通信路符号化法
ガロア体とBCH符号

ガロア体

- 体：加減乗除の四則演算について閉じている系.
- 有限体（ガロア体）：有限個の元しか持たない体

  $\mathrm{GF}(q)$ … qは元の数（「位数」）

  $\mathrm{GF}(q) \Leftrightarrow q = p^m$（$p$は素数，$m$は正整数）
- 素体 $\mathrm{GF}(q)$（pは素数）… mod演算で作られる

素体の例

GF(2)

$+$	0	1
0	0	1
1	1	0

$-$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

$/$	0	1
0	$\perp$	0
1	$\perp$	1

素体の例

GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

拡大体

- 拡大体 $\mathrm{GF}(p^m)$（pは素数，$2 \leq m$）は，素体$\mathrm{GF}(p)$に，m次原始多項式（周期が$p^m - 1$となるm次の多項式）の根を1個追加して体を作る.

- $\mathrm{GF}(2)$のm次の拡大体$\mathrm{GF}(2^m)$は，m次原始多項式の根αのべき：$\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{2^m-2}$と0から構成する.
  - つまり，$\mathrm{GF}(2^m) = \{0, 1, \alpha^1, \alpha^2, \cdots, \alpha^{2^m-2}\}$
  - $\alpha^{2^m-1} = 1$であり，αは$\mathrm{GF}(2^m)$の原始元と呼ばれる.

拡大体

例：$\mathrm{GF}(2^4)$の作り方

- $\mathrm{GF}(2)$上の多項式x^4+x+1は原始多項式である．その根をαとし，αを$\mathrm{GF}(2)$に付加した体を作ってみよう．
- この体は、基本要素の集まり$\{0,1,\alpha\}$を含んでいる．これを乗算と加算で閉じるまで拡張していく．
- 乗算の結果は，この体に含まれなければならない．
  $\alpha^{15}=1$なので，α^iという形の要素は次のものが全てこの体に含まれる．
  $\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}\}$
- 加算に関しては点検だけ．$\alpha^4+\alpha+1=0$つまり，$\alpha^4=\alpha+1$ であることに注意して，すべての$\{a_3,a_2,a_1,a_0\}$に対して，$a_3\alpha^3+a_2\alpha^2+a_1\alpha^1+a_0\alpha^0$がこの体に含まれることを確認する．

⇒ 完了！

$\mathrm{GF}(2^4)$
0
1
α
α^2
α^3
$\alpha^4=\alpha+1$
$\alpha^5=\alpha^2+\alpha$
$\alpha^6=\alpha^3+\alpha^2$
$\alpha^7=\alpha^4+\alpha^3=\alpha^3+\alpha+1$
$\alpha^8=\alpha^4+\alpha^2+\alpha=\alpha^2+1$
$\alpha^9=\alpha^3+\alpha$
$\alpha^{10}=\alpha^4+\alpha^2=\alpha^2+\alpha+1$
$\alpha^{11}=\alpha^3+\alpha^2+\alpha$
$\alpha^{12}=\alpha^4+\alpha^3+\alpha^2=\alpha^3+\alpha^2+\alpha+1$
$\alpha^{13}=\alpha^4+\alpha^3+\alpha^2+\alpha=\alpha^3+\alpha^2+1$
$\alpha^{14}=\alpha^4+\alpha^3+\alpha=\alpha^3+1$
$\alpha^{15}=\alpha^4+\alpha=1$

拡大体

GF(2^m)の元のベクトル表現

- αが，m次原始多項式
  $$F(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_1 x + 1$$
  の根であったとする．ここで，$f_1, \cdots, f_{m-1}$はGF(2)の元である．
- $F(\alpha) = 0$であるので，$\alpha^m = f_{m-1}\alpha^{m-1} + \cdots + f_1\alpha + 1$
- これを用いると，$\alpha^i = (i = 0,1,\cdots,2^m - 2)$を，GF(2)の元 $a_{m-1}, \cdots, a_1, a_0$を係数とする$\alpha^{m-1}, \cdots, \alpha, 1$の1次式
  $$\alpha^i = a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0$$
  で表すことができる．
- GF(2)の要素からなるGF(2)上の係数ベクトル
  $$(a_{m-1}, \cdots, a_1, a_0)$$
  をGF(2^m)の元のベクトル表現と呼ぶ．

例

べき表現	$\alpha^3, \alpha^2, \alpha^1, \alpha^0$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	$\alpha + 1$	0011
α^5	$\alpha^2 + \alpha$	0110
α^6	$\alpha^3 + \alpha^2$	1100
α^7	$\alpha^3 + \alpha + 1$	1011
α^8	$\alpha^2 + 1$	0101
α^9	$\alpha^3 + \alpha$	1010
α^{10}	$\alpha^2 + \alpha + 1$	0111
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101
α^{14}	$\alpha^3 + 1$	1001
α^{15}	1	0001

拡大体

$p > 2$に対する素体$\mathrm{GF}(p)$の拡大も同様に行う.

