## Hamming 符号

$c \geq 1$

$F_q{}^c$ 内で原点を通る直線の本数 $n = \dfrac{q^c - 1}{q - 1}$

ここから方向ベクトル $\boldsymbol{h}_i$ を $1$ 本づつ選ぶと
どの $2$ 本も同一直線上にない
$\longrightarrow \boldsymbol{h}_i$ 達の線型従属系は最小 $3$ 本

$H := (\boldsymbol{h}_1 \cdots \boldsymbol{h}_n)$

$\mathcal{C}$ : $H$ をパリティ検査行列とする符号

$\cdots$ **Hamming 符号** $\longrightarrow d = 3, t = 1$

# パリティ検査行列と最小距離 (再掲)

$H$ : $\mathcal{C}$ のパリティ検査行列　　とするとき

**最小距離** $d =$
($H$ **の線型従属な列ベクトルの個数の最小値**)

## 演習問題

**(1)** $3$ **次の** $2$ **元 Hamming 符号** $\mathcal{H}$ **は** $[7,4]$**-符号である。パリティ検査行列 (の一つ)** $H$ **を構成せよ。**

**(2)** $\mathcal{H}$ **の生成行列 (の一つで** $GH^T = O$ **となるような)** $G$ **を求めよ。**

**(3)** $w(\boldsymbol{e}) = 1$ **なる** $\boldsymbol{e} \in \boldsymbol{F}_2{}^7$ **を列挙し、そのシンドローム** $\boldsymbol{e}H^T$ **との対照表を作れ。**

**(4) 符号語** $\boldsymbol{x} \in \mathcal{H}$ **を適当に一つ生成し、適当に** $1$ **箇所だけ変えた (誤りを入れた) 語** $\boldsymbol{y} \in \boldsymbol{F}_2{}^7$ **について、シンドローム** $\boldsymbol{y}H^T$ **を計算せよ。また、正しく復号すると元の** $\boldsymbol{x} \in \mathcal{H}$ **が得られることを確かめよ。**

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

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

**符号語の例：**

**情報語** $\boldsymbol{s} = (1\ 0\ 0\ 1)$

$$\longmapsto \boldsymbol{x} = \boldsymbol{s}G = (1\ 0\ 0\ 1\ 1\ 0\ 0)$$

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

| $\boldsymbol{e}$ | $\boldsymbol{e}H^T$ |
|---|---|
| $\boldsymbol{e}_1$ | $(1\ 1\ 1)$ |
| $\boldsymbol{e}_2$ | $(1\ 1\ 0)$ |
| $\boldsymbol{e}_3$ | $(1\ 0\ 1)$ |
| $\boldsymbol{e}_4$ | $(0\ 1\ 1)$ |
| $\boldsymbol{e}_5$ | $(1\ 0\ 0)$ |
| $\boldsymbol{e}_6$ | $(0\ 1\ 0)$ |
| $\boldsymbol{e}_7$ | $(0\ 0\ 1)$ |

**符号語** $\boldsymbol{x} = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が**
1 **箇所誤って**

$$\boldsymbol{y} = (1\ 0\ 1\ 1\ 1\ 0\ 0)$$

**と受信されたとせよ。**

$$\boldsymbol{y}H^T = (1\ 0\ 1) = \boldsymbol{e}_3 H^T$$

$\longrightarrow$ $\boldsymbol{y} - \boldsymbol{e}_3 = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が正しい符号語**

$\longrightarrow$ **情報語は** $(1\ 0\ 0\ 1)$

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

| $\boldsymbol{e}$ | $\boldsymbol{e}H^T$ |
|---|---|
| $\boldsymbol{e}_1$ | $(1\ 1\ 1)$ |
| $\boldsymbol{e}_2$ | $(1\ 1\ 0)$ |
| $\boldsymbol{e}_3$ | $(1\ 0\ 1)$ |
| $\boldsymbol{e}_4$ | $(0\ 1\ 1)$ |
| $\boldsymbol{e}_5$ | $(1\ 0\ 0)$ |
| $\boldsymbol{e}_6$ | $(0\ 1\ 0)$ |
| $\boldsymbol{e}_7$ | $(0\ 0\ 1)$ |

**符号語** $\boldsymbol{x} = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が**
1 **箇所誤って**

$$\boldsymbol{y} = (1\ 0\ 1\ 1\ 1\ 0\ 0)$$

**と受信されたとせよ。**

$$\boldsymbol{y}H^T = (1\ 0\ 1) = \boldsymbol{e}_3 H^T$$

$\longrightarrow$ $\boldsymbol{y} - \boldsymbol{e}_3 = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が正しい符号語**

