12.1 ガロア体

加減乗除の四則演算について閉じている系を**体**(field)という. 有限個の要素数からなる有限体は**ガロア体**とも呼ばれGF(q)で表される. qはガロア体に含まれる要素の数を示す指標であり, **位数**と呼ばれる. ガロア体が存在するのは$q = p^m$ (p:素数, m:正整数)のときだけである. $m = 1$のとき素体, $1 < m$のとき拡大体と呼ばれる.

素体

素体GF(p)　(p:素数)はmod演算で作られる. p個の整数の集合$\{0,1,2,\cdots,p-1\}$においてmod p の加算と乗算を導入し, 要素間を関連づける. つまり, 加算, 乗算については整数として普通に行ってから, p による剰余を値とする. 減算, 除算は加算, 乗算の逆演算として定義する.

GF(7) = {0,1,2,3,4,5,6}を例にとって説明しよう. 加算, 乗算については,

$$x + y \bmod 7 \text{ および } x \times y \bmod 7$$

による. たとえば,

$$2 + 3 = 5 \bmod 7 \quad 5 + 6 = 4 \bmod 7$$
$$2 \times 3 = 6 \bmod 7 \quad 5 \times 6 = 2 \bmod 7$$

となる. その全体像は, 表 1, 表 2 のようにまとめられる.

表 1. GF(7)の加算

+	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

表 2. GF(7)の乗算

×	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

また, 減算$b - a$は, bにaの加法に関する逆元$-a$を加えることにより行う. $-a$は,

$$(-a) + a = 0 \bmod p$$

を満たす元であり,

$$-a = \begin{cases} 0 & ; a = 0 \\ p - a & ; \text{それ以外} \end{cases}$$

により求める. 非零の元aによる徐算b/aは, bにaの乗法に関する逆元a^{-1}を乗じることによって行える. a^{-1}は

$$a^{-1}a \equiv 1 \bmod p$$

表 3. GF(7)の減算：(x, y)要素は$x - y$を表す

−	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	1	0	6	5	4	3	2
2	2	1	0	6	5	4	3
3	3	2	1	0	6	5	4
4	4	3	2	1	0	6	5
5	5	4	3	2	1	0	6
6	6	5	4	3	2	1	0

表 4. GF(7)の除算：(x, y)要素はx/yを表す

/	0	1	2	3	4	5	6
0	-	0	0	0	0	0	0
1	-	1	4	5	2	3	6
2	-	2	1	3	4	6	5
3	-	3	5	1	6	2	4
4	-	4	2	6	1	5	3
5	-	5	6	4	3	1	2
6	-	6	3	2	5	4	1

を満たす元であり，ユークリッドの互除法でも求められるが，乗算の表 2 から逆算してもよい．

以下で用いるGF(2)や，GF(3)も同様に表 5～12 のように定義される．

表 5．GF(2)の加算

+	0	1
0	0	1
1	1	0

表 6．GF(2)の乗算

×	0	1
0	0	0
1	0	1

表 7．GF(2)の減算

−	0	1
0	0	1
1	1	0

表 8．GF(2)の除算

／	0	1
0	-	0
1	-	1

表 9．GF(3)の加算

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

表 10．GF(3)の乗算

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

表 11．GF(3)の減算

−	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

表 12．GF(3)の除算

／	0	1	2
0	-	0	0
1	-	1	2
2	-	2	1

拡大体

素体GF(p)上のm次原始多項式を$G(x)$とし，$G(x) = 0$の根の一つをαとしよう．すると，定義により，$G(x) \mid (x^{p^m-1} - 1)$であるので，

$$\alpha^{p^m-1} = 1$$
$$\alpha^i \alpha^j = \alpha^{[i+j] \bmod p^m-1}$$
$$\alpha^{-i} = \alpha^{[p^m-1-i] \bmod p^m-1}$$

などが成り立つ．

位数が$q = p^m$ $(2 \leq m)$ （pは素数）のガロア体GF(p^m)は，素体GF(p)上の一つのm次原始多項式の根の一つαをGF(p)に加えて四則演算に関して閉じた集合を作ることによって得られる．こ

れを$\mathrm{GF}(p)$の**拡大**と呼ぶ.