例:$\mathrm{GF}(3)$ の2次の拡大体$\mathrm{GF}(3^2)$の構成

(1) $\mathrm{GF}(3)$の原始多項式の探索:下記の通り，$x^2 + x + 2$は原始多項式である.

```
                1  2  2  0  2  1  1
        ┌──────────────────────────
1  1  2 ) 1  0  0  0  0  0  0  0  2
           1  1  2
           ─────────
              2  1  0
              2  2  1
              ──────────
                 2  2  0
                 2  2  1
                 ──────────
                    0  2  0
                    0  0  0
                    ──────────
                       2  0  0
                       2  2  1
                       ──────────
                          1  2  0
                          1  1  2
                          ──────────
                             1  1  2
                             1  1  2
                             ──────
                                   0
```

$\left(x^2 + x + 2\right) \mid \left(x^{3^2-1} - 1\right)$
かつ,
$n < 3^2 - 1$なるnに対して
$\left(x^2 + x + 2\right) \mid (x^n - 1)$
とならない.

拡大体

GF(3)の2次の拡大体GF(3^2)の構成 （つづき）

(2) x^2+x+2の根をβと置いて，GF(3)を拡張する．$\beta^2+\beta+2=0$であるから，

$$\beta^2=-\beta-2=2\beta+1$$
$$\beta^3=2\beta^2+\beta=2(2\beta+1)+\beta=2\beta+2$$
$$\beta^4=2\beta^2+2\beta=2(2\beta+1)+2\beta=2$$
$$\beta^5=2\beta$$
$$\beta^6=2\beta^2=2(2\beta+1)=\beta+2$$
$$\beta^7=\beta(\beta+2)=\beta^2+2\beta=2\beta+1+2\beta=\beta+1$$
$$\beta^8=\beta(\beta+1)=\beta^2+\beta=2\beta+1+\beta=1$$

さらに，$b_1\beta+b_0 \quad b_i\in \mathrm{GF}(3)$が全部そろっているから

$$\mathrm{GF}\left(3^2\right)=\left\{0,1,\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6,\beta^7\right\}$$

となっていることがわかる．　■

拡大体

$GF(3^2)$のべき表現とベクトル表現

$GF(3^2)$のべき表現	$b_1\beta + b_0$形式の表現	ベクトル表現
0	0	00
1	1	01
β	β	10
β^2	$2\beta + 1$	21
β^3	$2\beta + 2$	22
β^4	2	02
β^5	2β	20
β^6	$\beta + 2$	12
β^7	$\beta + 1$	11

BCH符号

t 誤り訂正可能なBCH符号

- $d = 2t + 1$とする．$d < 2^m - 1$となるようにmを選ぶ．$\mathrm{GF}(2^m)$の原始元をαとする．
- $\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+d-2}$をすべて根として持つ最小次数の$\mathrm{GF}(2)$上の多項式を生成多項式とする符号長$n = 2^m - 1$の2元巡回符号がBCH符号である．
- l はふつう1か0に選ばれる．このBCH符号は（少なくとも）t 誤り訂正可能
- 最もよく用いられるBCH符号：$l = 1, d = 2t + 1$.
- このとき，生成多項式は，$2t$ 個の元：$\alpha, \alpha^2, \cdots, \alpha^{2t}$を根とする最小次数の多項式

$$G(x) = \mathrm{LCM}(m_1(x), m_2(x), \cdots, m_{2t}(x))$$

として与えられる．

BCH符号

- $m_i(x)$はα^iを根とする最小次数の多項式であり，α^iの最小多項式と呼ばれる．また，$m_i(x)$の x^0の係数は1である．すなわち，

$$m_i(x) = x^p + \cdots + a_1 x + 1$$

という形をしている．

- α^iは，$\mathrm{GF}(2)$上のm次ベクトルとして表現できるので，未知数がm個の連立1次方程式を解くことにより，

$$m_i(\alpha^i) = \alpha^{ip} + \cdots + a_1 \alpha^i + 1 = 0$$

を満足する$\mathrm{GF}(2)$上の多項式$m_i(x)$を定めることができる．

- $m_i(x)$は高々m次多項式である

- 従って，

$$G(x) = \mathrm{LCM}(m_1(x), m_2(x), \cdots, m_{2t}(x))$$

は高々$2mt$次多項式である．

BCH符号

- GF(2)上の多項式$F(x) = f_s x^s + f_{s-1} x^{s-1} + \cdots + f_1 x + f_0 = 0$
  の根をβとすると，β^2も根である．なぜならば，

