代数系と符号理論　第12回板書プリント

植松友彦 2007.6.19

1　最小多項式（復習）

定理 1 F_p 上のある多項式 $m(x)$ が β を根として持てば、β^p もまた $m(x)$ の根である。

(証明) $p=2$ について証明する ($p\neq 2$ の場合は各自考えよ)。$m(x)$ の次数を n として、

$$m(x)=\sum_{i=0}^{n} m_i x^i$$

とすれば

$$\begin{aligned}
(m(x))^2 &= \sum_{i=0}^{n} m_i^2 x^{2i} + \sum_{i=0}^{n}\sum_{j\neq i} m_i m_j x^{i+j} \\
&= \sum_{i=0}^{n} m_i^2 x^{2i} + \underbrace{\sum_{i=0}^{n}\sum_{j>i} m_i m_j x^{i+j}} + \underbrace{\sum_{i=0}^{n}\sum_{j<i} m_i m_j x^{i+j}} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad = \\
&= \sum_{i=0}^{n} m_i^2 x^{2i} \\
&= \sum_{i=0}^{n} m_i x^{2i} \quad (\because GF(2)\text{ の全ての元は } x^2=x \text{ をみたす}) \\
&= m(x^2)
\end{aligned}$$

従って、$m(\beta)=0$ ならば、$m(\beta^2)=(m(\beta))^2=0$ である。 □

定理 2　β を F_{p^m} の元とするとき、β の最小多項式は

$$m(x)=(x-\beta)(x-\beta^p)(x-\beta^{p^2})\cdots(x-\beta^{p^{l-1}})$$

で与えられる。但し、l は $\beta^{p^l}=\beta$ をみたす最小の正整数である。特に、$\beta\in F_{p^m}$ から $\beta^{p^m}=\beta$ が成り立つので、$l\leq m$ である。

(証明) 再び $p=2$ について証明する。

$$\begin{aligned}
\{m(x)\}^2 &= (x-\beta)^2(x-\beta^2)^2(x-\beta^4)^2\cdots(x-\beta^{2^{l-1}})^2 \\
&= (x^2-\beta^2)(x^2-\beta^4)(x^2-\beta^8)\cdots(x^2-\beta^{2^{l-1}})(x^2-\beta^{2^l}) \\
&= (x^2-\beta^2)(x^2-\beta^4)\cdots(x^2-\beta^{2^{l-1}})(x^2-\beta) \\
&= m(x^2)
\end{aligned}$$

従って、$m(x)=\sum_{i=0}^{n} m_i x^i$ とすると

$$\sum_{i=0}^{n} m_i x^{2i} = m(x^2) = \{m(x)\}^2 = \sum_{i=0}^{n} m_i^2 x^{2i}$$

から、$m_i^2 = m_i \quad (i=0,1,\cdots,n)$ が成り立つ。ここで、m_i は $x^2=x$ の根なので $m_i \in F_2$ であることが分る。 □

例 **1** $\beta \in F_{64}$ とし、β の位数は 21 であるとする。このとき、β の F_2 上の最小多項式 $m_\beta(x)$ は、$\beta^{64}=1$ から

$$m_\beta(x) = (x-\beta)(x-\beta^2)(x-\beta^4)(x-\beta^8)(x-\beta^{16})(x-\beta^{11}) = x^6+x^4+x^2+x+1$$

となる。

他方、β^3 の F_2 上の最小多項式 β^3 は、$\beta^{24}=\beta^3$ から

$$m_{\beta^3}(x) = (x-\beta^3)(x-\beta^6)(x-\beta^{12}) = x^3+x^2+1$$

となる。

2 巡回符号の最小距離について

定理 6.3.1 F_q 上の (n,k) 巡回符号 C の生成多項式 $g(x)$ が根の中に $\beta^a, \beta^{a+1}, \cdots, \beta^{a+d-2}$ をもつとする。ただし、$\beta \in F_{q^m}$ は位数 n の元である。このとき、最小距離 $d_{min}(C) \geq d$ が成り立つ。

例 **6.3.1** 生成多項式

$$g(x) = (x^6+x^4+x^2+x+1)(x^3+x^2+1) = m_\beta(x) m_{\beta^3}(x)$$

をもつ (21,12) 巡回符号を考えよう。但し、$\beta(\in F_{64})$ は位数 21 の元であり、$m_{\beta^j}(x)$ は β^j を根として持つ最小多項式である。このとき、$g(x)$ は根として、

$$\underline{\beta}, \underline{\beta^2}, \beta^3, \underline{\beta^4}, \beta^6, \underline{\beta^8}, \underline{\beta^{11}}, \beta^{12}, \underline{\beta^{16}} \quad \text{(下線は } m_\beta(x) \text{ の根)}$$