$\mathrm{GF}(2)$のm次の拡大体$\mathrm{GF}(2^m)$は, $\mathrm{GF}(2)$上の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で構成できる要素数$2^m$の集合である.

【例 1】 $\mathrm{GF}(2^4)$

$\mathrm{GF}(2)$上の原始多項式x^4+x+1の根をαとする. 次に, αを$\mathrm{GF}(2)$に追加した$\{0,1,\alpha\}$を含む体を構成してみる. 乗算の結果はこの体に含まれなければならない. αが$x^4+x+1=0$の根である, つまり, $\alpha^4=\alpha^1+\alpha^0$であることに注意して, この体に含まれるべき要素を順に追加していくと,

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

となり,

$$\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}\}$$

で閉じていることがわかる. すべての$a_i \in \mathrm{GF}(2)$に対して, $a_3\alpha^3+a_2\alpha^2+a_1\alpha^1+a_0\alpha^0$が出現しているので, この集合は加算に関しても閉じていることがわかる.

【例 2】 $\mathrm{GF}(3)$の2次の拡大体$\mathrm{GF}(3^2)$を構成してみよう.

まず, $\mathrm{GF}(3)$の原始多項式を探してみよう. 図 1 の計算から, x^2+x+2が$\mathrm{GF}(3)$の原始多項式, つまり, $(x^2+x+2) \mid (x^{3^2-1}-1)$であり, かつ, $b<3^2-1$なるbに対して$(x^2+x+2) \mid (x^b-1)$とならないことがわかる.

そこでx^2+x+2の根をβとおいて, $\mathrm{GF}(3)$を拡張してみよう. $\beta^2+\beta+2=0$であるから,

```
                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
```

図 1.　$(x^2+x+2)\mid\left(x^{3^2-1}-1\right)$であることの組み算による確認

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

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

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

となっていることがわかる．ここで，$\beta^4=2$であるので，

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

である．

以上のように，素体$\mathrm{GF}(p)$の原始多項式の根αを用いてp^m個の要素から成る

$$\mathrm{GF}(p^m)=\{0\}\cup\left\{\alpha^i\,\middle|\,0\le i\le p^m-2\right\}$$
$$=\{a_{m-1}\alpha^{m-1}+\cdots+a_0\mid a_i\in \mathrm{GF}(p),0\le i\le m\}$$

を構成できる．ここでαは**原始元**，$\mathrm{GF}(p^m)$の元の原始元のべきによる表現は**べき表現**と呼ばれる．

また，GF(p^m) の元 γ を $a_{m-1}\alpha^{m-1}+\cdots+a_0$ と表したときの係数で構成されるベクトル $(a_{m-1},\cdots,a_0)$ $a_i \in \mathrm{GF}(p)$をγの**ベクトル表現**と呼ぶ．表 13，表 14 にGF(2^4)とGF(3^2)のべき表現とベクトル表現をそれぞれ示す．

表 13. GF(2^4)のべき表現とベクトル表現

GF(2^4)のべき表現	$\alpha^3,\alpha^2,\alpha,1$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	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^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}	α^3+1	1001

表 14.　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

【問題】GF(3)の原始多項式でx^2+x+2以外のものを探し，GF(3^2)を構成せよ．

12.2 BCH (Bose-Chaudhuri-Hocqenghem「ボーズ・チョドーリ・ボッケンジェム」)符号

BCH 符号は巡回符号の一種であり，ブロック長や誤り訂正能力を目的に応じてカスタマイズできる．符号化は生成多項式を用いて，巡回符号と同様に行う．復号はシンドロームに基づいて行う．シンドロームが零ならば誤りなしと判定し，非零のときは，シンドロームから誤り位置を同定する．

以下で述べる BCH 符号は，

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　$t_0 \geq t$　ただし，tは$d = 2^{m-1} - 1$以下の正整数．

という特性を持つ（ユーザは必要に応じて，パラメータmとtを指定する）．

生成多項式

$\mathrm{GF}(2^m)$の原始元をαとする．BCH 符号の生成多項式$G(x)$は，$\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+d-2}$のすべてを根とする，$\mathrm{GF}(2)$上の最小次数の多項式である．ここで，$d = 2t + 1$．また，$l$は，$l \leq n - 1$を満たす非負整数であり，ふつう1か0が選ばれる．

