代数系と符号理論　第11回板書プリント

植松友彦 2007.6.8

1　巡回符号と生成多項式

定義 6.1.1 F_q 上の (n,k) 線形符号 C で、符号語の巡回シフトが符号語であるとき、符号 C を巡回符号であるという。すなわち、

$$c=(c_0,c_1,\cdots,c_{n-1})\in C \Rightarrow \hat{c}=(c_{n-1},c_0,\cdots,c_{n-2})\in C$$

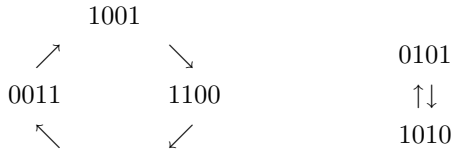
が成り立つ線形符号は巡回符号である。

例 **1** $C=\{(000),(111)\}$ は巡回符号である。

例 **2** 単一パリティ検査符号は巡回符号である。たとえば、符号長 4 の単一パリティ検査符号

$$\begin{aligned}C=\{&(0000),(1001),(0101),(1100),\\&(0011),(1010),(0110),(1111)\}\end{aligned}$$

において、



例 **3** $C=\{(0000),(1000),(0100),(0010),(0001)\}$ は巡回シフトについて閉じているが、

$$(1000)+(0100)=(1100)\notin C$$

であり、線形符号ではないので巡回符号ではない。

巡回符号は、符号語を $F_q[x]$ の多項式で表すと、より理解しやすい。すなわち、

$$\begin{aligned}&F_q\text{ 上の符号語}\quad c=(c_0,c_1,\cdots,c_{n-1})\in F_q^n\\&\qquad\qquad\qquad\qquad\downarrow F_q[x]\text{ の多項式表現}\\&\text{符号語多項式}\quad c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\end{aligned}$$

多項式表現を用いたとき、線形符号 C が巡回符号であるための条件は

$$c(x)\in C\quad\text{ならば}\quad \underbrace{R_{x^n-1}}_{x^{n-1}\text{で割ったときの剰余}}[xc(x)]\in C$$

と書ける。なぜならば

$$\begin{aligned} xc(x) &= c_0x + c_1x^2 + \cdots + c_{n-1}x^n \\ &= c_0x + c_1x^2 + \cdots + c_{n-1}(x^n - 1) + c_{n-1} \end{aligned}$$

から直ちに

$$R_{x^n-1}[xc(x)] = c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}$$

が得られ、これは $c(x)$ の巡回シフトに一致するからである。同様にして

$$R_{x^n-1}[x^ic(x)] = c_{n-i} + c_{n-i+1}x + \cdots + c_{n-i-1}x^{n-1} \in C$$

も成り立つことが分る。一方 C は線形符号なので、$i(x) = \sum_j i_jx^j$ とすれば

$$\begin{aligned} R_{x^n-1}[i(x)c(x)] &= R_{x^n-1}[\sum_j i_jx^jc(x)] \\ &= \sum_j i_jR_{x^n-1}[x^jc(x)] \in C \end{aligned}$$

となる。従って $c(x) \in C$ ならば任意の $i(x) \in F_q[x]$ について

$$R_{x^n-1}[i(x)c(x)] \in C$$

が成り立つ。

定理 6.1.1 C を F_q 上の (n, k) 巡回符号とし、$g(x)$ を $C \setminus \{0\}$ に含まれる次数最小のモニック (最高次数の係数が 1) 多項式とする。このとき、

0. $g(x)$ は一意的に定まる。
1. 全ての $c(x) \in C$ に対し、$g(x)$ は $c(x)$ を割り切る。
2. $g(x)$ は $F_q[x]$ において $x^n - 1$ を割り切る。
3. $k = n - \deg(g(x))$

また、$g(x)$ を生成多項式と呼ぶ。

例 4 巡回符号 $C = \{(000), (111)\}$ の生成多項式は

$$\begin{aligned} (000) &\longrightarrow 0 \\ (111) &\longrightarrow 1 + x + x^2 \end{aligned}$$

から $g(x) = 1 + x + x^2$ である。また、

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

から、生成多項式 $g(x)$ が $x^3 - 1$ を割り切ることが分る。

例 **5** 符号長 4 の単一パリティ検査符号の生成多項式は

$$
\begin{aligned}
&(0000) \longrightarrow 0\\
&(1001) \longrightarrow 1+x^3\\
&(0101) \longrightarrow x+x^3\\
&(1100) \longrightarrow 1+x\\
&(0011) \longrightarrow x^2+x^3\\
&(1010) \longrightarrow 1+x^2\\
&(0110) \longrightarrow x+x^2\\
&(1111) \longrightarrow 1+x+x^2+x^3
\end{aligned}
$$