を持つので、最小距離は少なくとも 5 である。他方、

$$(x^2+x+1)g(x) = 1+x^3+x^4+x^9+x^{11}$$

は符号語なので、最小距離は 5 である。

3 巡回 RS 符号

α を F_q の原始元、n を $q-1$ の約数とし、

$$\beta = \alpha^{\frac{q-1}{n}}$$

とする。また、

$$x_i = \beta^{i-1}, \quad i=1,2,\cdots,n$$

として、RS 符号 C_s を

$$C_s = \{(f(x_1), \cdots, f(x_n)) : f(x) \in F_q[x] : \deg(f(x)) < s\}$$

によって定める。

定理 6.4.1 RS 符号 C_s は F_q 上の (n, s) 巡回符号であって、その生成多項式は、

$$g(x) = (x - \beta)(x - \beta^2) \cdots (x - \beta^{n-s})$$

である。

(証明)　線形符号であることは明らかなので、巡回符号であることを示す。符号語

$$c = (f(x_1), \cdots, f(x_n)) = (f(\beta^0), f(\beta), \cdots, f(\beta^{n-1}))$$

に対し、その巡回シフト

$$\hat{c} = (f(\beta^{n-1}), f(\beta^0), \cdots, f(\beta^{n-2}))$$

を考える。$f_1(x) = f(\beta^{n-1}x) \in F_q[x]$ とすれば、$\deg(f_1(x)) < s$ であり、$\beta^n = 1$ から

$$\hat{c} = (f_1(\beta^0), f_1(\beta^1), \cdots, f_1(\beta^{n-1})) \in C_s$$

が成り立つ。従って、この符号は巡回符号である。

一方、C_s の一次独立な符号語は、

$$\begin{aligned}
f(x) = 1 &\leftrightarrow (1, 1, \cdots, 1) \\
f(x) = x &\leftrightarrow (1, \beta, \beta^2, \cdots, \beta^{n-1}) \\
f(x) = x^2 &\leftrightarrow (1, \beta^2, \beta^4, \cdots, \beta^{2(n-1)}) \\
&\vdots \\
f(x) = x^{s-1} &\leftrightarrow (1, \beta^{s-1}, \beta^{2(s-1)}, \cdots, \beta^{(s-1)(n-1)})
\end{aligned}$$

であり、これに直交するパリティ検査行列は、補題 5.3.1 から

$$H = \begin{bmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \cdots & \beta^{2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{n-s} & \cdots & \beta^{(n-s)(n-1)} \end{bmatrix}$$

である。これは、全ての符号語多項式が根 $\beta, \beta^2, \cdots, \beta^{n-s}$ をもつことを意味するので、この RS 符号の生成多項式は、

$$g(x) = (x - \beta)(x - \beta^2) \cdots (x - \beta^{n-s})$$

である。　□

4　BCH 符号とその復号法

教科書では、Reed-Solomon 符号の部分体部分符号として BCH 符号を定義しているが、ここでは、以下のように F_p 上の巡回符号として直接定義する。

定義 **(BCH 符号)** α を F_{p^m} の原始元とする。このとき

$$\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$$

の全てを根とする次数最小の多項式 $g(x)$ を生成多項式とする F_p 上の符号長 $n = p^m - 1$ の巡回符号を BCH 符号という。

従って、α^i の F_p 上の最小多項式を $m_i(x)$ とすれば、BCH 符号の生成多項式は、

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

となる。これと定理 6.3.1 から、BCH 符号の最小距離 d は $d \geq 2t + 1$ を満足する。

他方、定理 2 から $\deg m_i(x) \leq m$ が成り立つので

$$\deg g(x) \leq 2tm$$

が成り立つ。特に $p = 2$ のときは、α^i と α^{2i} の最小多項式は一致するので

$$g(x) = \mathrm{LCM}\{m_1(x), m_3(x), \cdots, m_{2t-1}(x)\}$$

としても良い。この場合

$$\deg g(x) \leq tm$$

が成り立つ。 従って、2 元 BCH 符号の次元は $n - mt$ 以上である（非 2 元 BCH 符号の次元は $n - 2mt$ 以上である）。以上をまとめて、BCH 符号のパラメータについて下記の表を得る。

BCH 符号のパラメータ

	$p = 2$	$p \neq 2$
符号長 n	$n = 2^m - 1$	$n = p^m - 1$
情報記号数 k	$k \geq n - mt$	$k \geq n - 2mt$
検査記号数 $n - k$	$n - k \leq mt$	$n - k \leq 2mt$
最小距離 d	$d \geq 2t + 1$	$d \geq 2t + 1$

