巡回符号の課題

2022 年 7 月 18 日

1　$n = 5$ の巡回符号

生成多項式 $g(x)$ は $1 + x^n$ の因数なので、

$$1 + x^5 = (1 + x)(1 + x + x^2 + x^3 + x^4)$$

より、$g(x)$ の候補は $1+x$ と $1+x+x^2+x^3+x^4$ である。$g(x) = 1+x$ のときの全ての符号を表 1 に示す。表 1 より、$g(x) = 1+x$ のときの最小ハミング距離は 2 である。$g(x) = 1+x+x^2+x^3+x^4$

表 1　$g(x) = 1 + x$ の符号

00000				
00011	00110	01100	11000	10001
00101	01010	10100	01001	10010
01111	11110	11101	11011	10111

のとき、符号は 00000 と 11111 のみなので、最小ハミング距離は 5 である。

2　$n = 6$ の巡回符号

生成多項式 $g(x)$ は $1 + x^n$ の因数なので、

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

より、$g(x)$ の候補を k の昇順に並べると表 2 になる。

表 2　$n = 6$ の巡回符号の生成多項式

k	$g(x)$
1	$(1+x)(1+x+x^2)^2$
2	$(1+x+x^2)^2$
2	$(1+x)^2(1+x+x^2)$
3	$(1+x)(1+x+x^2)$
4	$1+x+x^2$
4	$(1+x)^2$
5	$1+x$

3　$g(x) = (1+x)(1+x^2+x^3)$ の巡回符号の生成行列

$n = 7$ の場合、$g(x)$ の次数が 4 なので、情報源の長さは 3 である。$g(x)$ を展開すると $1 + x + x^2 + x^4$ となり、生成行列は 1 行目が $x^2 g(x)$, 2 行目が $xg(x)$, 3 行目が $g(x)$ になるので、

$$\boldsymbol{G} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

となる。これを組織符号に変換すると

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$