$\longrightarrow$ **情報語は** $(1\ 0\ 0\ 1)$

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

| $\boldsymbol{e}$ | $\boldsymbol{e}H^T$ |
|---|---|
| $\boldsymbol{e}_1$ | $(1\ 1\ 1)$ |
| $\boldsymbol{e}_2$ | $(1\ 1\ 0)$ |
| $\boldsymbol{e}_3$ | $(1\ 0\ 1)$ |
| $\boldsymbol{e}_4$ | $(0\ 1\ 1)$ |
| $\boldsymbol{e}_5$ | $(1\ 0\ 0)$ |
| $\boldsymbol{e}_6$ | $(0\ 1\ 0)$ |
| $\boldsymbol{e}_7$ | $(0\ 0\ 1)$ |

**符号語** $\boldsymbol{x} = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が**
1 **箇所誤って**

$$\boldsymbol{y} = (1\ 0\ 1\ 1\ 1\ 0\ 0)$$

**と受信されたとせよ。**

$$\boldsymbol{y}H^T = (1\ 0\ 1) = \boldsymbol{e}_3 H^T$$

$\longrightarrow$ $\boldsymbol{y} - \boldsymbol{e}_3 = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が正しい符号語**

$\longrightarrow$ **情報語は** $(1\ 0\ 0\ 1)$

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

| $\boldsymbol{e}$ | $\boldsymbol{e}H^T$ |
|---|---|
| $\boldsymbol{e}_1$ | $(1\ 1\ 1)$ |
| $\boldsymbol{e}_2$ | $(1\ 1\ 0)$ |
| $\boldsymbol{e}_3$ | $(1\ 0\ 1)$ |
| $\boldsymbol{e}_4$ | $(0\ 1\ 1)$ |
| $\boldsymbol{e}_5$ | $(1\ 0\ 0)$ |
| $\boldsymbol{e}_6$ | $(0\ 1\ 0)$ |
| $\boldsymbol{e}_7$ | $(0\ 0\ 1)$ |

**符号語** $\boldsymbol{x} = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が**
1 **箇所誤って**

$$\boldsymbol{y} = (1\ 0\ 1\ 1\ 1\ 0\ 0)$$

**と受信されたとせよ。**

$$\boldsymbol{y}H^T = (1\ 0\ 1) = \boldsymbol{e}_3 H^T$$

$\longrightarrow \boldsymbol{y} - \boldsymbol{e}_3 = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が正しい符号語**

$\longrightarrow$ **情報語は** $(1\ 0\ 0\ 1)$

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

| $\boldsymbol{e}$ | $\boldsymbol{e}H^T$ |
|---|---|
| $\boldsymbol{e}_1$ | $(1\ 1\ 1)$ |
| $\boldsymbol{e}_2$ | $(1\ 1\ 0)$ |
| $\boldsymbol{e}_3$ | $(1\ 0\ 1)$ |
| $\boldsymbol{e}_4$ | $(0\ 1\ 1)$ |
| $\boldsymbol{e}_5$ | $(1\ 0\ 0)$ |
| $\boldsymbol{e}_6$ | $(0\ 1\ 0)$ |
| $\boldsymbol{e}_7$ | $(0\ 0\ 1)$ |

**符号語** $\boldsymbol{x} = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が**
1 **箇所誤って**

$$\boldsymbol{y} = (1\ 0\ 1\ 1\ 1\ 0\ 0)$$

**と受信されたとせよ。**

$$\boldsymbol{y}H^T = (1\ 0\ 1) = \boldsymbol{e}_3 H^T$$

$\longrightarrow$ $\boldsymbol{y} - \boldsymbol{e}_3 = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が正しい符号語**