から $g(x) = 1 + x$ である。また、$x^4 - 1 = (x + 1)^4$ から、生成多項式 $g(x)$ は $x^4 - 1$ を割り切る。

(証明)

1. まず一意性を示す。$g_1(x), g_2(x)$ をモニックな次数最小の 2 つの符号語とすれば、$g(x) = g_1(x) - g_2(x)$ もまた符号語であり、$g(x)$ の次数は $g_1(x)$ の次数よりも低い。従って、$g_1(x)$ の次数最小性から $g(x) = 0$ でなければならない。

2. 次に $g(x)$ が符号語 $c(x)$ を割り切ることを示す。

$$c(x) = q(x)g(x) + r(x) \quad \deg(r(x)) < \deg(g(x))$$

とすると

$$r(x) = c(x) - q(x)g(x)$$

となり、$\deg(q(x)g(x)) < n$ であるから、

$$R_{x^n-1}[q(x)g(x)] = q(x)g(x) \in C$$

であり、$r(x)$ も符号語でなければならない。ここで、$r(x) \neq 0$ とすれば、$g(x)$ の次数最小性に矛盾する。従って、$g(x)$ は $c(x)$ を割り切る。

3.

$$x^n - 1 = q(x)g(x) + r(x) \quad \deg(r(x)) < \deg(g(x))$$

とすると

$$r(x) = R_{x^n-1}[-q(x)g(x)]$$

となり、$r(x)$ は符号語である。$r(x) \neq 0$ とすると、$g(x)$ の次数最小性に矛盾する。従って、$r(x) = 0$ でなければならず、$g(x)$ は $x^n - 1$ を割り切る。

4. $g(x)$ の次数を s とするとき、符号語 $c(x) = a(x)g(x)$ において、$a(x)$ の係数として任意に選べるのは、$n - s$ 個であり、かつ異なる $a(x)$ は異なる $c(x)$ を与えるので、

$$k = n - s = n - \deg(g(x))$$

である。 □

定理 6.1.2 $g(x) \in F_q[x]$ はモニックで、$x^n - 1$ を割り切るとする。このとき、

$$C = \{i(x)g(x) : i(x) \in F_q[x], \deg(i(x)) < n - \deg(g(x))\}$$

は生成多項式 $g(x)$ を有する巡回符号である。

例 6 符号長 21 の 2 元巡回符号を考えよう。

$$x^{21} - 1 = (x-1)(x^6 + x^4 + x^2 + x + 1)(x^3 + x^2 + 1)(x^6 + x^5 + x^4 + x^2 + 1)(x^2 + x + 1)(x^3 + x + 1)$$

から、

$$g(x) = (x^6 + x^4 + x^2 + x + 1)(x^3 + x^2 + 1)$$

を使うと、(21,12)2 元巡回符号を得る。また、

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

を使っても、(21,12)2 元巡回符号を得る。

(証明) C が線形符号であることは明らかであるので、巡回符号であることを示す。

$$h(x) = \frac{x^n - 1}{g(x)} \quad = h_0 + h_1 x + \cdots + h_{n-s} x^{n-s}$$

とおくと、$h(x)$ はモニック多項式である。一方、$c(x) = i(x)g(x)$, $\deg(i(x)) < n - \deg(g(x))$ に対して、

$$\begin{aligned} R_{x^n-1}[xc(x)] &= R_{x^n-1}[xc(x) - c_{n-1}(x^n - 1)] \\ &= R_{x^n-1}[xi(x)g(x) - c_{n-1}h(x)g(x)] \\ &= R_{x^n-1}[(xi(x) - c_{n-1}h(x))g(x)] \end{aligned}$$

