

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 (8, 4) 組織符号

$$p_0 = u_1 + u_2 + u_3$$

$$p_1 = u_0 + u_1 + u_2$$

$$p_2 = u_0 + u_1 + u_3$$

$$p_3 = u_0 + u_2 + u_3$$

3.1 生成行列

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

3.2 パリティ検査行列

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (1)$$

3.3 最小ハミング距離

表 3 より、0 ベクトル以外の符号の最小ハミング重みが 4 なので、最小ハミング距離は 4 である。

表 3 情報源と符号の対応

情報源	符号
0000	00000000
0001	00011011
0010	00101101
0011	00110110
0100	01001110
0101	01010101
0110	01100011
0111	01111000
1000	10000111
1001	10011100
1010	10101010
1011	10110001
1100	11001001
1101	11010010
1110	11100100
1111	11111111

3.4 訂正できる誤りパターン

訂正できる誤りパターン数は、0 誤りを含むと

$$2^{n-k} = 2^{8-4} = 2^4 = 16$$

である。誤りパターンは表 4 のように選択できる。

表 4 訂正できる誤りパターンの一例

00000000	00000001	00000010	00000100
00001000	00010000	00100000	01000000
10000000	00000011	00000110	00001010
00010010	00100010	01000010	10000010

3.5 符号化回路

図 1 に示す。

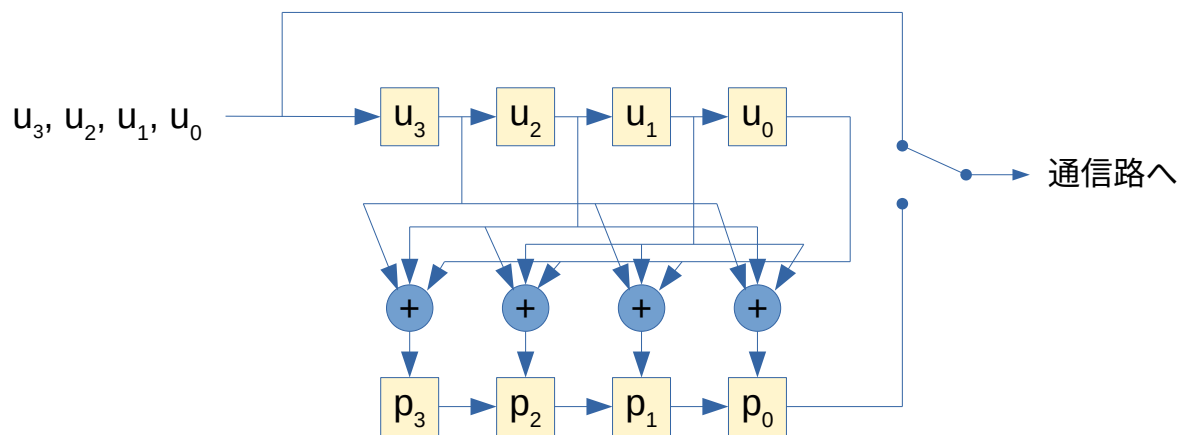


図 1 符号化回路

3.6 シンドローム計算回路

図 2 に示す。

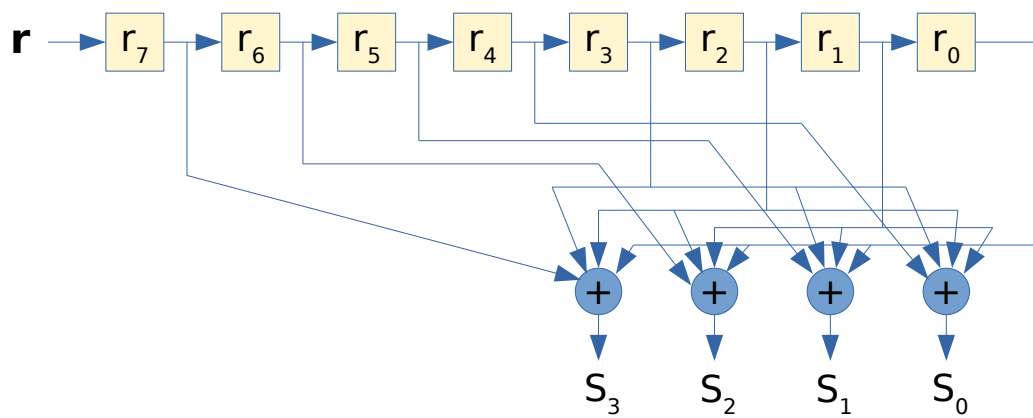


図 2 シンドローム計算回路

3.7 重み分布と誤りを検出できない確率

表 3 より、重み分布は表 5 となる。

表 5 重み分布

i	0	4	8
A_i	1	14	1

$p = 0.01$ のとき、誤りを検出できない確率は

$$\begin{aligned}
 P_U(E) &= \sum_{i=1}^n A_i p^i (1-p)^{n-i} \\
 &= 14p^4(1-p)^4 + 1p^8(1-p)^0 \\
 &\simeq 1.345 \times 10^{-7}
 \end{aligned}$$

