# 情報理論
# 第 14 回 線型符号と巡回符号

**堀田 政二**
**工学部 情報工学科**

# 線型符号 (linear code)

情報ビット数が $4$，検査ビット数が $3$ からなる $7$ ビットのハミング符号は

$$\boldsymbol{w} = (w_1, w_2, ..., w_7) = (x_1, x_2, x_3, x_4, c_1, c_2, c_3) = (\boldsymbol{x}, \boldsymbol{c})$$

として与えられる．ここで，検査ビットは

$$c_1 = x_1 \oplus x_2 \oplus x_3$$
$$c_2 = x_2 \oplus x_3 \oplus x_4$$
$$c_3 = x_1 \oplus x_2 \oplus x_4$$

として与えられたことを思い出そう．このように，検査ビットの値が情報ビットの線型な関数で定められる符号を線型符号という

**線型符号の特徴**

任意の二つの符号をビットごとに $\oplus$ で加算してやると，それがまた符号になる

(2)

# $(7,4)$ ハミング符号は線型符号

**情報ビット数が $4$，検査ビット数が $3$ からなる $7$ ビットのハミング符号**

| 符号語 | 情報ビット | 検査ビット | $\oplus$ の例 |
|---|---|---|---|
| $w_0$ | 0000 | 000 | |
| $w_1$ | 0001 | 011 | $w_{14} \oplus w_{15}$ |
| $w_2$ | 0010 | 110 | $w_1 \oplus w_3$ |
| $w_3$ | 0011 | 101 | $w_1 \oplus w_2$ |
| $w_4$ | 0100 | 111 | $w_1 \oplus w_5$ |
| $w_5$ | 0101 | 100 | $w_1 \oplus w_4$ |
| $w_6$ | 0110 | 001 | $w_1 \oplus w_7$ |
| $w_7$ | 0111 | 010 | $w_3 \oplus w_4$ |
| $w_8$ | 1000 | 101 | $w_7 \oplus w_{15}$ |
| $w_9$ | 1001 | 110 | $w_1 \oplus w_8$ |
| $w_{10}$ | 1010 | 011 | $w_1 \oplus w_{11}$ |
| $w_{11}$ | 1011 | 000 | $w_1 \oplus w_{10}$ |
| $w_{12}$ | 1100 | 010 | $w_{11} \oplus w_{15}$ |
| $w_{13}$ | 1101 | 001 | $w_1 \oplus w_{12}$ |
| $w_{14}$ | 1110 | 100 | $w_2 \oplus w_{12}$ |
| $w_{15}$ | 1111 | 111 | $w_1 \oplus w_{14}$ |

(3)

# ハミング符号の行列表現

7 ビットのハミング符号
$\boldsymbol{w} = (w_1, w_2, ..., w_7) = (x_1, x_2, x_3, x_4, c_1, c_2, c_3)$ は，情報ビット
$\boldsymbol{x} = (x_1, x_2, x_3, x_4)$ と $4 \times 7$ の生成行列 (generator matrix)

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

により $w = xG$ として与えられる．すなわち，$(n, k)$ ハミング符号の符号語 $w$ $(1 \times n)$ は情報ビット $x$ $(1 \times k)$ と $k \times n$ の生成行列 $G$ の積で与えられる．ただし，長さが $n$ の二つのベクトル
$\boldsymbol{a} = (a_1, ..., a_n)$ と $\boldsymbol{b} = (b_1, ..., b_n)$ の内積は
$\boldsymbol{ab}^\top = (a_1 \times b_1) \oplus (a_2 \times b_2) \oplus \cdots \oplus (a_n \times b_n)$ で与えられる

# 生成行列の構成

| 誤り箇所 | 誤りパターン | | | | | | | シンドローム | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | x1 | x2 | x3 | x4 | c1 | c2 | c3 | s1 | s2 | s3 |
| なし | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 左から1桁 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 左から2桁 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 左から3桁 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 左から4桁 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 左から5桁 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 左から6桁 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 左から7桁 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |

$4 \times 7$ の生成行列 $G$ は $4 \times 4$ の単位行列 $I_k$ と，エラーテーブルで誤りの生じている場合のシンドローム上位 4 つを並べた $4 \times 3$ 行列

$$\boldsymbol{P} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

を並べたもの $G = [I_k, P]$ である．この $P$ は情報検査ビット関連行列と呼ばれるもので $c = xP$ が成り立つ (5)

# パリティ検査行列 (parity check matrix)

**生成行列 $G = [I_k, P]$ に対して，次の形の行列 $H = [P^\top, I_{n-k}]$ をパリティ検査行列，あるいは単に検査行列と呼ぶ:**

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

**この行列により，シンドロームを並べた $(n-k) \times 1$ のベクトル $s = (s_1, s_2, ..., s_{n-k})$ は，$1 \times n$ の受信符号 $y = (y_1, y_2, ..., y_n)$ と検査行列の転置 $H^\top$ を用いて $s = yH^\top$ により与えられる**

# 生成行列と検査行列の演算例

情報ビットが $x = 0101$ で与えられたとする．ハミング符号 $w$ は

$$w = xG = (0,1,0,1) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0,1,0,1,1,0,0)$$

もし，誤りなくハミング符号が受信されたとする．すなわち $y = w$ とすると，検査行列からシンドロームは

$$s = yH^{\top} = (0,1,0,1,1,0,0) \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (0,0,0)$$

となる．一方，$y = (1,1,0,1,1,0,0) = w \oplus (1,0,0,0,0,0,0)$ と最初のビットが誤って受信されたとすると $s = (1,0,1)$ ($H^{\top}$ の 1 行目) となり最初のビットが誤っていることが分かる (7)

# 生成行列と検査行列の関係

生成行列は $G = [I_k, P]$，検査行列は $H = [P^\top, I_{n-k}]$ で与えられるが，これらに対して $GH^\top$ を計算すると

$$\boldsymbol{GH^\top = [I_k, P][P^\top, I_{n-k}]^\top = P \oplus P = O}$$

となる．ここで $O$ は $k \times (n-k)$ の要素がすべて $0$ の行列である

$$\boldsymbol{GH^\top} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

この関係が満たされるように符号語を作成すれば，$H$ を検査行列として用いることができる (8)

# 巡回符号 (cyclic code)

## 巡回置換 (cyclic shift)

**ある長さ $n$ の符号語が与えられたとき，最上位のシンボルを最下位に移動させて符号をずらす処理を，符号語の巡回シフトという:**

$$(w_{n-1}, w_{n-2}, \ldots, w_1, w_0) \Rightarrow (w_{n-2}, \ldots, w_1, w_0, w_{n-1})$$

**符号語を巡回置換させたものが，再び符号語になるような符号を巡回符号という**

**【例】$(7,4)$ ハミング符号では**

$$\boldsymbol{w}_1 \to \boldsymbol{w}_2 \to \boldsymbol{w}_5 \to \boldsymbol{w}_{11} \to \boldsymbol{w}_6 \to \boldsymbol{w}_{12} \to \boldsymbol{w}_8 \to \boldsymbol{w}_1$$

$$\boldsymbol{w}_3 \to \boldsymbol{w}_7 \to \boldsymbol{w}_{14} \to \boldsymbol{w}_{13} \to \boldsymbol{w}_{10} \to \boldsymbol{w}_4 \to \boldsymbol{w}_9 \to \boldsymbol{w}_3$$

**といった巡回が見られる**

# 符号の多項式表現

巡回符号を簡単に表現するために，符号と多項式を対応させることを考える．すなわち，長さ $n$ の符号語

$$\boldsymbol{w} = (w_{n-1}, w_{n-2}, \ldots, w_1, w_0)$$

を係数が 1，または 0 の多項式で表すことにする．すなわち，

$$F(\boldsymbol{x}) = w_{n-1}x^{n-1} + w_{n-2}x^{n-2} + \cdots + w_1 x^1 + w_0$$

という $(n-1)$ 次の多項式で表す．このように，符号語に対応する多項式を符号多項式 (code polynominal) と呼ぶ

【例】

$$\boldsymbol{w}_1 : 0001011 \rightarrow F_1(\boldsymbol{x}) = x^3 + x + 1$$

$$\boldsymbol{w}_2 : 0010110 \rightarrow F_2(\boldsymbol{x}) = x^4 + x^2 + x$$

このように多項式表現をすると，左にシフトすることは，多項式に $x$ を掛けることに相当する．ただし，左から溢れ出たビットは右に戻す（これは $x^7$ を 1 とすることに相当）

