$ は GF(2) の拡大体
  - 既約多項式の根を元に加える
  - $x^2+x+1=0$ は2次既約多項式であり，この根αを元に加える

Extension Field

- What is extension field?
  - Finite field GF(P) is extended
  - $GF(2^m)$ is extension field for GF(2)
  - In extension field, element is not only integer but root of m-th degree irreducible polynomial
- Example of extension field
  - $GF(2^2)=GF(4)$ is an extension field for GF(2)
  - Root of irreducible polynomial is added
  - $x^2+x+1=0$ is 2nd degree irreducible polynomial, thus this equation's root α is added to the element

拡大体 (2)

- 拡大体の例(続き)
  - 0, 1, αから他の元を求める
  - 体では積も同じ体の元に含まれる

$$\alpha^0 = 1$$
$$\alpha^1 = \alpha$$
$$\alpha^2 = \alpha + 1 \quad (\alpha^2 + \alpha + 1 = 0, \alpha = -\alpha)$$
$$\alpha^3 = \alpha\alpha^2 = \alpha(\alpha + 1) = \alpha + 1 + \alpha = 1$$

Extension Field (2)

- Example of extension field(cntd.)
  - Obtain other element from 0, 1, α
  - In field, product of elements is included in the elements of the same filed

$$\alpha^0 = 1$$
$$\alpha^1 = \alpha$$
$$\alpha^2 = \alpha + 1 \quad (\alpha^2 + \alpha + 1 = 0, \alpha = -\alpha)$$
$$\alpha^3 = \alpha\alpha^2 = \alpha(\alpha + 1) = \alpha + 1 + \alpha = 1$$

拡大体 (3)

- 拡大体の例(続き)
  - GF(4) 0, 1, α, α^2 を元とする

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

x	-x
0	0
1	1
α	α
α^2	α^2

x	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

x	-x
0	-
1	1
α	α^2
α^2	α

Extension Field (3)

- Example of extension field(cntd.)
  - GF(4) has element 0, 1, α , α^2

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

x	-x
0	0
1	1
α	α
α^2	α^2

x	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

x	-x
0	-
1	1
α	α^2
α^2	α

拡大体 (4)

- 一般に GF(2) のm次拡大体 GF(2^m)
  - 0 および m次既約多項式の根

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

を GF(2^m) の原始元と呼ぶ
  - なお, αは 2^m-1 乗で1に戻る

$$\alpha^{2^m-1} = 1$$

  - GF(2^m) の原始元のべきによる表現を"べき表現"という

Extension Field (4)

- In general, m-th degree extension field GF(2^m) for GF(2)
  - We call 0 and root of m-th degree irreducible polynomial

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

primitive element of GF(2^m)
  - Here, α to the power of 2^m-1 result in 1

$$\alpha^{2^m-1} = 1$$

  - Representation of GF(2^m) by primitive element is called "power representation"

拡大体 (5)

- べき表現とベクトル表現
- GF(2^4), 既約多項式 x^4+x+1 の根をαとした場合

べき表現	α^3, α^2, α, 1 による展開				ベクトル表現
0				0	0000
1				1	0001
α			α		0010
α^2		α^2			0100
α^3	α^3				1000
α^4			α	+1	0011
α^5		α^2	+α		0110

Extension Field (5)

- Power and vector representation
- GF(2^4), let root of irreducible polynomial x^4+x+1 be α

Power Rep.	Extension by α^3, α^2, α, 1				Vector Rep.
0				0	0000
1				1	0001
α			α		0010
α^2		α^2			0100
α^3	α^3				1000
α^4			α	+1	0011
α^5		α^2	+α		0110

拡大体 (6)

べき表現	α^3, α^2, α, 1 による展開				ベクトル表現
α^6	α^3	$+\alpha^2$			1100
α^7	α^3		$+\alpha$	+1	1011
α^8		α^2		+1	0101
α^9	α^3		$+\alpha$		1010
α^{10}		α^2	$+\alpha$	+1	0111
α^{11}	α^3	$+\alpha^2$	$+\alpha$		1110
α^{12}	α^3	$+\alpha^2$	$+\alpha$	+1	1111
α^{13}	α^3	$+\alpha^2$		+1	1101
α^{14}	α^3			+1	1001

Extension Field (6)

Power Rep.	Extension by α^3, α^2, α, 1				Vector Rep.
α^6	α^3	$+\alpha^2$			1100
α^7	α^3		$+\alpha$	+1	1011
α^8		α^2		+1	0101
α^9	α^3		$+\alpha$		1010
α^{10}		α^2	$+\alpha$	+1	0111
α^{11}	α^3	$+\alpha^2$	$+\alpha$		1110
α^{12}	α^3	$+\alpha^2$	$+\alpha$	+1	1111
α^{13}	α^3	$+\alpha^2$		+1	1101
α^{14}	α^3			+1	1001