$$
\begin{aligned}
F^2(x) &= (f_s x^s + f_{s-1} x^{s-1} + \cdots + f_1 x + f_0)^2 \\
&= f_s f_s x^{s+s} + f_{s-1} f_{s-1} x^{(s-1)+(s-1)} + \cdots + f_0 f_0 \\
&\quad + f_s f_{s-1} x^{s+(s-1)} + f_{s-1} f_s x^{(s-1)+s} \\
&\quad + f_s f_{s-2} x^{s+(s-2)} + f_{s-2} f_s x^{(s-2)+s} \\
&\quad + \cdots + f_1 f_0 x^{1+0} + f_0 f_1 x^{0+1} \\
&= f_s x^{2s} + f_{s-1} x^{2(s-1)} + \cdots + f_0 = F\left(x^2\right)
\end{aligned}
$$

  であるので，$F(\beta) = 0$ならば，$F\left(\beta^2\right) = 0$であるから．

- このように t 個の元：$\alpha, \alpha^3, \cdots, \alpha^{2t-1}$を根とする最小次数の多項式の次数は mt 以下であり，それを生成多項式として使うBCH符号の検査ビット数 $n-k$を mt 以下にすることができる．

BCH符号

- BCH限界：BCH符号の最小距離$d_{\min}$は$d_{\min} \geq d$を満たす.
- BCH符号は，次のように特徴づけられる巡回符号である.

符号長	$n = 2^m - 1$
情報ビット数	$k \geq 2^m - 1 - mt$
誤り訂正能力	$t_0 \geq t$

BCH符号

（例）原始多項式$x^4 + x + 1$（根をαとする）を用いて，$m = 4, t = 2$とする（少なくとも）2誤り訂正能力をもつ(15,7)BCH符号を構成する.

(1) 生成多項式の構成

$m_1(x)$: αを根とする多項式 → 原始多項式そのもの : $x^4 + x + 1$

$m_3(x)$: α^3を根とする多項式 : $x^4 + x^3 + x^2 + x + 1$ → 求め方は次スライド

生成多項式 : $\mathrm{GF}(x) = \mathrm{LCM}\big(m_1(x), m_3(x)\big)$

$$= (x^4 + x + 1)\big(x^4 + x^3 + x^2 + x + 1\big)$$

$$= x^8 + x^7 + x^6 + x^4 + 1$$

(2) 符号語は$G(x)$を使って巡回符号の場合と同様に構成する.

BCH符号

$m_3(x)$の求め方：

$$m_3(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1$$

と置き，

$$m_3(\alpha^3) = a_4\alpha^{12} + a_3\alpha^9 + a_2\alpha^6 + a_1\alpha^3 + 1 = 0$$

が満たされるような$\{a_4, a_3, a_2, a_1\}$を求める．

ベクトル表現を使うと，上式は，

$$\begin{bmatrix}1\\1\\1\\1\end{bmatrix}a_4 + \begin{bmatrix}1\\0\\1\\0\end{bmatrix}a_3 + \begin{bmatrix}1\\1\\0\\0\end{bmatrix}a_2 + \begin{bmatrix}1\\0\\0\\0\end{bmatrix}a_1 + \begin{bmatrix}0\\0\\0\\1\end{bmatrix} = 0$$

となる．

これを解いて，

$$a_4 = 1, a_3 = 1, a_2 = 1, a_1 = 1$$

を得る．

BCH符号の復号

- 受信多項式$Y(x) = y_{n-1}x^{n-1} + \cdots + y_1 x + y_0$に対して,

$$S_i = Y(\alpha^i) \ (i = 1,2,\cdots,2t)$$

によりシンドローム $S_1, S_2, \cdots, S_{2t}$を計算する.

- シンドロームがすべて0ならば, 誤りなしと判定する.
- シンドロームのなかに0でないものがあるときは, $j_1, j_2, \cdots, j_l$を誤り位置と仮定して, シンドロームから誤り位置多項式

$$\sigma(z) = (1 - \alpha^{j_1} z)(1 - \alpha^{j_2} z) \cdots (1 - \alpha^{j_l} z)$$

を構成する.

