

## 線型符号 (linear codes)

To construct a code with many code-words  
systematically,

the code-words of  $\mathcal{C}$  should be distributed  
as “equally” as possible.

→ Use mathematical structures (symmetry)  
of  $V = \mathbb{T}^n$   
... **linear codes** (線型符号)

## 線型符号 (linear codes)

$T = F_q$  : a finite field (有限体)

$V = F_q^n$  : a linear space over  $F_q$   
... 和・スカラ倍がある  
(equipped with sum and scalar multiplication)

$C$  : 線型符号 (linear code)

$\iff C$  is a subspace of  $V$

## 線型符号の不変量 (invariants of linear codes)

the code-word length (符号語長)  $n = \dim_{\mathbb{F}_q} V$

the dimension (次元)  $k := \dim_{\mathbb{F}_q} \mathcal{C}$  over  $\mathbb{F}_q$

→  $[n, k]$ -code (符号語数  $M = \#\mathcal{C} = q^k$ )

$w(\mathbf{x}) := \#\{i \mid x_i \neq 0\}$  : the weight (重み) of  $\mathbf{x} \in V$

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

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

→  $[n, k, d]$ -code

## Hamming 距離 (Hamming distance)

**Hamming distance** on  $V = T^n$

$$d : V \times V \longrightarrow \mathbf{R}_{\geq 0}$$

**is defined as follows:**

**for**  $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in V,$

$$d(\mathbf{x}, \mathbf{y}) := \#\{i \mid x_i \neq y_i\}.$$

## 線型符号の不変量 (invariants of linear codes)

- the code-word length (符号長)  $n = \dim_{\mathbb{F}_q} V$   
(temporarily fix)
- the **dimension** (次元)  $k = \dim_{\mathbb{F}_q} \mathcal{C}$   
(larger, better)
- the **minimum distance** (最小距離)  $d$   
(larger, better)

$R := \frac{k}{n}$  : **transmission rate** (伝送レート)

$\delta := \frac{d}{n}$  : **relative minimum distance**

(相対最小距離)

→  $R, \delta$  : **both larger (conflicting request)**

## 線型符号の例 (examples of linear codes)

- 多数決符号 (反復符号) (repetition codes)
- パリティ検査符号 (parity-check codes)  
(誤り検出のみ, only error-detection)
- Hamming codes

## 多数決符号 (反復符号, repetition codes)

$$n = 2t + 1, V = \mathbb{F}_q^n$$

**Send each symbol  $n$  times repeatedly.**

$$\mathcal{C} = \{(x, x, \dots, x) \mid x \in \mathbb{F}_q\} \subset V$$

$$\mathcal{C} = \mathbb{F}_q \mathbf{v} \quad \text{with } \mathbf{v} = (1, 1, \dots, 1)$$

- 符号長  $n = \dim_{\mathbb{F}_q} V$
- 次元  $k = \dim_{\mathbb{F}_q} \mathcal{C} = 1$
- 最小距離  $d = n$  (**t-error correction**)

## パリティ検査符号 (parity-check codes)

$$V = \mathbb{F}_q^n$$

$$\mathcal{C} = \left\{ \mathbf{x} = (x_1, x_2, \dots, x_n) \mid \sum_{i=1}^n x_i = 0 \right\} \subset V$$

- 符号長  $n = \dim_{\mathbb{F}_q} V$
- 次元  $k = \dim_{\mathbb{F}_q} \mathcal{C} = n - 1$
- 最小距離  $d = 2$

**(only 1 error-detection, no error-correction)**

## 拡大符号 (extended codes)

$$V = \mathbb{F}_q^n$$

$$\mathcal{C} : [n, k, d]\text{-code} \subset V$$

$$\bar{\mathcal{C}} := \left\{ (x_1, \dots, x_n, x_{n+1}) \mid \begin{array}{l} (x_1, \dots, x_n) \in \mathcal{C} \\ \sum_{i=1}^{n+1} x_i = 0 \end{array} \right\}$$

:  $\mathcal{C}$  の**拡大符号 (extended code)**  $\subset \mathbb{F}_q^{n+1}$

$$\bar{\mathcal{C}} : [n + 1, k, d + \varepsilon]\text{-code} \quad (\varepsilon = 0, 1)$$

## 線型符号の生成行列 (generator matrix)

$$\mathcal{C} \subset V = \mathbf{F}_q^n = \{\mathbf{x} = (x_1, \dots, x_n) \mid x_i \in \mathbf{F}_q\}$$

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

$(\mathbf{v}_1, \dots, \mathbf{v}_k)$  : a basis of  $\mathcal{C}$

$$\mathbf{v}_i = (a_{i1}, \dots, a_{in})$$

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

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

## 符号語の生成 (generation of code-words)

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

**: a generator matrix of  $\mathcal{C}$**

$$\mathcal{C} = \{\mathbf{s}G \mid \mathbf{s} \in \mathbf{F}_q^k\}$$

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

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

## 符号語の検査 (Checking code-words)

**How to check**

**whether a received word  $y \in V$   
is a correct code-word ( $y \in \mathcal{C}$ ) or not**

$\pi_{\mathcal{C}} : V \longrightarrow V/\mathcal{C} \simeq \mathbb{F}_q^{n-k}$  : **projection**