(10)

# $(7,4)$ ハミング符号の多項式表現

| 多項式 | 情報ビット | 検査ビット | 多項式表現 |
|---|---|---|---|
| $F_0$ | 0000 | 000 | $0$ |
| $F_1$ | 0001 | 011 | $x^3+x+1$ |
| $F_2$ | 0010 | 110 | $x^4+x^2+x$ |
| $F_3$ | 0011 | 101 | $x^4+x^3+x^2+1$ |
| $F_4$ | 0100 | 111 | $x^5+x^2+x+1$ |
| $F_5$ | 0101 | 100 | $x^5+x^3+x^2$ |
| $F_6$ | 0110 | 001 | $x^5+x^4+1$ |
| $F_7$ | 0111 | 010 | $x^5+x^4+x^3+x$ |
| $F_8$ | 1000 | 101 | $x^6+x^2+1$ |
| $F_9$ | 1001 | 110 | $x^6+x^3+x^2+x$ |
| $F_{10}$ | 1010 | 011 | $x^6+x^4+x+1$ |
| $F_{11}$ | 1011 | 000 | $x^6+x^4+x^3$ |
| $F_{12}$ | 1100 | 010 | $x^6+x^5+x$ |
| $F_{13}$ | 1101 | 001 | $x^6+x^5+x^3+1$ |
| $F_{14}$ | 1110 | 100 | $x^6+x^5+x^4+x^2$ |
| $F_{15}$ | 1111 | 111 | $x^6+x^5+x^4+x^3+x^2+x+1$ |

(11)

# 生成多項式 (generator polynominal)

$(7,4)$ **ハミング符号において，** $F_1(\boldsymbol{x}) = x^3 + x + 1$ **はすべての多項式の因数になっている (排他的論理和の演算であることに注意):**

$$
\begin{aligned}
F_2(\boldsymbol{x}) &= x^4 + x^2 + x = xF_1(\boldsymbol{x}) \\
F_3(\boldsymbol{x}) &= x^4 + x^3 + x^2 + 1 = (x+1)F_1(\boldsymbol{x}) \\
F_4(\boldsymbol{x}) &= x^5 + x^2 + x + 1 = (x^2+1)F_1(\boldsymbol{x}) \\
&\vdots \\
F_{15}(\boldsymbol{x}) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x^2 + 1)F_1(\boldsymbol{x})
\end{aligned}
$$

**このように，すべての符号多項式を割り切ることができる** $n-k$ **次多項式で，かつ** $x^n + 1$ **の因数であるものを生成多項式と呼び** $G(\boldsymbol{x})$ **で表す．** $G(\boldsymbol{x})$ **を用いれば，各符号多項式は** $F(\boldsymbol{x}) = G(\boldsymbol{x})Q(\boldsymbol{x})$ **と因数の積で表すことができる**

(12)

# 巡回符号の生成手順

**巡回符号では，$(n-1)$ 次の生成多項式 $G(x)$ と $k$ 個の情報ビット $(d_{k-1}, d_{k-2}, ..., d_0)$ が与えられたとき，次の手順で長さ $n$ の符号語を求める**:

- **情報ビットだけからなる $(k-1)$ 次多項式を $p(x) = d_{k-1}x^{k-1} + d_{k-2}x^{k-2} + \cdots + d_0$ とする**
- **両辺に $x^{n-k}$ (検査ビット数の多項式) を掛ける**:

$$x^{n-k}p(x) = d_{k-1}x^{n-1} + d_{k-2}x^{n-2} + \cdots + d_0x^{n-k}$$

- **$x^{n-k}p(x)$ を $G(x)$ で割った商を $Q(x)$，余りを $R(x)$ とすると**

$$x^{n-k}p(x) = Q(x)G(x) + R(x)$$

- **したがって $F(x) = Q(x)G(x) = x^{n-k}p(x) + R(x)$**

(13)