- $\sigma(z) = 0$の根 $\alpha^{-j_1}, \alpha^{-j_2}, \cdots, \alpha^{-j_l}$を求める.
- $\alpha^{-j_1}, \alpha^{-j_2}, \cdots, \alpha^{-j_l}$から, $j_1, j_2, \cdots, j_l$を求め, これらの位置の記号を訂正する.

BCH符号の復号

誤りが2個，すなわち，$t = 2$の場合について，与えられたシンドローム $\{S_1, S_2, S_3, S_4\}$ から，未知の誤りに対する誤り位置方程式を構成する方法：

目標の誤り位置多項式は，

$$\sigma(z) = \left(1 - \alpha^{j_1} z\right)\left(1 - \alpha^{j_2} z\right) = 1 + \left(\alpha^{j_1} + \alpha^{j_2}\right) z + \alpha^{j_1}\alpha^{j_2} z^2$$

という形式をしている．

定義により，

$$S_1 = \alpha^{j_1} + \alpha^{j_2}$$
$$S_3 = \alpha^{3j_1} + \alpha^{3j_2}$$

さらに，

$${S_1}^3 = \left(\alpha^{j_1} + \alpha^{j_2}\right)^3 = \alpha^{3j_1} + \alpha^{3j_2} + \alpha^{j_1}\alpha^{j_2}\left(\alpha^{j_1} + \alpha^{j_2}\right) = S_3 + \alpha^{j_1}\alpha^{j_2} S_1$$

から

$$\alpha^{j_1}\alpha^{j_2} = ({S_1}^3 + S_3){S_1}^{-1}$$

が得られるので，

$$\sigma(z) = 1 + S_1 z + ({S_1}^3 + S_3){S_1}^{-1} z^2$$

BCH符号の復号

【例題】 GF(2)上の原始多項式x^4+x+1の原始元αをGF(2)に加えて得られるGF(2^4)の根α, α^3を根に持つ多項式$x^8+x^7+x^6+x^4+1$を生成多項式とする(15,7)BCH符号において，ある符号語を送ったところ，受信語 111000011110010 が得られたという．もとの入力語は何であったか？ただし，誤りは高々2個であると仮定する．

解

(a) 受信語の多項式表現は，

$$x^{14}+x^{13}+x^{12}+x^7+x^6+x^5+x^4+x$$

(b) シンドローム$\{S_1, S_3\}$は

$$S_1=\alpha^{14}+\alpha^{13}+\alpha^{12}+\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha=\alpha^2+1=\alpha^7$$

$$S_3=\alpha^{42}+\alpha^{39}+\alpha^{36}+\alpha^{21}+\alpha^{18}+\alpha^{15}+\alpha^{12}+\alpha^3=\alpha^7$$

BCH符号の復号

(c) 誤り位置方程式は,

$$\sigma(z) = 1 + S_1 z + \left({S_1}^3 + S_3\right){S_1}^{-1} z^2 = 1 + \alpha^7 z + \alpha^3 z^2$$

(d) $\sigma(1), \sigma(\alpha), \sigma\left(\alpha^2\right), \cdots, \sigma(\alpha^{14})$を順に計算する.

$$\sigma\left(\alpha^0\right) = 1 + \alpha^7 + \alpha^3 = 1 + \left(\alpha^3 + \alpha + 1\right) + \alpha^3 = \alpha$$

$$\sigma(\alpha^1) = 1 + \alpha^8 + \alpha^5 = 1 + \left(\alpha^2 + 1\right) + \left(\alpha^2 + \alpha\right) = \alpha$$

$$\sigma\left(\alpha^2\right) = 1 + \alpha^9 + \alpha^7 = 1 + \left(\alpha^3 + \alpha\right) + \left(\alpha^3 + \alpha + 1\right) = 0$$

$$\sigma\left(\alpha^3\right) = 1 + \alpha^{10} + \alpha^9 = 1 + \left(\alpha^2 + \alpha + 1\right) + \left(\alpha^3 + \alpha\right) = \alpha^3 + \alpha^2 = \alpha^6$$

$$\sigma(\alpha^4) = 1 + \alpha^{11} + \alpha^{11} = 1$$

$$\sigma\left(\alpha^5\right) = 1 + \alpha^{12} + \alpha^{13} = 1 + \left(\alpha^3 + \alpha^2 + \alpha + 1\right) + \left(\alpha^3 + \alpha^2 + 1\right)$$

$$= \alpha + 1 = \alpha^4$$

$$\sigma\left(\alpha^6\right) = 1 + \alpha^{13} + \alpha^{15} = 1 + \left(\alpha^3 + \alpha^2 + 1\right) + 1 = \alpha^3 + \alpha^2 + 1 = \alpha^{13}$$

$$\sigma(\alpha^7) = 1 + \alpha^{14} + \alpha^{17} = 1 + \left(\alpha^3 + 1\right) + \alpha^2 = \alpha^3 + \alpha^2 = \alpha^6$$