次に、RS 符号の部分体部分符号として、BCH 符号を特徴付けよう。$q = 2^m$ の場合、RS 符号 C_s に含まれる 2 元符号語の全体を $C_s(sub)$ とする。すなわち、

$$C_s(sub) = C_s \cap F_2^n$$

である。

定理 6.4.2 符号 $C_s(sub)$ は巡回符号であり、生成多項式は、

$$g(x) = \mathrm{LCM}\{m_\beta(x), m_{\beta^2}(x), \cdots, m_{\beta^{n-s}}(x)\}$$

である。この符号は、最小距離 $n - s + 1$ 以上を有する。また、この保証された最小距離 $n - s + 1$ のことを設計距離という。

(証明) 2 つの符号語の和が $C_s(sub)$ に含まれるのは自明。RS 符号が巡回符号であるので、この部分符号も巡回符号である。生成多項式は、$\beta, \beta^2, \cdots, \beta^{n-s}$ を根として持ち、これらの根をもつ最

小次数の 2 元多項式は、最小多項式 $m_\beta(x), m_{\beta^2}(x), \cdots, m_{\beta^{n-s}}(x)$ の最小公倍多項式である。また、定理 6.3.1 から最小距離は $n-s+1$ 以上である。 □

この定理から、BCH 符号が RS 符号の部分体部分符号であり、RS 符号の復号アルゴリズムである Peterson の復号アルゴリズムによって復号できることが分かる。

例 **6.4.1** 原始既約多項式 $x^4+x^3+1=0$ の根を α とし、この既約多項式によって定まる有限体 F_{16} を考える。$\beta=\alpha$ として、$n=15, s=9$ の場合、生成多項式は根として、

$$\beta, \beta^2, \beta^3, \cdots, \beta^{n-s}=\beta^6$$

を根として持つ。

$$m_\beta(x)=m_{\beta^2}(x)=m_{\beta^4}(x)$$

および

$$m_{\beta^3}(x)=m_{\beta^6}(x)$$

に注意すれば、生成多項式は、

$$g(x)=m_\beta(x)m_{\beta^3}(x)m_{\beta^5}(x)=1+x^2+x^5+x^6+x^8+x^9+x^{10}$$

である。従って、符号の次元 k は、

$$k=15-10=5$$

となる。最小距離は 7 以上であるが、$g(x)$ の重みが 7 なので、

$$d_{min}=7$$

である。

受信語 $r(x)=x+x^3+x^4+x^5$ を復号しよう。シンドロームは、

$$\begin{aligned}
S_1 &= r(\alpha)=\alpha+\alpha^3+\alpha^4+\alpha^5=\alpha^3\\
S_2 &= r(\alpha^2)=r(\alpha)^2=\alpha^6\\
S_3 &= r(\alpha^3)=\alpha^6\\
S_4 &= r(\alpha^4)=r(\alpha^2)^2=\alpha^{12}\\
S_5 &= r(\alpha^5)=\alpha^5\\
S_6 &= r(\alpha^6)=r(\alpha^3)^2=\alpha^{12}
\end{aligned}$$

となる。次に連立方程式

$$\begin{bmatrix} S_1 & S_2 & S_3 & S_4\\ S_2 & S_3 & S_4 & S_5\\ S_3 & S_4 & S_5 & S_6 \end{bmatrix} \begin{bmatrix} Q_{1,0}\\ Q_{1,1}\\ Q_{1,2}\\ Q_{1,3} \end{bmatrix} = 0$$

を解いて、

$$Q_{1,0}=\alpha^7, Q_{1,1}=\alpha^8, Q_{1,2}=\alpha^3, Q_{1,3}=1$$

すなわち、

$$Q_1(x)=x^3+\alpha^3x^2+\alpha^8x+\alpha^7$$

を得る。この根は、$\alpha^0, \alpha^{10}, \alpha^{12}$ である。従って、誤り多項式は、

$$e(x) = 1 + x^{10} + x^{12}$$

となり、送信符号語は、

$$c(x) = r(x) - e(x) = 1 + x + x^3 + x^4 + x^5 + x^{10} + x^{12}$$

である。

老婆心: 2 元 BCH 符号の場合、全てのシンドロームは独立ではないことに注意する。受信語多項式 $r(x)$ は F_2 上の多項式なので、

$$r(x^2) = \{r(x)\}^2$$

が成り立つ。従って、

$$S_{2t} \quad = \quad r(\alpha^{2t}) = \{r(\alpha^t)\}^2 = \{S_t\}^2$$

であり、奇数番目のシンドロームのみを計算すれば良い。