$l = 1$の場合については，$\alpha, \alpha^2, \cdots, \alpha^{2t}$のすべてを根とする$\mathrm{GF}(2)$上の最小次数の多項式が$G(x)$となるが，これは，$\mathrm{LCM}(m_1(x), m_2(x), \cdots, m_{2t}(x))$として与えられる．ここで，$m_i(x)$は$\alpha^i$を根とする最小次数の多項式であり，$\alpha^i$の**最小多項式**と呼ばれる．

αは$\mathrm{GF}(2^m)$の原始元であり，$m_i(x)$のx^0の係数が1，すなわち，$m_i(x) = x^p + \cdots + a_1 x + 1$という形であり，さらに，$\alpha^i$が$\mathrm{GF}(2)$上の$m$の要素のベクトルとして表現できることに着目すると，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ので，$m_i(x)$は高々$m$次多項式であることがわかる．従って，$G(x)$が高々$2mt$次多項式であることがわかる．

さらに，$\mathrm{GF}(2)$上の多項式$F(x) = f_s x^s + f_{s-1} x^{s-1} + \cdots + f_1 x + f_0$について，

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

であるので，α^iが$\mathrm{GF}(2)$上の多項式$F(x) = f_s x^s + f_{s-1} x^{s-1} + \cdots + f_1 x + f_0 = 0$の根であれば，$\alpha^{2i}$も根となるという性質を利用すると，$G(x)$は，$t$個の元$\alpha, \alpha^3, \cdots, \alpha^{2t-1}$を根とする最小次数の多項式$\mathrm{LCM}(m_1(x), m_3(x), \cdots, m_{2t-1}(x))$で与えられ，高々$mt$次である，つまり，この巡回符号の検査ビット数を$mt$以下にできることがわかる．さらに，$\alpha^i$が$F(x)$の根ならば$\alpha^{4i}, \alpha^{8i}, \cdots$も$F(x)$の根となる

ので，$G(x)$の次数をさらに下げることができる．

$t=1$の場合，生成多項式は$\mathrm{GF}(2^m)$の原始元αを根として持つ最小次数の多項式，すなわち，m次の原始多項式であるので，$t=1$の BCH 符号は巡回ハミング符号となることがわかる．

【例】$m=4, t=2$とする（少なくとも）2誤り訂正能力を持つ(15,7)BCH 符号を構成してみよう．αを原始多項式x^4+x+1の根とすると，定義により，$m_1(x)=x^4+x+1$となる．一方，$m_3(x)$については，

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

と置いて，この方程式がα^3を根に持つよう$\{a_4,a_3,a_2,a_1\}$を定めることにより求める．すなわち，

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

が満たされるような$\{a_4,a_3,a_2,a_1\}$を求める．上式は，ベクトル表現を使うと，

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

となる．これを解くと，

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

を得る．

以上から，求める生成多項式は，

$$\begin{aligned}\mathrm{GF}(x)&=\mathrm{LCM}(m_1(x),m_3(x))\\&=(x^4+x+1)(x^4+x^3+x^2+x+1)\\&=x^8+x^7+x^6+x^4+1\end{aligned}$$

であることがわかる．

別解：生成多項式$G(x)$の次数は$mt=8$以下であることに注目し，$G(x)=g_8x^8+\cdots+g_1x+1$と置き，$G(x)$が$\alpha,\alpha^3$を根として持つから係数$\{g_8,\cdots,g_1\}$を求めてもよい．

一般の場合も同様にする．連立方程式が不定になり，解が一意に定まらなければ，最小次数の$G(x)$にする．

BCH 符号の性質

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．

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

なぜならば,

$j=0$の場合:nが奇数であるので,

$$\sum_{i=0}^{n-1}\alpha^{ij}=\sum_{i=0}^{n-1}1=1$$

である.

