線型符号

$T = \boldsymbol{F}_q$: 有限体にとる

$V = \boldsymbol{F}_q^n$: $\boldsymbol{F}_q$ 上の線型空間の構造を持つ

$\mathcal{C}$: V の部分線型空間のとき

$\mathcal{C}$: **線型符号**と呼ぶ

線型符号の不変量

$k := \dim_{\boldsymbol{F}_q} \mathcal{C}$ **：** $\mathcal{C}$ **の** $\boldsymbol{F}_q$ **上の次元**

符号語数 $M = \#\mathcal{C} = q^k$ $\longrightarrow$ $[n, k]$**-符号**

$w(\boldsymbol{x}) := \#\{i \,|\, x_i \neq 0\}$ **：** $\boldsymbol{x} \in V$ **の重み (weight)**

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

最小距離 $d = d(\mathcal{C}) = \min\{w(\boldsymbol{x}) \,|\, \boldsymbol{x} \in \mathcal{C}, \boldsymbol{x} \neq 0\}$

$\longrightarrow$ $[n, k, d]$**-符号**

線型符号の不変量

$R := \dfrac{k}{n}$: **伝送レート**

$\delta := \dfrac{d}{n}$

$\longrightarrow$ R, δ : **共に大きくしたい (相反する要求)**

線型符号の表示

$$\mathcal{C} \subset V = \boldsymbol{F}_q^n = \{\boldsymbol{x} = (x_1, \ldots, x_n) \,|\, x_i \in \boldsymbol{F}_q\}$$

$$\dim_{\boldsymbol{F}_q} \mathcal{C} = k$$

$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$: $\mathcal{C}$ の基底 (の 1 組)

$$\boldsymbol{v}_i = (a_{i1}, \ldots, a_{in})$$

$$G := \begin{pmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{k1} & \cdots & a_{kn} \end{pmatrix} \in M(k, n; \boldsymbol{F}_q)$$

: $\mathcal{C}$ の 生成行列 (generator matrix)

符号語の生成 (符号化)

$$G := \begin{pmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{k1} & \cdots & a_{kn} \end{pmatrix} \in M(k, n; \boldsymbol{F}_q)$$

: $\mathcal{C}$ の生成行列

$$\mathcal{C} = \{\boldsymbol{v}G \,\big|\, \boldsymbol{v} \in \boldsymbol{F}_q^k\}$$

$$\varphi_G : \boldsymbol{F}_q^k \xrightarrow{\sim} \mathcal{C} \subset V = \boldsymbol{F}_q^n$$

$$\boldsymbol{s} = (s_1, \ldots, s_k) \longmapsto \boldsymbol{s}G = s_1\boldsymbol{v}_1 + \cdots + s_k\boldsymbol{v}_k$$

符号語の検査

受信語 $y \in V$ が正しい符号語かどうか
($y \in \mathcal{C}$ かどうか) 検査する

$$\pi_{\mathcal{C}} : V \longrightarrow V/\mathcal{C} \simeq \boldsymbol{F}_q^{n-k}$$ **: 標準射影**

$V/\mathcal{C}$ の適当な基底を取って
(同型 $V/\mathcal{C} \simeq \boldsymbol{F}_q^{n-k}$ を選んで)
$\pi_{\mathcal{C}}$ を行列表示する

符号語の検査

$$\varphi_A : V = \boldsymbol{F}_q^n \longrightarrow \boldsymbol{F}_q^{n-k}$$
$$\boldsymbol{y} \longmapsto \boldsymbol{y}A$$

$$\boldsymbol{y} \in \mathcal{C} \Longleftrightarrow \varphi_A(\boldsymbol{y}) = \boldsymbol{y}A = 0$$

通常、

転置行列 $H = A^T \in M(n-k, n; \boldsymbol{F}_q)$ **で表示**

: $\mathcal{C}$ **の パリティ検査行列**

(parity-check matrix)

$$\boxed{\boldsymbol{y} \in \mathcal{C} \Longleftrightarrow \boldsymbol{y}H^T = 0}$$

復号 (誤り訂正)

$$y \notin \mathcal{C} \Longleftrightarrow yH^T \neq 0$$

yH^T : y の シンドローム (syndrome)

正しい符号語 $x \in \mathcal{C}$ をどう見付けるか ?

$\Longleftrightarrow$ 誤りベクトル $e := y - x$ をどう求めるか?

復号 (誤り訂正)

- $\boldsymbol{y} \equiv \boldsymbol{y}' \pmod{\mathcal{C}} \Longleftrightarrow \boldsymbol{y}H^T = \boldsymbol{y}'H^T$
- $\boldsymbol{y} \equiv \boldsymbol{e} \pmod{\mathcal{C}}$
- $w(\boldsymbol{e}) \leq t$ **(仮定)**

に注意

- $w(\boldsymbol{e}) \leq t$ **なる** $\boldsymbol{e} \in V$ **を予めリストアップ**
  $\longrightarrow \boldsymbol{e}H^T$ **の表を持っておく**
- **受信語** $\boldsymbol{y} \in V$ **に対し、**
  $\boldsymbol{y}H^T = \boldsymbol{e}H^T$ **なる** $\boldsymbol{e}$ **を表から探す**

$\longrightarrow$ **これを如何に効率良く行なうか**

等距離線型同型

$V = (V, d)$：**距離付き線型空間**

$f : V \longrightarrow V$：**等距離線型同型**

$\Longleftrightarrow$ f：**線型同型で距離を保つ**

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

d：**Hamming 距離の場合には、**

$\Longleftrightarrow$ f：**線型同型で重みを保つ**

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

等距離線型同型

$V = (V, d)$ **の等距離線型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

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

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

同値な符号は、

誤り訂正に関して同様の性質を持つ

符号の標準形

必要なら同値な符号で取替えることにより、

$[n,k]$-符号は次の形の

生成行列 G・パリティ検査行列 H を持つ

$$G = (I_k | P), \quad H = \left(-P^T \middle| I_{n-k}\right)$$

$$(P \in M(k, n-k; \boldsymbol{F}_q), GH^T = O)$$

このとき、

$$\varphi_G : \boldsymbol{F}_q^k \xrightarrow{\sim} \mathcal{C} \subset V = \boldsymbol{F}_q^n$$

$$\boldsymbol{s} = (s_1, \ldots, s_k) \longmapsto \boldsymbol{s}G = (\boldsymbol{s} | \boldsymbol{s}P)$$

(前半： 情報桁、後半： 検査桁)

線型符号の例

- **多数決符号 (反復符号)**
- **パリティ検査符号 (誤り検出のみ)**
- **Hamming 符号**

(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 $x \in \mathcal{H}$ **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** $x \in \mathcal{H}$ **が得られることを確かめよ。**

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

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

符号語の例：

情報語 $\boldsymbol{s} = (1\ 0\ 0\ 1)$

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

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

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

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** $(1\ 0\ 0\ 1)$

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

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

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** $(1\ 0\ 0\ 1)$

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

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

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。

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

$\longrightarrow y - e_3 = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が正しい符号語**

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

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

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

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** $(1\ 0\ 0\ 1)$

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

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

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**

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**

$\Longleftrightarrow$ $f : V \longrightarrow V$: **等距離線型同型で** $f(\mathcal{C}) = \mathcal{C}$

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)**