$\longrightarrow$ **情報語は** $(1\ 0\ 0\ 1)$

さて、“良い” 符号であるためには、

符号語が “均等” に散らばっているのが
望ましかった。

平行移動で重なる $\longrightarrow$ 線型符号

もっと “対称性” が高いと良いのでは ？

“対称性” $\longrightarrow$ 符号の自己同型

さて、“良い” 符号であるためには、

符号語が “均等” に散らばっているのが
望ましかった。

平行移動で重なる $\longrightarrow$ 線型符号

もっと “対称性” が高いと良いのでは ？

“対称性” $\longrightarrow$ 符号の自己同型

さて、“良い” 符号であるためには、

符号語が “均等” に散らばっているのが
望ましかった。

平行移動で重なる $\longrightarrow$ 線型符号

もっと “対称性” が高いと良いのでは ？

“対称性” $\longrightarrow$ 符号の**自己同型**

# 等距離線型自己同型 (再掲)

$V = (V, d)$ : 距離付き線型空間

$f : V \longrightarrow V$ : **等距離線型自己同型**

$\Longleftrightarrow$ $f$ : 線型自己同型で距離を保つ

$(d(f(\boldsymbol{x}), f(\boldsymbol{y})) = f(\boldsymbol{x}, \boldsymbol{y}))$

$d$ : Hamming 距離の場合には、

$\Longleftrightarrow$ $f$ : 線型自己同型で重みを保つ

$(w(f(\boldsymbol{x})) = w(\boldsymbol{x}))$

# 等距離線型自己同型 (再掲)

$V = (V, d)$ **の等距離線型自己同型全体は**
**群を成す** $\cdots \mathrm{Aut}(V, d)$

$\mathrm{Aut}(V, d)$ **は次の** $2$ **種で生成される:**

- **符号語の位置の置換**
  **(生成行列の列の置換)**
- **或る位置の非零定数倍**
  **(生成行列の或る列の非零定数倍)**

$$\mathrm{Aut}(V, d) = \mathfrak{S}_n \wr \boldsymbol{F}_q{}^{\times} = \mathfrak{S}_n \ltimes \left(\boldsymbol{F}_q{}^{\times}\right)^n$$

# 符号の同値 (再掲)

**符号** $\mathcal{C}, \mathcal{C}' \subset V$ **が同値 (equivalent)**

$$\overset{\leftarrow}{\Longleftrightarrow} \exists f \in \mathrm{Aut}(V, d) : \mathcal{C}' = f(\mathcal{C})$$

**同値な符号は、**

**誤り訂正に関して同様の性質を持つ**

# 符号の自己同型

$\mathcal{C}$：符号 $\subset V = \boldsymbol{F}_q{}^n$

$f$：$\mathcal{C}$ の**自己同型 (automorphism)**

$$\Longleftrightarrow f : V \longrightarrow V \text{：等距離線型自己同型で } f(\mathcal{C}) = \mathcal{C}$$

**その全体は群を成す** $\cdots \mathrm{Aut}(\mathcal{C})$

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V, d) = \mathfrak{S}_n \wr \boldsymbol{F}_q{}^{\times}$$

## 符号の自己同型

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V,d) = \mathfrak{S}_n \wr \boldsymbol{F}_q{}^{\times}$$

**特に、$q = 2$ のときは、**

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V,d) = \mathfrak{S}_n$$

**$\longrightarrow$ 対称群の有限体上の線型表現の問題に**

**典型的な場合:**

$\sigma = (1\ 2\ \cdots\ n) \in \mathrm{Aut}(\mathcal{C})$ **のとき**

$\cdots$ **巡回符号 (cyclic code)**

## 符号の自己同型

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V,d) = \mathfrak{S}_n \wr \boldsymbol{F}_q{}^{\times}$$

**特に、$q = 2$ のときは、**

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V,d) = \mathfrak{S}_n$$

$\longrightarrow$ **対称群の有限体上の線型表現の問題に**

**典型的な場合:**

$\sigma = (1\ 2\ \cdots\ n) \in \mathrm{Aut}(\mathcal{C})$ **のとき**

$\cdots$ 巡回符号 (cyclic code)

## 符号の自己同型

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V,d) = \mathfrak{S}_n \wr \boldsymbol{F}_q{}^{\times}$$

**特に、$q = 2$ のときは、**

$$\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(V,d) = \mathfrak{S}_n$$

$\longrightarrow$ **対称群の有限体上の線型表現の問題に**

**典型的な場合:**

$\sigma = (1\ 2\ \cdots\ n) \in \mathrm{Aut}(\mathcal{C})$ **のとき**

$\cdots$ **巡回符号 (cyclic code)**

# 巡回符号

**線型符号 $\mathcal{C}$ が 巡回符号 (cyclic code)**

$$\Longleftrightarrow \sigma = (1\ 2\ \cdots\ n) \in \mathrm{Aut}(\mathcal{C})$$

$$\Longleftrightarrow \quad 「(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Longrightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}」$$

## 巡回符号

$$\sigma = (1\ 2\ \cdots\ n) \in \mathfrak{S}_n, \quad \sigma^n = 1$$

$$\boldsymbol{F}_q[\langle\sigma\rangle] \simeq \boldsymbol{F}_q[X]/(X^n - 1) =: R \curvearrowright V = {\boldsymbol{F}_q}^n$$

