巡回符号の課題

2022 年 7 月 19 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 $x^2g(x)$, 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

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

4　$g(x)=1+x^2+x^3$ の (7,4) 巡回符号

4.1　符号化回路とその動作

$g(x)=1+x^2+x^3$ の (7,4) 巡回符号の符号化回路を図 1 に示す。この回路に入力情報 $u(x)=1+x^2$ を入れたときの動作を表 3 に示す。情報の長さは 4 なので、入力の順番は 0101 である。

4.2　シンドローム計算回路

シンドローム計算回路を図 2 に示す。受信語が $r(x)=x^2+x^4+x^5$ の場合の回路の動作を表 4 に示す。シンドロームが最終的に 0 になったので誤りなし。また、$r(x)=x^2g(x)$ であることからも、誤りがないことが分かる。

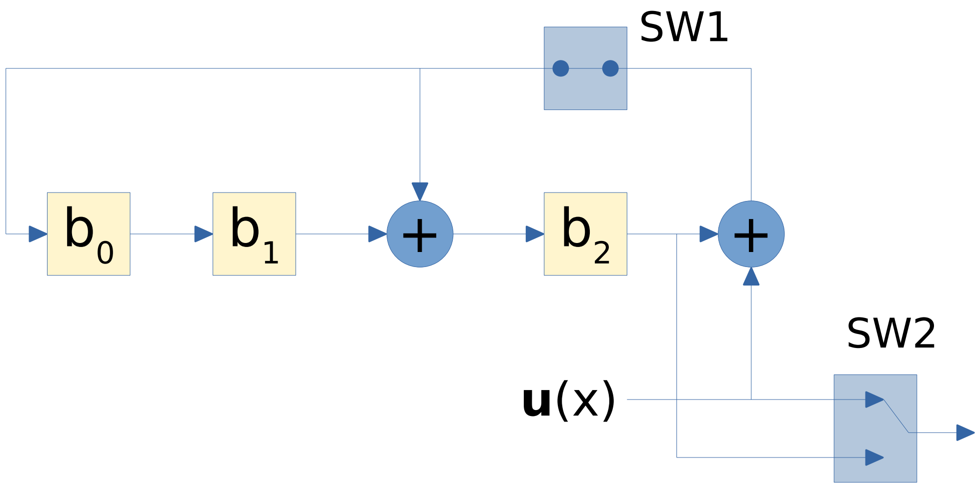

図 1　符号化回路

表 3　$u(x) = 1 + x^2$ を入れたときの動作

	入力	b_0	b_1	b_2	出力
	-	0	0	0	-
	0	0	0	0	0
SW1: 閉	1	1	0	1	1
SW2: 上	0	1	1	1	0
	1	0	1	1	1
SW1: 開	-	0	0	1	1
SW2: 下	-	0	0	0	1
	-	0	0	0	0