BCH符号の構成

- 根の重なり
  - GF(2^4)上の多項式 $F(x)=1+x+x^3$ がα^i を根とするとき, α^{2i} も根となる

$$\begin{aligned}\{f(x)\}^2 &= \left(x^3+x+1\right)^2 \\ &= x^6+x^4+x^3+x^4+x^2+x+x^3+x+1 \\ &= x^6+(x^4+x^4)+(x^3+x^3)+x^2+(x+x)+1 \\ &= x^6+x^2+1 \\ &= f(x^2)\end{aligned}$$

Construction of BCH Code

- Double root
  - When polynomial $F(x)=1+x+x^3$ has root α^i on GF(2^4), α^{2i} is also a root

$$\begin{aligned}\{f(x)\}^2 &= \left(x^3+x+1\right)^2 \\ &= x^6+x^4+x^3+x^4+x^2+x+x^3+x+1 \\ &= x^6+(x^4+x^4)+(x^3+x^3)+x^2+(x+x)+1 \\ &= x^6+x^2+1 \\ &= f(x^2)\end{aligned}$$

BCH符号の構成 (2)

- 根の重なり(続き)
  - 多項式の根をαとすれば一般に以下の式が成り立つ

$$f(\alpha^2)=\{f(\alpha)\}^2=0 \quad (t=1)$$
$$f(\alpha^4)=\{f(\alpha)\}^4=0 \quad (t=2)$$
$$f(\alpha^8)=\{f(\alpha)\}^8=0 \quad (t=3)$$

  - α, α^3, α^5, … を根として持つGF(2)上の多項式は, α^2, α^4, α^6, … も根として持つので, α, α^3, …, α^{2t-1} のt個の元を根として持つ最小次数の多項式を生成多項式とする

Construction of BCH Code (2)

- Double root(cntd.)
  - In general the following relation holds when root of polynomial is written by α

$$f(\alpha^2)=\{f(\alpha)\}^2=0 \quad (t=1)$$
$$f(\alpha^4)=\{f(\alpha)\}^4=0 \quad (t=2)$$
$$f(\alpha^8)=\{f(\alpha)\}^8=0 \quad (t=3)$$

  - Polynomial on GF(2) having α, α^3, α^5, … as roots also has α^2, α^4, α^6, … as its roots. Thus, the minimum degree polynomial having t elements α, α^3, …, α^{2t-1} as its root is the generator polynomial

BCH符号の構成 (3)

- BCH符号の符号長を $n=2^m-1$, $GF(2^m)$ の原始元を α とし, α^i の最小多項式を $M_i(x)$ とする
- 生成多項式 G(x) は
  - $G(x)=LCM\{M_1(x), M_2(x), \ldots, M_{2t}(x)\}$
    (ここに, LCMは最小公倍多項式)
  - しかし, $M_{2t}(x)= M_{2t-1}(x)$ なる関係が成立するので
  - $G(x)=LCM\{M_1(x), M_3(x), \ldots, M_{2t-1}(x)\}$
- G(x)の最高次数がmであれば, 検査ビットがmビット, 情報ビットkは $k=n-m=2^m-1-m$
- 生成多項式に含む最小多項式の数が誤り訂正能力に相当

Construction of BCH Code (3)

- Let the length of BCH code be $n=2^m-1$, let the primitive element of $GF(2^m)$ be α, the minimum polynomial of α^i is $M_i(x)$
- Generator polynomial G(x) is given as follows.
  - $G(x)=LCM\{M_1(x), M_2(x), \ldots, M_{2t}(x)\}$
    (Here, LCM is Least Common Multiple polynomial)
  - However, the relation $M_{2t}(x)= M_{2t-1}(x)$ holds. Thus we have
  - $G(x)=LCM\{M_1(x), M_3(x), \ldots, M_{2t-1}(x)\}$
- When the maximum degree of G(x) is m, parity bit is m, information bit k is $k=n-m=2^m-1-m$
- The number of minimum polynomial in generator polynomial corresponds to the error correction capability

BCH符号の例

- m=4 ($GF(2^4)$, $n=2^m-1=2^4-1=15$, のとき2ビットエラー訂正可能なBCH符号の生成多項式の導出
  - t=2 より $M_1(x)$ と $M_3(x)$ を求めればよい

$$\begin{aligned}M_1(x)&=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)\\&=(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)\\&=x^4+(\alpha+\alpha^2+\alpha^4+\alpha^8)x^3\\&\quad+(\alpha^3+\alpha^5+\alpha^9+\alpha^6+\alpha^{10}+\alpha^{12})x^2\\&\quad+(\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14})x+\alpha^{15}\\&=x^4+x+1\end{aligned}$$