BCH符号の復号

$$\sigma(\alpha^8) = 1 + \alpha^{15} + \alpha^{19} = 1 + (\alpha + 1) + 1 = \alpha + 1 = \alpha^4$$

$$\sigma(\alpha^9) = 1 + \alpha^{16} + \alpha^{21} = 1 + \alpha + (\alpha^3 + \alpha^2) = \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^{12}$$

$$\sigma(\alpha^{10}) = 1 + \alpha^{17} + \alpha^{23} = 1 + \alpha^2 + (\alpha^2 + 1) = 0$$

$$\sigma(\alpha^{11}) = 1 + \alpha^{18} + \alpha^{25} = 1 + \alpha^3 + (\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha^{11}$$

$$\sigma(\alpha^{12}) = 1 + \alpha^{19} + \alpha^{27} = 1 + (\alpha + 1) + (\alpha^3 + \alpha^2 + \alpha + 1)$$
$$= \alpha^3 + \alpha^2 + 1 = \alpha^{13}$$

$$\sigma(\alpha^{13}) = 1 + \alpha^{20} + \alpha^{29} = 1 + (\alpha^2 + \alpha) + (\alpha^3 + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha^{11}$$

$$\sigma(\alpha^{14}) = 1 + \alpha^{21} + \alpha^{31} = 1 + (\alpha^3 + \alpha^2) + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^{12}$$

(e) 以上から，誤り位置多項式が次のように分解されることが分かる．

$$\sigma(z) = (1 + \alpha^{-2}z)(1 + \alpha^{-10}z)$$

(f) ゆえに，誤り位置：$\alpha^{-2} = \alpha^{13} = \alpha^{j_1}, \alpha^{-10} = \alpha^5 = \alpha^{j_2}$の2か所．つまり

入力語：1010000110010010

BCH符号の基本的性質

BCH符号の最小距離 $d_{\min}$は$d_{\min} \geq d$を満たす.
（dはBCH限界と呼ばれる）

証明

$\mathrm{GF}(2^m)$の原始元を α とし，$n = 2^m - 1$とおく.

(a) jを$0 \leq j < n$となる整数とすれば，次の等式が成り立つ.

$$\sum_{i=0}^{n-1} \alpha^{ij} = \begin{cases} 1 & ;j = 0 \\ 0 & ;\text{その他} \end{cases}$$

BCH符号の基本的性質

(b) $\mathrm{GF}(2^m)$上のn次元ベクトル$w = (w_0, w_1, \cdots, w_{n-1})$に対し,

$$\widetilde{w}_j = \sum_{i=0}^{n-1} w_i \alpha^{ij} \quad (j = 0,1,\cdots,n-1)$$

と置くと,

$$w_i = \sum_{j=0}^{n-1} \widetilde{w}_j \alpha^{-ij} \quad (i = 0,1,\cdots,n-1)$$

が成立する.

(c) $1, \alpha, \cdots, \alpha^{d-2}$を根とする生成多項式$G(x)$から生成される符号長 n の符号$w = (w_0, w_1, \cdots, w_{n-1})$のフーリエ変換を$\widetilde{w} = (\widetilde{w}_0, \widetilde{w}_1, \cdots, \widetilde{w}_{n-1})$とすると,
$\widetilde{w}_0 = \widetilde{w}_1 = \cdots = \widetilde{w}_{d-2} = 0$が成立する.

BCH符号の基本的性質

従って,

$$\widetilde{W}(x) = \widetilde{w}_{n-1}x^{n-1} + \cdots + \widetilde{w}_{d-1}x^{d-1} = \left(\widetilde{w}_{n-1}x^{n-d} + \cdots + \widetilde{w}_{d-1}\right)x^{d-1}$$

であり, $\widetilde{W}(x) = 0$の非零の根は高々$n-d$個である.

従って,

$$w_i = \sum_{j=0}^{n-1} \widetilde{w}_j \alpha^{-ij} \quad (i = 0,1,\cdots,n-1)$$

と規定されるw_iのうち0になるものは高々$n-d$個しかない.

従って, どの符号も 0 との距離は d 以上であり, BCH符号の線形性から $d_{\min} \geq d$が示された.

(d) $\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+d-2}$を根とする生成多項式を用いてBCH符号を構成する場合も上と同様. ■

まとめ

- ガロア体
  - 素体
  - 素体の拡張
- BCH符号
  - 構成法
  - 復号法
  - 基本的性質