ここで、係数 c_{n-1} は、$i(x)$ の最高次数の係数に等しいので、

$$\deg(xi(x) - c_{n-1}h(x)) < n - s$$

であり、

$$R_{x^n-1}[xc(x)] = (xi(x) - c_{n-1}h(x))g(x)$$

と書けるので、C は巡回符号となる。 □

以上のことから、$x^n - 1$ を因数分解することで、巡回符号を構成できることが分る。

2 巡回符号の生成行列とパリティ検査行列

符号 C を F_q 上の (n, k) 巡回符号とする。このとき、C は生成多項式

$$g(x) = g_0 + g_1 x + \cdots x^{n-k}$$

を有する。また、$x^j g(x)\ j = 0, 1, \cdots, k-1$ が一次独立な符号語を与えることも分っている。これらの符号語をベクトルで表すと

$$\begin{aligned} g(x) &\leftrightarrow (g_0, g_1, \cdots, g_{n-k-1}, 1, 0, \cdots, 0) \\ xg(x) &\leftrightarrow (0, g_0, g_1, \cdots, g_{n-k-1}, 1, 0, \cdots, 0) \\ x^2 g(x) &\leftrightarrow (0, 0, g_0, g_1, \cdots, g_{n-k-1}, 1, 0, \cdots, 0) \\ &\vdots \\ x^{k-1} g(x) &\leftrightarrow (0, \cdots, 0, g_0, g_1, \cdots, g_{n-k-1}, 1) \end{aligned}$$

となり、これらのベクトルを並べることで生成行列

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

が得られる。

一方、パリティ検査行列を得る為には、

$$g(x)h(x) = x^n - 1$$

に着目する。任意の $k-1$ 次以下の多項式 $i(x)$ について、符号語は

$$c(x) = i(x)g(x)$$

と書けるので、

$$c(x)h(x) = i(x)g(x)h(x) = i(x)(x^n - 1) = i(x)x^n - i(x)$$

が得られ、$c(x)h(x)$ の次数 $k, k+1, k+2, \cdots, n-1$ の項は零である。すなわち、

$$c(x)h(x) \text{ の } j \text{ 次の係数} = \sum_{i=0}^{j} c_i h_{j-i} = 0, \quad j = k, k+1, \cdots, n-1$$

が成り立つ。

従って、ベクトル

$$\begin{gathered} (h_k, h_{k-1}, \cdots, h_0, 0, \cdots, 0) \\ (0, h_k, h_{k-1}, \cdots, h_0, 0, \cdots, 0) \\ (0, 0, h_k, h_{k-1}, \cdots, h_0, 0, \cdots, 0) \\ \vdots \\ (0, \cdots, 0, h_k, h_{k-1}, \cdots, h_0) \end{gathered}$$

が $n-k$ 個の一次独立なパリティ検査を与えるので，パリティ検査行列は

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & h_0 \end{bmatrix}$$

H はその第 1 行に $h(x)$ の係数を逆順に並べ、さらに残りの $n-k-1$ 個の行に第 1 行の巡回シフトを順に並べたものである。次の定理は明らかである。

定理 6.2.1 C が生成多項式 $g(x)$ をもつ (n,k) 巡回符号ならば、双対符号 $C^{\perp}$ もまた巡回符号であって、生成多項式

$$g^{\perp}(x) = h_k + h_{k-1}x + h_{k-2}x^2 + \cdots + h_0 x^k$$

を持つ。ここで、

$$h_0 + h_1 x + h_2 x^2 + \cdots + h_k x^k = \frac{x^n - 1}{g(x)}$$

である。

他方、$g(x)$ が F_{q^n} 内に根 $x_1, x_2, \cdots, x_{n-k}$ を有したとする。このとき、任意の符号語は、$c(x) = i(x)g(x)$ と書けるから、

$$c(x_j) = c_0 + c_1 x_j + c_2 x_j^2 + \cdots + c_{n-1} x_j^{n-1} = 0, \quad j = 1, 2, \cdots, n-k$$

が成り立つ。これから、

$$H = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_{n-k} & x_{n-k}^2 & \cdots & x_{n-k}^{n-1} \end{bmatrix}$$

もまた、パリティ検査行列となる。

例 6.2.1 生成多項式 $g(x) = 1 + x^2 + x^3 + x^4$ を有する (7,3) 巡回符号について

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

が成り立つ。また、$g(x) = (x+1)(x^3 + x + 1)$ である。そこで、既約多項式 $p(x) = x^3 + x + 1$ の根を β とし、$p(x)$ によって有限体 F_8 を定めると、$g(x)$ の根は、$\beta^0, \beta, \beta^2, \beta^4$ と書ける。従って、

$$H = \begin{bmatrix} 1 & \beta^0 & \beta^0 & \cdots & \beta^0 \\ 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \beta^4 & \cdots & \beta^{2(n-1)} \\ 1 & \beta^4 & \beta^8 & \cdots & \beta^{4(n-1)} \end{bmatrix}$$

もまたパリティ検査行列である。