Example of BCH Code

- Derivation of generator polynomial of BCH code for 2 bit error correction when m=4 ($GF(2^4)$, $n=2^m-1=2^4-1=15$
- From t=2 , we only need $M_1(x)$ and $M_3(x)$

$$\begin{aligned}M_1(x)&=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)\\&=(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)\\&=x^4+(\alpha+\alpha^2+\alpha^4+\alpha^8)x^3\\&\quad+(\alpha^3+\alpha^5+\alpha^9+\alpha^6+\alpha^{10}+\alpha^{12})x^2\\&\quad+(\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14})x+\alpha^{15}\\&=x^4+x+1\end{aligned}$$

BCH符号の例 (2)

- 同様にして

$$\begin{aligned} M_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) \\ &= (x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^9) \\ &= x^4 + (\alpha^3+\alpha^6+\alpha^{12}+\alpha^9)x^3 \\ &\quad + (\alpha^{21}+\alpha^9+\alpha^{15}+\alpha^{12}+\alpha^{18}+\alpha^{15})x^2 \\ &\quad + (\alpha^{21}+\alpha^{18}+\alpha^{24}+\alpha^{27})x + \alpha^{30} \\ &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

Example of BCH Code (2)

- Similarly

$$\begin{aligned} M_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) \\ &= (x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^9) \\ &= x^4 + (\alpha^3+\alpha^6+\alpha^{12}+\alpha^9)x^3 \\ &\quad + (\alpha^{21}+\alpha^9+\alpha^{15}+\alpha^{12}+\alpha^{18}+\alpha^{15})x^2 \\ &\quad + (\alpha^{21}+\alpha^{18}+\alpha^{24}+\alpha^{27})x + \alpha^{30} \\ &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

BCH符号の例 (3)

- 生成多項式は $G(x)=M_1(x)M_3(x)$ であるから

$$\begin{aligned} G(x) &= (x^4+x+1)(x^4+x^3+x^2+x+1) \\ &= x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

- BCH符号の検査ビットは8ビット, 符号長は15ビットであるから, 情報ビットは7ビット, 2ビットの誤り訂正が可能

Example of BCH Code (3)

- Generator polynomial is $G(x)=M_1(x)M_3(x)$

$$\begin{aligned} G(x) &= (x^4+x+1)(x^4+x^3+x^2+x+1) \\ &= x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

- Parity bit of BCH code is 8 bit, code length is 15 bit, so that information bit is 7 bit, and 2 bit error correction is possible

BCH符号の例 (4)

- 情報ビット (1000 000) に対する2ビット誤り訂正可能なBCH符号の算出
  - n=15, m=8, k=7
  - 情報の各ビットを多項式P(x)の各係数に対応させると P(x)=1
  - 符号長に合わせてビットシフト

$$x^8 P(x) = x^8$$

Example of BCH Code (4)

- Derivation of BCH code which can correct 2 bit to information bit (1000 000)
  - n=15, m=8, k=7
  - By comparing information bit to each coefficient of polynomial P(x), we have P(x)=1
  - bit shift by considering code length

$$x^8 P(x) = x^8$$

BCH符号の例 (5)

- BCH符号の検査ビットは上式を生成多項式で割った余り

$$x^8 P(x) \div G(x) = x^8 \div (x^8 + x^7 + x^6 + x^4 + 1)$$
$$Q(x) = 1$$
$$R(x) = x^7 + x^6 + x^4 + 1$$

- 符号F(x)は次式で計算できる

$$F(x) = x^8 P(x) + R(x)$$
$$= 1 + x^4 + x^6 + x^7 + x^8$$

Example of BCH Code (5)

- Parity bit of BCH code is the residual of the previous equation divided by generator polynomial

$$x^8 P(x) \div G(x) = x^8 \div (x^8 + x^7 + x^6 + x^4 + 1)$$
$$Q(x) = 1$$
$$R(x) = x^7 + x^6 + x^4 + 1$$

- Code F(x) can be calculated by

$$F(x) = x^8 P(x) + R(x)$$
$$= 1 + x^4 + x^6 + x^7 + x^8$$

BCH符号の例 (6)

- (1000000) に対するBCH符号

1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}	x^{14}
1	0	0	0	1	0	1	1	1	0	0	0	0	0	0

