

10 第10回

10.1 巡回符号

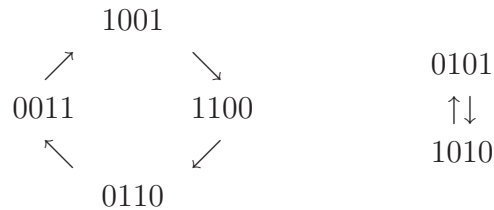
有限体 F 上の線形符号で、符号語の巡回シフトもまた符号語であるような符号 C を巡回符号と呼ぶ。すなわち C を巡回符号とすれば $(v_0, v_1, \dots, v_{n-1}) \in C$ ならば $(v_{n-1}, v_0, \dots, v_{n-2}) \in C$ である。

[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。

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

なぜなら



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

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

であり、線形符号ではないので巡回符号ではない。

10.2 巡回符号の多項式表現

$$F \text{ 上の符号語 } \mathbf{v} = (v_0, v_1, \dots, v_{n-1}) \in F^n$$

↓ 多項式表現

$$\text{符号語多項式 } v(x) = v_0 + v_1x + \dots + v_{n-1}x^{n-1}$$

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

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

と書ける。なぜならば

$$\begin{aligned} xv(x) &= v_0x + v_1x^2 + \cdots + v_{n-1}x^n \\ &= v_0x + v_1x^2 + \cdots + v_{n-1}(x^n - 1) + v_{n-1} \end{aligned}$$

から直ちに

$$R_{x^n-1}[xv(x)] = v_{n-1} + v_0x + v_1x^2 + \cdots + v_{n-2}x^{n-1}$$

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

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

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

$$\begin{aligned} R_{x^n-1}[i(x)v(x)] &= R_{x^n-1}\left[\sum_j i_j x^j v(x)\right] \\ &= \sum_j i_j R_{x^n-1}[x^j v(x)] \in C \end{aligned}$$

となる。従って $v(x) \in C$ ならば任意の $i(x) \in \underline{F[x]}$ について

F 上の多項式の集合

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

が成り立つ。

10.3 生成多項式

定理 F 上の巡回符号 C があり、 $g(x) \in C$ をモニックな次数最小の符号語とする。このとき、 $g(x)$ は一意に定まり、任意の符号語 $v(x) \in C$ を割り切る。このような $g(x)$ を生成多項式と呼ぶ。

(証明) 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。

次に $g(x)$ が $v(x)$ を割り切ることを示す。

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

とすると

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

となり、 $r(x)$ 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 $v(x)$ を割り切る。

[例 1] 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 $1 + x + x^2$ である。

[例 2] 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 $1 + x$ である。

定理 23 F 上の符号長 n の巡回符号の生成多項式 $g(x)$ は $x^n - 1$ を割り切る。また逆に、 $g(x)$ を $x^n - 1$ を割り切る任意のモニック多項式とすると

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

は巡回符号となる。

(証明) 再び

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

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。

次に逆を示す。 $v_1(x), v_2(x) \in C$ すなわち、ある $i_1(x), i_2(x) \in F[x]$ に対して

$$\begin{aligned}v_1(x) &= R_{x^n-1}[i_1(x)g(x)] \\ v_2(x) &= R_{x^n-1}[i_2(x)g(x)]\end{aligned}$$

とすれば、 $\alpha_1, \alpha_2 \in F$ に対して

$$\begin{aligned}\alpha_1 v_1(x) + \alpha_2 v_2(x) &= \alpha_1 R_{x^n-1}[i_1(x)g(x)] + \alpha_2 R_{x^n-1}[i_2(x)g(x)] \\ &= R_{x^n-1}[\alpha_1 i_1(x)g(x) + \alpha_2 i_2(x)g(x)] \\ &= R_{x^n-1}[(\alpha_1 i_1(x) + \alpha_2 i_2(x))g(x)] \in C\end{aligned}$$

となる。他方

$$R_{x^n-1}[xv_1(x)] = R_{x^n-1}[xi_1(x)g(x)] \in C$$

であるので、 C は巡回符号となる。

[例 1] $C = \{(000), (111)\}$ の場合

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

から、生成多項式 $g(x) = x^2 + x + 1$ が $x^3 - 1$ を割り切ることが分る。

[例 2] 符号長 4 の単一パリティ検査符号の場合、 $x^4 - 1 = (x + 1)^4$ から、生成多項式 $g(x) = x + 1$ は $x^4 - 1$ を割り切る。

10.4 巡回符号の生成行列

$g(x)$ を F 上の符号長 n の巡回符号 C の生成多項式とし、 $\deg g(x) = n - k$ とする。このとき、任意の $v(x) \in C$ に対し、 $\deg v(x) < n$ が成り立つので、

$$C = \{i(x)g(x) | i(x) \in F[x], \deg i(x) < k\}$$

と書ける。従って、 $g(x) = \sum_{i=0}^{n-k} g_i x^i$ とすれば

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

は C の基底となる。従って、 C の生成行列 G は

$$G = \left[\begin{array}{ccccccc} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{array} \right] \left. \vphantom{\begin{array}{ccccccc} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{array}} \right\} k$$

で与えられる。

このように情報系列を表す多項式 $i(x) = i_0 + i_1x + \cdots + i_{k-1}x^{k-1}$ に対し、符号語を $i(x)g(x)$ で定めた場合、この符号は非組織符号となる。そこで、組織符号とする為に、次の対応を考える。

$$x^{n-k}i(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x)$$

とする。このとき

$$v(x) = x^{n-k}i(x) - r(x) = q(x)g(x)$$

は n 次未満の多項式であり、かつ $g(x)$ で割り切れるので符号語である。しかも、 $\deg r(x) < n - k$ であるので、 $v(x)$ の $n - k$ 次から $n - 1$ 次までの係数は情報系列 $(i_0, i_1, \dots, i_{k-1})$ と一致するので、組織符号である。

[例] $GF(2)$ 上で、 $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ と因数分解されるので、 $g(x) = x^3 + x + 1$ を生成多項式とする符号長 $n = 7$ の巡回符号を考える。 $i(x) = x + 1$ とすれば、 $n - k = 3$ なので、

$$x^{n-k}i(x) = x^3(x + 1) = x^4 + x^3$$

を考え、 $x^4 + x^3$ を $g(x)$ で割った商と余りを求めると

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

となる。従って

$$v(x) = 1 + x^2 + x^3 + x^4$$

が符号語となる。