3.8 双対符号

(1) の検査行列 \mathbf{H} を組織符号に変換すると、

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

より、生成行列 \mathbf{G} と等しくなる。

4 (7,4) ハミング符号の復号誤り率の上限

BSC における復号誤り率の上限は

$$P_{\max}(E) = \sum_{i=t+1}^n \binom{n}{i} p^i (1-p)^{n-i}$$

なので、(7,4) ハミング符号の場合

$$P_{\max}(E) = \sum_{i=2}^7 \binom{7}{i} p^i (1-p)^{7-i}$$

である。二項定理より、

$$\begin{aligned}
 1^n &= ((1-p) + p)^n = \sum_{i=0}^n \binom{n}{i} p^i (1-p)^{n-i} \\
 &= \sum_{i=0}^t \binom{n}{i} p^i (1-p)^{n-i} + \sum_{i=t+1}^n \binom{n}{i} p^i (1-p)^{n-i}
 \end{aligned}$$

となるので、

$$\begin{aligned}
 P_{\max}(E) &= \sum_{i=2}^7 \binom{7}{i} p^i (1-p)^{7-i} = 1 - \sum_{i=0}^1 \binom{7}{i} p^i (1-p)^{7-i} \\
 &= 1 - (1p^0(1-p)^7 + 7p^1(1-p)^6) = 1 - (1-p)^6(1-6p)
 \end{aligned}$$

と簡略化できる。これを $10^{-5} \leq p \leq 10^{-1}$ の範囲でプロットしたものが図 3 である。

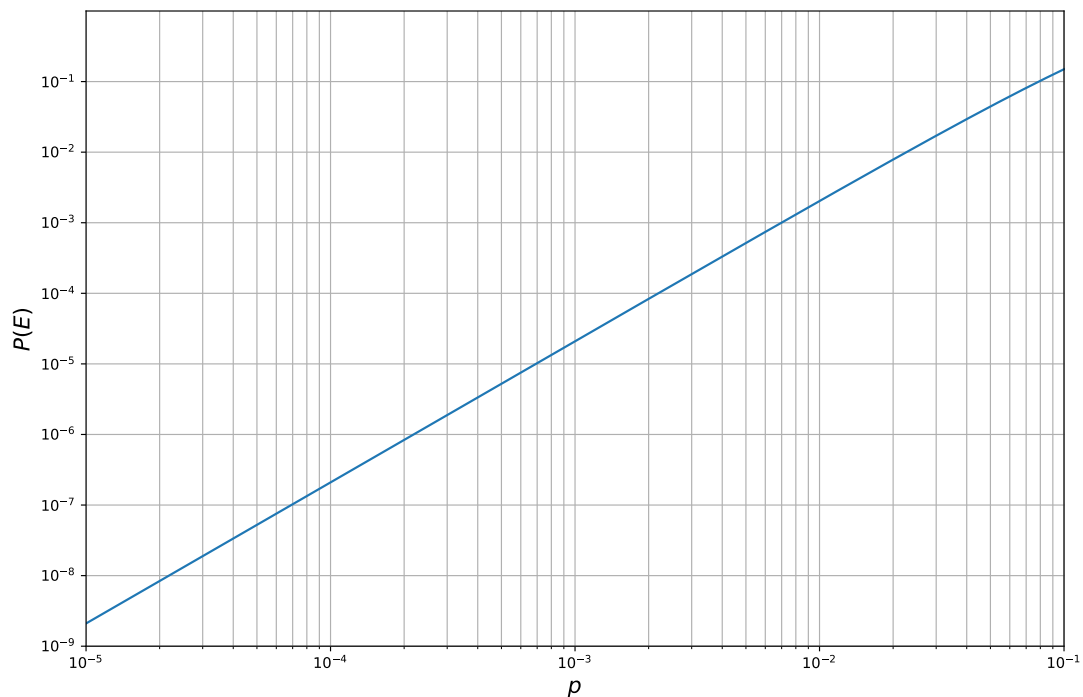


図3 (7,4) ハミング符号の復号誤り率の上限

5 $d_{\min} \geq 2t + 1$ の (n,k) 線形符号の場合

符号長 n の符号で、各誤りビット数の誤りパターン数を整理すると表6になる。なお、 ${}_nC_t$ は $\binom{n}{t}$ と同じ意味なので $\binom{n}{t}$ に統一する。表6より、 t ビット以下の誤りパターン数は

表6 誤りビット数と誤りパターン数

誤りビット数	誤りパターン数
0	$\binom{n}{0}$
1	$\binom{n}{1}$
2	$\binom{n}{2}$
\vdots	\vdots
t	$\binom{n}{t}$
\vdots	\vdots
n	$\binom{n}{n}$

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}$$

である。 $d_{\min} \geq 2t + 1$ の符号は t ビット以下の誤りを全て訂正可能であり、 (n,k) 線形符号が訂正可能な誤りパターン数は 2^{n-k} なので、

$$2^{n-k} \geq \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots \binom{n}{t}$$

$$\therefore n - k \geq \log_2 \left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots \binom{n}{t} \right)$$