$j\neq 0$の場合:$\alpha^n=1$であるので, $\alpha^{jn}=(\alpha^n)^j=1^j=1$である. 従って, α^jはx^n-1の根である. ここで, $0\leq j<n$であるので$\alpha^j\neq 1$であり, かつ$x^n-1=(x-1)(x^{n-1}+\cdots+x+1)$であるので, α^jは$x^{n-1}+\cdots+x+1$, つまり,

$$\sum_{i=0}^{n-1}x^i=0$$

の根となる. つまり,

$$\sum_{i=0}^{n-1}\alpha^{ij}=0$$

である. □

(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,

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

と置くと,

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

が成立する. $\tilde{w}=(\tilde{w}_0,\tilde{w}_1,\cdots,\tilde{w}_{n-1})$は$w$の**フーリエ変換**と呼ばれる. なぜならば,

$$\begin{aligned}\sum_{j=0}^{n-1}\tilde{w}_j\alpha^{-ij}&=\sum_{j=0}^{n-1}\left(\sum_{k=0}^{n-1}w_k\alpha^{kj}\right)\alpha^{-ij}\\&=\sum_{j=0}^{n-1}\left(\sum_{k=0}^{n-1}w_k\alpha^{(k-i)j}\right)\\&=\sum_{k=0}^{n-1}\left(w_k\sum_{j=0}^{n-1}\alpha^{(k-i)j}\right)\\&=w_i\end{aligned}$$

となるからである. □

(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 の符号語 $w = (w_0, w_1, \cdots, w_{n-1})$ のフーリエ変換を $\tilde{w} = (\tilde{w}_0, \tilde{w}_1, \cdots, \tilde{w}_{n-1})$ とする.

w は生成多項式 $G(x)$ から生成された符号であるので, w の多項式表現

$$W(x) = \sum_{i=0}^{n-1} w_i x^{ij}$$

は, ある多項式 $A(x)$ に対して,

$$W(x) = A(x)G(x)$$

となっている. また, フーリエ変換の定義から

$$\tilde{w}_j = \sum_{i=0}^{n-1} w_i \alpha^{ij}$$

であるので,

$$\tilde{w}_0 = \tilde{w}_1 = \cdots = \tilde{w}_{d-2} = 0$$

である. 従って,

$$\begin{aligned} \tilde{W}(x) &= \tilde{w}_{n-1}x^{n-1} + \cdots + \tilde{w}_{d-1}x^{d-1} \\ &= (\tilde{w}_{n-1}x^{n-d} + \cdots + \tilde{w}_{d-1})x^{d-1} \end{aligned}$$

となり, $\tilde{W}(x) = 0$ の非零の根で $\mathrm{GF}(2^m)$ に含まれるものは高々 $n-d$ 個である.

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

であるので, w_i $(0 \le i \le n-1)$ のうち0となるものの個数は高々 $n-d$ 個である. 換言すれば, w_i のうち1となるものは少なくとも d 個あるので, どの符号も0との距離は, 少なくとも d である. BCH 符号は線形符号であるので, 符号語間の最小距離 $d_{\min}$ について, $d_{\min} \ge d$ であることが示された. □

(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についても, 上記の $l = 0$ の場合と同様に証明できる.

$$\tilde{w}_j = \sum_{i=0}^{n-1} w_i \alpha^{ij}$$

であり, $w_{n-1}, \cdots, w_0$ は符号語であるので, $j = l, l+1, \cdots, l+d-2$ について, $\tilde{w}_j = 0$, つまり, $\tilde{w}_l = \tilde{w}_{l+1} = \cdots = \tilde{w}_{l+d-2} = 0$ となる. 従って, $\tilde{w}_j$ を x^j の係数とする多項式 $\tilde{W}(x)$ は,

$$\begin{aligned} \tilde{W}(x) &= \tilde{w}_{n-1}x^{n-1} + \cdots + \tilde{w}_1 x + \tilde{w}_0 \\ &= \tilde{w}_{n-1}x^{n-1} + \cdots + \tilde{w}_{l+d-1}x^{l+d-1} + \tilde{w}_{l-1}x^{l-1} + \cdots + \tilde{w}_0 \end{aligned}$$