# 巡回符号の生成例

**生成多項式が** $G(\boldsymbol{x}) = x^3 + x + 1$ **の時，長さ** $4$ **の情報ビット** $0101$ **に対応する長さ** $n = 7$ **の符号語を求めてみよう**

- **情報ビットだけからなる多項式は** $p(\boldsymbol{x}) = x^2 + 1$
- **両辺に** $x^3$ **を掛ける**: $x^3 p(\boldsymbol{x}) = x^5 + x^3$
- $x^3 p(\boldsymbol{x})$ **を** $G(\boldsymbol{x})$ **で割った商は** $Q(\boldsymbol{x}) = x^2$**，余りも** $R(\boldsymbol{x}) = x^2$ **となる**
- **求めたい符号多項式は** $F(\boldsymbol{x}) = G(\boldsymbol{x})Q(\boldsymbol{x}) = x^3 p(\boldsymbol{x}) + R(\boldsymbol{x}) = x^5 + x^3 + x^2$ **となる．したがって，対応する符号語は** $0101100$

# 巡回符号の誤り検出

符号多項式 $F(x)$ を受信したときの多項式を $F'(x)$ とする．誤りがない場合には

$$F'(\boldsymbol{x}) = F(\boldsymbol{x}) = G(\boldsymbol{x})Q(\boldsymbol{x})$$

となる．今，通信路の雑音によって 1 ビットの誤りが発生したとすると，誤りも雑音信号なので，次の多項式 $N(x) = x^i \ (i = 0, ..., n-1)$ によって表すことができる．したがって，受信信号は

$$F'(\boldsymbol{x}) = F(\boldsymbol{x}) + N(x) = G(\boldsymbol{x})Q(\boldsymbol{x}) + x^i$$

となる．これを $G(x)$ で割ると，誤りがない場合は 0，そうでない場合は 0 とはならない．その余りは $x^i$ を $G(\boldsymbol{x})$ で割った $n-k-1$ 次の多項式 $E(x)$ となる．これまでの例では $E(x)$ は次の二次の多項式

$$E(\boldsymbol{x}) = s_2x^2 + s_1x + s_0$$

となるので，その係数の組み合わせによって誤り訂正が可能である (ハミング符号のシンドロームと同じ)

# 巡回符号の誤り検出と訂正の例

**生成多項式が $G(x) = x^3 + x + 1$ の時，長さ $4$ の情報ビット $0101$ に対応する長さ $n = 7$ の符号語は $0101100$ であった．このうち，$1$ ビット目が $0 \to 1$ に誤ったとしよう $(1101100)$．すると，受信される多項式は**

$$F'(x) = x^6 + x^5 + x^3 + x^2$$

**となる．これを $G(x)$ で割ると**

$$F'(x) = G(x)(x^3 + x^2 + x + 1) + x^2 + 1$$

**となる．これから**

$$E(x) = 1 \times x^2 + 0 \times x + 1$$

**となっていることから，係数の組み合わせ $101$ より $1$ ビット目が誤っていることが分かる．そのため，訂正は $1$ ビット目を反転させればよい**

(16)

# 問題

- 【14.1】垂直水平パリティ符号も線型符号である．垂直水平パリティ符号の生成行列，および検査行列を求めよ．
- 【14.2】$(7,4)$ ハミング符号の検査行列が次のように与えられているとする

$$\boldsymbol{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

この時，次の受信符号に対するシンドロームを計算し，誤りがある場合には誤り訂正を行え

$$\boldsymbol{y}_1 = 1110111,\ \boldsymbol{y}_2 = 0111101$$

- 【14.3】$(7,4)$ ハミング符号の生成多項式を $G(\boldsymbol{x}) = x^3 + x + 1$ とする．受信側の多項式が $F'(\boldsymbol{x}) = x^5 + x$ の時，誤りが生じているかどうか答えよ．また，誤りが生じている場合には誤り訂正を行え (17)