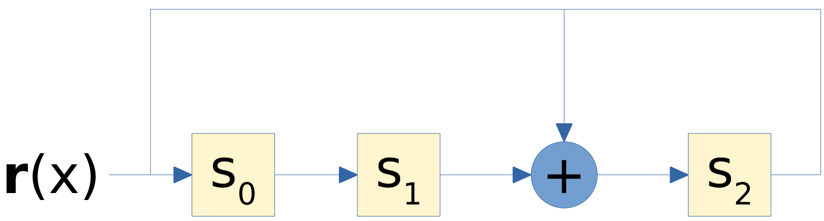

図 2　シンドローム計算回路

表 4　$r(x) = x^2 + x^4 + x^5$ を入れたときの動作

入力	s_0	s_1	s_2
-	0	0	0
0	0	0	0
1	1	0	0
1	1	1	0
0	0	1	1
1	0	0	0
0	0	0	0
0	0	0	0

5　$g(x) = 1 + x + x^4$ の (15, 11) ハミング符号

符号化回路を図 3 に示す。

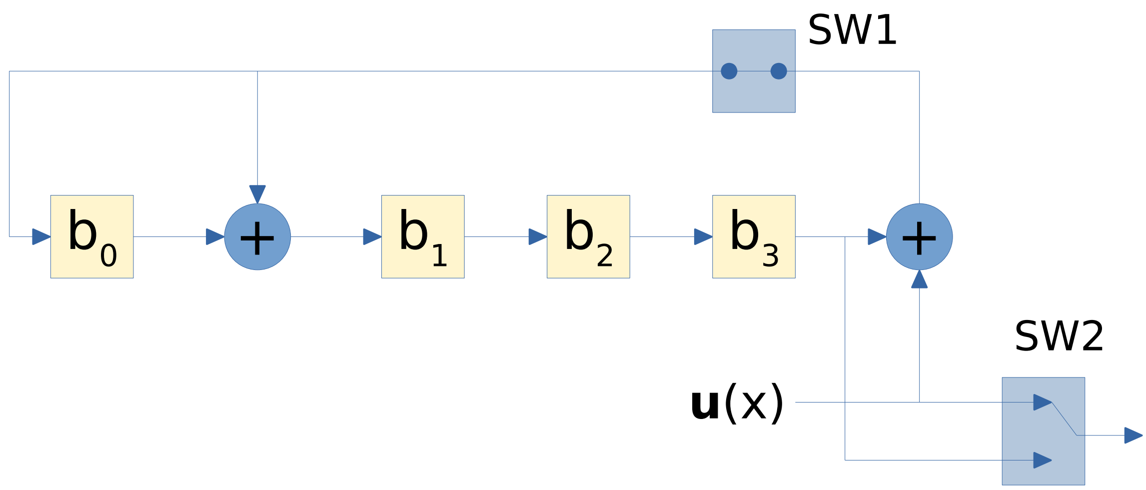

図 3　$g(x) = 1 + x + x^4$ の (15, 11) ハミング符号の符号化回路

復号回路では x^{n-1} のシンドロームだけ探せばよいので、

$$x^{14} = (1 + x + x^4)(1 + x + x^2 + x^4 + x^6 + x^7 + x^{10}) + (1 + x^3)$$

より、$1 + x^3$ で 1 になる論理回路を使う。復号回路を図 4 に示す。

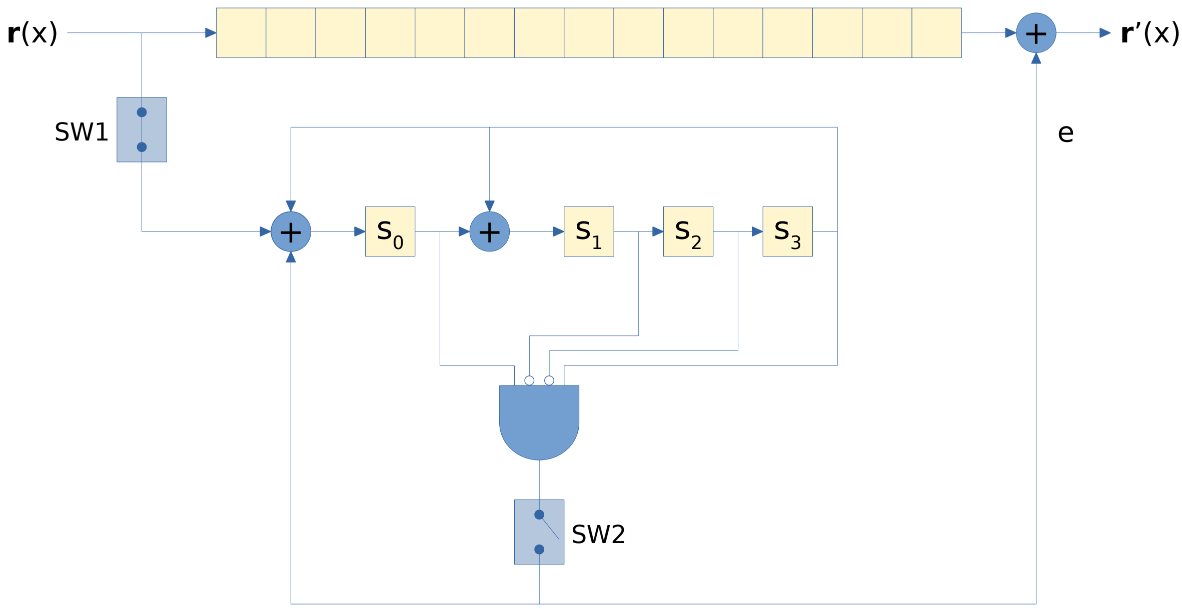

図 4　$g(x) = 1 + x + x^4$ の (15, 11) ハミング符号の復号回路

6　生成多項式が $g(x)$、長さ n の符号

6.1　$(1 + x)$ が $g(x)$ の因数であれば、奇数重みの符号語が存在しないことを示せ

$g(x)$ が $(1 + x)$ を因数に持つとき、$g(x) = (1 + x)a(x)$ と表せる。$g(x)$ に $x = 1$ を代入すると

$$g(1) = (1 + 1)a(1) = 0$$

となる。符号語 $w(x)$ は $g(x)$ で割り切れるので $w(x) = b(x)g(x)$ と表せ、

$$w(1) = b(1)g(1) = 0$$

となる。1 を代入して 0 になる多項式は項数が偶数なので、符号語は必ず偶数重みになる。つまり、$(1 + x)$ が $g(x)$ の因数であれば、奇数重みの符号語が存在しない。

6.2　n が奇数で、$(1 + x)$ が $g(x)$ の因数でない場合、符号語の一つは (111...1) であることを示せ。

$(1 + x)$ は $(1 + x^n)$ の因数であり、

$$1 + x^n = (1 + x)(1 + x + x^2 + \cdots + x^{n-1})$$

と因数分解できる。$g(x)$ は $(1+x^n)$ の因数であるため、$(1+x)$ が $g(x)$ の因数でないとき、$g(x)$ は $(1+x+x^2+\cdots+x^{n-1})$ の因数である。$g(x)$ で割り切れる多項式は符号語なので、$(1+x+x^2+\cdots+x^{n-1})$ (ベクトル表現: 111...1) も符号語である。

補足

$$
\begin{aligned}
1+x^n &= (1+x)(1+x+x^2+\cdots+x^{n-1}) \\
&= (1+x)a(x)b(x)c(x)\cdots
\end{aligned}
$$

であり、$(1+x)$ が $g(x)$ の因数でない。つまり $g(x)$ は $(1+x)$ で割り切れず、

$$
g(x) \neq (1+x)q(x) \tag{1}
$$

なので、

$$
\begin{array}{cccccccccc}
 & s(x) & = & 1 & +x & +x^2 & +\cdots & +x^{n-1} & \\
+) & xs(x) & = & & x & +x^2 & +\cdots & +x^{n-1} & +x^n \\
\hline
 & (1+x)s(x) & = & 1 & & & & & +x^n
\end{array}
$$

6.3 $(1+x^i)$ が $g(x)$ で割り切れる一番小さい値 i が n である場合、最小ハミング距離が 3 以上であることを示せ。

$(1+x^i)$ が $g(x)$ で割り切れるような i の最小値を $g(x)$ の周期という。$g(x)$ の周期を n とし、ハミング重みが 2 の符号が存在すると仮定する。