**Take a basis of  $V/\mathcal{C}$**

**(or, choose an isomorphism  $V/\mathcal{C} \simeq \mathbb{F}_q^{n-k}$ ),  
for matrix representation of  $\pi_{\mathcal{C}}$ .**

## 符号語の検査 (Checking code-words)

$$\varphi_A : V = \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k}$$

$$\mathbf{y} \longmapsto \mathbf{y}A$$

$$\mathbf{y} \in \mathcal{C} \iff \varphi_A(\mathbf{y}) = \mathbf{y}A = 0$$

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

$H : \mathcal{C}$  のパリティ検査行列 (**parity-check matrix**)

$$\mathbf{y} \in \mathcal{C} \iff \mathbf{y}H^T = 0$$

## 誤り訂正 (error correction)

$$\mathbf{y} \notin \mathcal{C} \iff \mathbf{y}\mathbf{H}^T \neq \mathbf{0}$$

$\mathbf{y}\mathbf{H}^T$  : the **syndrome** (シンドローム) of  $\mathbf{y}$

**How to find the correct code-word  $\mathbf{x} \in \mathcal{C}$**

$\iff$  **How to obtain the error vector  $\mathbf{e} := \mathbf{y} - \mathbf{x}$**

## 誤り訂正 (error correction)

- $\mathbf{y} \equiv \mathbf{y}' \pmod{\mathcal{C}} \iff \mathbf{y}\mathbf{H}^T = \mathbf{y}'\mathbf{H}^T$
  - $\mathbf{y} \equiv \mathbf{e} \pmod{\mathcal{C}}$
  - $w(\mathbf{e}) \leq t$  (assumption)
- 

- **Enumerate all  $\mathbf{e} \in V$  with  $w(\mathbf{e}) \leq t$**   
→ **make the table of  $\mathbf{e}\mathbf{H}^T$  in advance**
- **For a received word  $\mathbf{y} \in V$ ,**  
**seek for  $\mathbf{e}$  with  $\mathbf{y}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$  from the table**  
→ **How to do this efficiently**

## 等距離線型自己同型 (linear isometry)

$V = (V, d)$  : a metric linear space

(距離付き線型空間)

$f : V \longrightarrow V$  : a linear isometry

(等距離線型自己同型, isometric linear autom.)

$\iff f$  : a linear autom. preserving distances  
( $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$ )

For  $d$  : Hamming distance,

$\iff f$  : a linear autom. preserving weights  
( $w(f(\mathbf{x})) = w(\mathbf{x})$ )

## 等距離線型自己同型 (linear isometry)

$\text{Aut}(V, d)$  : the group consisting of  
all the linear isometries of  $V = (V, d)$

$\text{Aut}(V, d)$  is generated by  
the following two kinds of autom's:

- permutations of components  
(成分 (文字の場所) の置換)
- non-zero const. multipl'ns of a component  
(或る成分の非零定数倍)

$$\text{Aut}(V, d) = \mathfrak{S}_n \wr \mathbf{F}_q^\times = \mathfrak{S}_n \ltimes (\mathbf{F}_q^\times)^n$$

## 符号の同値 (equivalence of codes)

Two codes  $\mathcal{C}, \mathcal{C}' \subset V$  are **equivalent** (同値)

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

同値な符号は、誤り訂正に関して同様の性質を持つ

**Equivalent codes have the same properties  
w.r.t. error-correction.  
(the dimension, the minimum distance)**

Good representatives of equivalent classes  
= standard forms of linear codes  
= systematic codes

## 符号の同値 (equivalence of codes)

Two codes  $\mathcal{C}, \mathcal{C}' \subset V$  are **equivalent** (同値)

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

同値な符号は、誤り訂正に関して同様の性質を持つ

**Equivalent codes have the same properties**

**w.r.t. error-correction.**

**(the dimension, the minimum distance)**

**Good representatives of equivalent classes**

**= standard forms of linear codes**

**= systematic codes**

## 組織符号 (systematic codes)

$\mathcal{C}$  : a **systematic code** (組織符号)

$\iff \mathcal{C}$  has a generator matrix  $G$  of the form  
 $G = (I_k | P)$ , where  $P \in M(k, n - k; \mathbb{F}_q)$ .

$G = (I_k | P)$  : **gen.matrix** ( $P \in M(k, n - k; \mathbb{F}_q)$ )

$H = (-P^T | I_{n-k})$  : **check matrix**

$$GH^T = 0$$

## 組織符号 (systematic codes)

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

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

$$\mathbf{s} = (s_1, \dots, s_k) \mapsto \mathbf{s}G = (\mathbf{s} | \mathbf{s}P)$$

$\mathbf{s}$  : **information symbols**(情報桁)

$\mathbf{s}P$  : **check symbols**(検査桁)

Thm

Any linear code is equivalent  
to a systematic code.

## 組織符号 (systematic codes)

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

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

$$\mathbf{s} = (s_1, \dots, s_k) \mapsto \mathbf{s}G = (\mathbf{s} | \mathbf{s}P)$$

$\mathbf{s}$  : **information symbols**(情報桁)

$\mathbf{s}P$  : **check symbols**(検査桁)

Thm

**Any linear code is equivalent  
to a systematic code.**