Example of BCH Code (6)

- BCH Code for (1000000)

1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}	x^{14}
1	0	0	0	1	0	1	1	1	0	0	0	0	0	0

BCH符号の復号

- 生成多項式 $G(x)=x^8+x^7+x^6+x^4+1$ で作成した符号を受信した結果が (1000 1011 0100 000) のとき，誤り2ビットの位置を求める
  - 受信多項式 $Y(x)=1+x^4+x^6+x^7+x^9$ 誤り位置を i,j とすると, $E(x)=x^i+x^j$
  - t=2 より α, α^2, α^3, α^4 に対するシンドローム S_1-S_4

$$S_1 = E(\alpha) = \alpha^i + \alpha^j$$
$$S_2 = E(\alpha^2) = \alpha^{2i} + \alpha^{2j}$$
$$S_3 = E(\alpha^3) = \alpha^{3i} + \alpha^{3j}$$
$$S_4 = E(\alpha^4) = \alpha^{4i} + \alpha^{4j}$$

Decoding of BCH Code

- Obtain location of 2 bit error when (1000 1011 0100 000) is received, originally coded by $G(x)=x^8+x^7+x^6+x^4+1$
  - received polynomial is $Y(x)=1+x^4+x^6+x^7+x^9$, location of error is i,j, then $E(x)=x^i+x^j$
  - from t=2, syndrome S_1-S_4 are given by α, α^2, α^3, α^4

$$S_1 = E(\alpha) = \alpha^i + \alpha^j$$
$$S_2 = E(\alpha^2) = \alpha^{2i} + \alpha^{2j}$$
$$S_3 = E(\alpha^3) = \alpha^{3i} + \alpha^{3j}$$
$$S_4 = E(\alpha^4) = \alpha^{4i} + \alpha^{4j}$$

BCH符号の復号 (2)

- シンドロームの計算(αの受信多項式への代入)

$$S_1 = Y(\alpha) = 1 + \alpha^4 + \alpha^6 + \alpha^7 + \alpha^9 = \alpha^{12}$$
$$S_2 = Y(\alpha^2) = \{Y(\alpha)\}^2 = \alpha^{24} = \alpha^9$$
$$S_3 = Y(\alpha^3) = 1 + \alpha^{12} + \alpha^{18} + \alpha^{21} + \alpha^{27} = \alpha^8$$
$$S_4 = Y(\alpha^4) = \{Y(\alpha^2)\}^2 = \{S_2\}^2 = \alpha^{18} = \alpha^3$$

Decoding of BCH Code (2)

- Calculation of syndrome (substitute to received polynomial expressed by α)

$$S_1 = Y(\alpha) = 1 + \alpha^4 + \alpha^6 + \alpha^7 + \alpha^9 = \alpha^{12}$$
$$S_2 = Y(\alpha^2) = \{Y(\alpha)\}^2 = \alpha^{24} = \alpha^9$$
$$S_3 = Y(\alpha^3) = 1 + \alpha^{12} + \alpha^{18} + \alpha^{21} + \alpha^{27} = \alpha^8$$
$$S_4 = Y(\alpha^4) = \{Y(\alpha^2)\}^2 = \{S_2\}^2 = \alpha^{18} = \alpha^3$$

BCH符号の復号 (3)

- S1-S4の展開

$$S_1 = \alpha^{12} = 1 + \alpha^2 + \alpha + \alpha^3$$
$$= \alpha^8 + \alpha^9$$

$$S_2 = \alpha^9 = \alpha + \alpha^3$$
$$= \alpha^{2\times 8} + \alpha^{2\times 9}$$

$$S_3 = \alpha^8 = 1 + \alpha^2 = \alpha^{3\times 8} + \alpha^{3\times 9}$$
$$S_4 = \alpha^3 = \alpha^3 + \alpha^2 + \alpha^2 = \alpha^{4\times 8} + \alpha^{4\times 9}$$

i=8, j=9

Decoding of BCH Code (3)

- Extension of S1-S4

$$S_1 = \alpha^{12} = 1 + \alpha^2 + \alpha + \alpha^3$$
$$= \alpha^8 + \alpha^9$$

$$S_2 = \alpha^9 = \alpha + \alpha^3$$
$$= \alpha^{2\times 8} + \alpha^{2\times 9}$$

$$S_3 = \alpha^8 = 1 + \alpha^2 = \alpha^{3\times 8} + \alpha^{3\times 9}$$
$$S_4 = \alpha^3 = \alpha^3 + \alpha^2 + \alpha^2 = \alpha^{4\times 8} + \alpha^{4\times 9}$$

i=8, j=9