

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)

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

: a generator matrix of \mathcal{C}

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

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

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

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

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.**

パリティ検査行列と最小距離

(check matrices and minimum distances)

H : a check matrix of C

the minimum distance $d =$

(the minimum # of column vectors of H
which are linearly dependent)

(H の線型従属な列ベクトルの個数の最小値)

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**

Hamming 符号 (Hamming codes)

$$c \geq 1$$

of the lines in \mathbb{F}_q^c through the origin

$$n = \frac{q^c - 1}{q - 1}$$

Choose a direction vector \mathbf{h}_i for each line.

→ No two vectors are colinear.

→ A linearly dependent system of \mathbf{h}_i 's
consists of at least 3 vectors.

$$H := (\mathbf{h}_1 \cdots \mathbf{h}_n) \in M(c, n; \mathbb{F}_q)$$

\mathcal{C} : the code with check matrix H

... **Hamming code** → $d = 3, t = 1$

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 $GH^T = 0$ となるような) G を求めよ。
- (3) $w(e) = 1$ なる $e \in \mathbb{F}_2^7$ を列挙し、そのシンδροーム eH^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 $y \in \mathbb{F}_2^7$ について、シンδροーム yH^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。

符号の自己同型 (automorphisms of a code)

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 $V = \mathbb{T}^n$

invariant under translation (平行移動で不変)
→ linear codes (線型符号)

符号の自己同型 (automorphisms of a code)

To be more efficient, more “symmetric” !!

“symmetry of a code”

... **automorphisms** of a code
(符号の**自己同型**)

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)**

符号の自己同型 (automorphisms of a code)

\mathcal{C} : a linear code $\subset V = \mathbb{F}_q^n$

f : \mathcal{C} の自己同型 (automorphism)

$$\iff f \in \text{Aut}(V, d) \text{ s.t. } f(\mathcal{C}) = \mathcal{C}$$

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

: \mathcal{C} の自己同型群

(the automorphism group of \mathcal{C})

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

符号の自己同型 (automorphisms of a code)

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

In particular, when $q = 2$,

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

→ 対称群の有限体上の線型表現の問題に
(linear representations of symmetric groups
over finite fields)

A typical case:

$$\sigma = (1 \ 2 \ \dots \ n) \in \text{Aut}(\mathcal{C})$$

… 巡回符号 (cyclic codes)