**により、$V$ : 階数 $1$ の自由 $R$-加群**

$$V = {\boldsymbol{F}_q}^n \ \simeq \ R$$

$$(1, 0, \ldots, 0) \leftrightsquigarrow 1$$

$$(c_0, c_1, \ldots, c_{n-1}) \leftrightsquigarrow c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

## 巡回符号

$V$ : 階数 $1$ の自由 $R$-加群 $\supset \mathcal{C}$　　に対し、

$\mathcal{C}$ : 巡回符号 $\iff \mathcal{C}$ : 部分 $R$-加群

$V \simeq R$ と同一視するとき

$\iff \mathcal{C}$ : $R$ の ideal

---

$R$ : 可換環 に対し、

$$I : R \text{ の ideal} \overset{\leftarrow}{\iff} \begin{cases} \bullet\ \forall a, b \in I : a + b \in I \\ \bullet\ \forall a \in I, \forall r \in R : ra \in I \end{cases}$$

## 巡回符号

$\mathcal{C}$ : **巡回符号**

$\longleftrightarrow$ $R = \boldsymbol{F}_q[X]/(X^n - 1)$ **の ideal** $I$

$\longleftrightarrow$ $\widetilde{I} \supset (X^n - 1)$ **なる** $\boldsymbol{F}_q[X]$ **の ideal** $\widetilde{I}$

**(**$\boldsymbol{F}_q[X]$ **: PID なので** $\exists f \in R : \widetilde{I} = (f)$**)**

$\longleftrightarrow$ $f | (X^n - 1)$ **なる** $f \in \boldsymbol{F}_q[X]$

$X^n - 1 \in \boldsymbol{F}_q[X]$ **の分解が判れば、**
**巡回符号が分類・構成できる !!**

## 巡回符号

$X^n - 1 = g(X)h(X) \in \boldsymbol{F}_q[X]$ **のとき、**

$$\mathcal{C} := gR \text{：巡回符号} \simeq \boldsymbol{F}_q[X]/(h)$$
$$= \{c(X) \in R | h(X)c(X) = 0 \text{ in } R\}$$

$g$：**生成元多項式 (generator polynomial)**

$h$：**検査多項式 (check polynomial)**

---

$X^n - 1 \in F_q[X]$ **の分解はどうなるのか ？**

$\longrightarrow$ **有限体の拡大・Galois 理論**

## 巡回符号

$X^n - 1 = g(X)h(X) \in \boldsymbol{F}_q[X]$ **のとき、**

$$\mathcal{C} := gR \text{：巡回符号} \simeq \boldsymbol{F}_q[X]/(h)$$
$$= \{c(X) \in R | h(X)c(X) = 0 \text{ in } R\}$$

$g$：**生成元多項式 (generator polynomial)**

$h$：**検査多項式 (check polynomial)**

---

$X^n - 1 \in \boldsymbol{F}_q[X]$ **の分解はどうなるのか？**

$\longrightarrow$ **有限体の拡大・Galois 理論**

## $X^\ell - 1 \in \boldsymbol{F}_q[X]$ の既約分解

$q = 2$, $n = \ell$ : **奇素数のとき、**

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

$$X^5 - 1 = (X+1)(X^4+X^3+X^2+X+1)$$

$$X^7 - 1 = (X+1)(X^3+X+1)(X^3+X^2+1)$$

$$X^{11} - 1 = (X+1)(X^{10}+X^9+\cdots+X+1)$$

$$X^{13} - 1 = (X+1)(X^{12}+X^{11}+\cdots+X+1)$$

$$X^{17} - 1 = (X+1)(X^8+X^5+X^4+X^3+1)$$
$$(X^8+X^7+X^6+X^4+X^2+X+1)$$

$$X^{19} - 1 = (X+1)(X^{18}+X^{17}+\cdots+X+1)$$

## $X^\ell - 1 \in \boldsymbol{F}_q[X]$ の既約分解

$$X^{23} - 1 = (X+1)$$
$$(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)$$
$$(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)$$
$$X^{29} - 1 = (X+1)(X^{28} + X^{27} + \cdots + X + 1)$$
$$X^{31} - 1 = (X+1)(X^5 + X^2 + 1)(X^5 + X^3 + 1)$$
$$(X^5 + X^3 + X^2 + X + 1)$$
$$(X^5 + X^4 + X^2 + X + 1)$$
$$(X^5 + X^4 + X^3 + X + 1)$$
$$(X^5 + X^4 + X^3 + X^2 + 1)$$
$$X^{37} - 1 = (X+1)(X^{36} + X^{35} + \cdots + X + 1)$$