という形になる. 従って,

$$\begin{aligned}\widetilde{W}(x)x^{n-l} &= \widetilde{w}_{n-1}x^{2n-l-1} + \cdots + \widetilde{w}_{l+d-1}x^{n+d-1} + \widetilde{w}_{l-1}x^{n-1} + \cdots + \widetilde{w}_0 x^{n-l} \\ &= \left(\widetilde{w}_{n-1}(x^{2n-l-1} - x^{n-l-1}) + \cdots + \widetilde{w}_{l+d-1}(x^{n+d-1} - x^{d-1})\right) \\ &\quad + \widetilde{w}_{n-1}x^{n-l-1} + \cdots + \widetilde{w}_{l+d-1}x^{d-1} + \widetilde{w}_{l-1}x^{n-1} + \cdots + \widetilde{w}_0 x^{n-l} \\ &= (\widetilde{w}_{n-1}x^{n-l-1} + \cdots + \widetilde{w}_{l+d-1}x^{d-1})(x^n - 1) \\ &\quad + (\widetilde{w}_{l-1}x^{n-d} + \cdots + \widetilde{w}_0 x^{n-l-d+1} + \widetilde{w}_{n-1}x^{n-l-d} + \cdots + \widetilde{w}_{l+d-1})x^{d-1}\end{aligned}$$

となる. $\mathrm{GF}(2^m)$の任意の非零の要素zについて$z^n = 1$であるので, 右辺の第 1 項は常に 0 であるのことに注意すると, 右辺を0にする$\mathrm{GF}(2^m)$の非零の要素の個数は, 高々, 多項式

$$\widetilde{w}_{l-1}x^{n-d} + \cdots + \widetilde{w}_0 x^{n-l-d+1} + \widetilde{w}_{n-1}x^{n-l-d} + \cdots + \widetilde{w}_{l+d-1}$$

の次元, すなわち$n-d$である. 従って, $\widetilde{W}(x) = 0$の非零の根で$\mathrm{GF}(2^m)$に含まれるものは高々$n-d$個であることがわかる.

(c)と同様に,

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

であるので, $w_i \quad (0 \le i \le n-1)$のうち0となるものの個数は高々$n-d$個である. つまり, w_iのうち1となるものは少なくともd個あることがわかり, BCH 符号の線形性から, 符号語間の最小距離$d_{\min}$について, $d_{\min} \ge d$であることが示された. ■

12.3 BCH 符号の復号

BCH 符号の復号は次のように行う.

(1) 受信語

$$Y(x) = y_{n-1}x^{n-1} + \cdots + y_1 x + y_0$$

が与えられたとき,

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

によりシンドロームを計算する.

符号多項式を,

$$W(x) = w_{n-1}x^{n-1} + \cdots + w_1 x + w_0$$

誤りパターンを表す多項式を

$$E(x) = e_{n-1}x^{n-1} + \cdots + e_1 x + e_0$$

とすれば,

$$\begin{aligned}Y(x) &= W(x) + E(x) \\ W(\alpha^i) &= 0\end{aligned}$$

であるので,

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

である.

$Y(x^2) = [Y(x)]^2$であるので, $S_{2i} = (S_i)^2$となり, $S_1, S_2, \cdots, S_{2t}$のうち偶数番目のシンドロームS_{2i}の値は, 他のシンドロームS_iの値から計算できる. シンドロームの値がすべて零ならば, 誤りがなかったと判定する.

(2) シンドロームの値のなかに零でないものが含まれていれば, シンドロームから次のように定義される誤り位置方程式:

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

を構成し, その根を求めることによって誤り位置を同定する. ここで, $j_1, j_2, \cdots, j_l$は未知の誤り位置$(l \le t, 0 \le j_1 < j_2 < \cdots < j_l \le n-1)$を表す. $\sigma(z)$の根は$\alpha^{-j_1}, \alpha^{-j_2}, \cdots, \alpha^{-j_l}$であるから, シンドローム$S_1, S_2, \cdots, S_{2t}$からうまく誤り位置方程式を立てることができれば, 例えば, $\sigma(z)$に$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$を順に代入することにより, 誤りの位置$j_1, j_2, \cdots, j_l$をすべて見つけることができる.

以下では, 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j_1, j_2に対する誤り位置方程式を構成する方法を示す.

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,

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

であり,

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

であるので,

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

となる. 以上により,

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

となる.

【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$x^8 + x^7 + x^6 + x^4 + 1$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. もとの入力語は何か？ただし, 誤りは高々2個であると仮定する.

受信語の多項式表現は,

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

である. シンドローム$\{S_1,S_3\}$を計算すると,

$$S_1=\alpha^{14}+\alpha^{13}+\alpha^{12}+\alpha^{7}+\alpha^{6}+\alpha^{5}+\alpha^{4}+\alpha=\alpha^{2}+1=\alpha^{7}$$
$$S_3=\alpha^{42}+\alpha^{39}+\alpha^{36}+\alpha^{21}+\alpha^{18}+\alpha^{15}+\alpha^{12}+\alpha^{3}=\alpha^{7}$$

従って,

$$\left({S_1}^3+S_3\right){S_1}^{-1}=\frac{(\alpha^7)^3+\alpha^7}{\alpha^7}=\frac{\alpha^{21}+\alpha^7}{\alpha^7}=\frac{\alpha^6+\alpha^7}{\alpha^7}=\frac{\alpha^{10}}{\alpha^7}=\alpha^3$$

誤り位置方程式は,

$$\sigma(z)=1+\alpha^7 z+\alpha^3 z^2$$

となる. $\sigma(1),\sigma(\alpha),\sigma(\alpha^2),\cdots,\sigma(\alpha^{14})$を順に計算すると,

$$\sigma(\alpha^0)=1+\alpha^7+\alpha^3=1+(\alpha^3+\alpha+1)+\alpha^3=\alpha$$
$$\sigma(\alpha^1)=1+\alpha^8+\alpha^5=1+(\alpha^2+1)+(\alpha^2+\alpha)=\alpha$$
$$\sigma(\alpha^2)=1+\alpha^9+\alpha^7=1+(\alpha^3+\alpha)+(\alpha^3+\alpha+1)=0$$
$$\sigma(\alpha^3)=1+\alpha^{10}+\alpha^9=1+(\alpha^2+\alpha+1)+(\alpha^3+\alpha)=\alpha^3+\alpha^2=\alpha^6$$
$$\sigma(\alpha^4)=1+\alpha^{11}+\alpha^{11}=1$$
$$\sigma(\alpha^5)=1+\alpha^{12}+\alpha^{13}=1+(\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+1)=\alpha+1=\alpha^4$$
$$\sigma(\alpha^6)=1+\alpha^{13}+\alpha^{15}=1+(\alpha^3+\alpha^2+1)+1=\alpha^3+\alpha^2+1=\alpha^{13}$$
$$\sigma(\alpha^7)=1+\alpha^{14}+\alpha^{17}=1+(\alpha^3+1)+\alpha^2=\alpha^3+\alpha^2=\alpha^6$$
$$\sigma(\alpha^8)=1+\alpha^{15}+\alpha^{19}=1+(\alpha+1)+1=\alpha+1=\alpha^4$$
$$\sigma(\alpha^9)=1+\alpha^{16}+\alpha^{21}=1+\alpha+(\alpha^3+\alpha^2)=\alpha^3+\alpha^2+\alpha+1=\alpha^{12}$$
$$\sigma(\alpha^{10})=1+\alpha^{17}+\alpha^{23}=1+\alpha^2+(\alpha^2+1)=0$$
$$\sigma(\alpha^{11})=1+\alpha^{18}+\alpha^{25}=1+\alpha^3+(\alpha^2+\alpha+1)=\alpha^3+\alpha^2+\alpha=\alpha^{11}$$
$$\sigma(\alpha^{12})=1+\alpha^{19}+\alpha^{27}=1+(\alpha+1)+(\alpha^3+\alpha^2+\alpha+1)=\alpha^3+\alpha^2+1=\alpha^{13}$$
$$\sigma(\alpha^{13})=1+\alpha^{20}+\alpha^{29}=1+(\alpha^2+\alpha)+(\alpha^3+1)=\alpha^3+\alpha^2+\alpha=\alpha^{11}$$
$$\sigma(\alpha^{14})=1+\alpha^{21}+\alpha^{31}=1+(\alpha^3+\alpha^2)+\alpha=\alpha^3+\alpha^2+\alpha+1=\alpha^{12}$$

以上から, $\sigma(z)=(1+\alpha^{-2}z)(1+\alpha^{-10}z)$と分解されることがわかる. ここから,

誤り位置: $\alpha^{-2}=\alpha^{13},\alpha^{-10}=\alpha^{5}$の2か所

入力された符号多項式:$x^{14}+x^{12}+x^{7}+x^{6}+x^{4}+x$ ／ 10100001101001 0

と結論される.