線型符号の生成行列 (generator matrix)

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

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

$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$: **a basis of** $\mathcal{C}$

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

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

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

符号語の生成 (generation of code-words)

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

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

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

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

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

符号語の検査 (Checking code-words)

How to check

whether a recieved word $y \in V$

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

$$\pi_{\mathcal{C}} : V \longrightarrow V/\mathcal{C} \simeq \mathbf{F_q}^{n-k} \text{ : projection}$$

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

(or, choose an isomorphism $V/\mathcal{C} \simeq \mathbf{F_q}^{n-k}$),

for matrix representation of $\pi_{\mathcal{C}}$.

符号語の検査 (Checking code-words)

$$\varphi_A : V = \mathbf{F}_q{}^n \longrightarrow \mathbf{F}_q{}^{n-k}$$
$$y \longmapsto yA$$
$$y \in \mathcal{C} \Longleftrightarrow \varphi_A(y) = yA = 0$$

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

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

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

誤り訂正 (error correction)

$$\mathbf{y} \notin \mathcal{C} \Longleftrightarrow \mathbf{y}\mathrm{H}^{\mathsf{T}} \neq 0$$

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

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

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

誤り訂正 (error correction)

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

- **Enumerate all $\boldsymbol{e} \in \mathrm{V}$ with $w(\boldsymbol{e}) \leq \mathrm{t}$**
  $\longrightarrow$ make the table of $\boldsymbol{e}\mathrm{H}^{\mathsf{T}}$ in advance
- **For a recieved word $\mathbf{y} \in \mathrm{V}$,**
  seek for $\boldsymbol{e}$ with $\mathbf{y}\mathrm{H}^{\mathsf{T}} = \boldsymbol{e}\mathrm{H}^{\mathsf{T}}$ from the table

  $\longrightarrow$ How to do this efficiently

等距離線型自己同型 (linear isometry)

$\mathrm{V} = (\mathrm{V}, \mathrm{d})$: a metric linear space
(距離付き線型空間)

$\mathrm{f} : \mathrm{V} \longrightarrow \mathrm{V}$: a **linear isometry**
(**等距離線型自己同型**, **isometric linear autom.**)

$\Longleftrightarrow$ f : a linear autom. preserving distances
$(\mathrm{d}(\mathrm{f}(\boldsymbol{x}), \mathrm{f}(\boldsymbol{y})) = \mathrm{f}(\boldsymbol{x}, \boldsymbol{y}))$

For d : Hamming distance,
$\Longleftrightarrow$ f : a linear autom. preserving weights
$(w(\mathrm{f}(\boldsymbol{x})) = w(\boldsymbol{x}))$

等距離線型自己同型 (linear isometry)

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

$\mathrm{Aut}(\mathrm{V}, \mathrm{d})$ **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)**

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

符号の同値 (equivalence of codes)

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

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

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)

$\overset{\leftarrow}{\Longleftrightarrow}$ $\mathcal{C}$ has a generator matrix G of the form

$$G = (I_k | P), \text{ where } P \in M(k, n-k; \mathbf{F}_q).$$

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

$H = \left(-P^T \middle| I_{n-k}\right)$: check matrix

$GH^T = O$

組織符号 (systematic codes)

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

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

$$s = (s_1, \ldots, s_k) \longmapsto sG = (s|sP)$$

s : **information symbols(情報桁)**

sP : **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 $\mathcal{C}$

the minimum distance $\mathrm{d} =$
(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**

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 $F_q{}^c$ through the origin

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

Choose a direction vector h_i for each line.

$\longrightarrow$ No two vectors are colinear.

$\longrightarrow$ A linearly dependent system of h_i's consists of at least 3 vectors.

$H := (h_1 \cdots h_n) \in M(c, n; F_q)$

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

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

Hamming 符号 (Hamming codes)

$c \geq 1$

of the lines in $F_q{}^c$ through the origin

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

Choose a direction vector h_i for each line.

$\longrightarrow$ **No two vectors are colinear.**

$\longrightarrow$ **A linearly dependent system of h_i's consists of at least 3 vectors.**

$H := (h_1 \cdots h_n) \in M(c, n; F_q)$

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

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

Hamming 符号 (Hamming codes)

$c \geq 1$

of the lines in $F_q{}^c$ through the origin

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

Choose a direction vector h_i for each line.

$\longrightarrow$ **No two vectors are colinear.**

$\longrightarrow$ **A linearly dependent system of h_i's consists of at least 3 vectors.**

$H := (h_1 \cdots h_n) \in M(c, n; F_q)$

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

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

Hamming 符号 (Hamming codes)

$c \geq 1$

of the lines in $F_q{}^c$ through the origin

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

Choose a direction vector h_i for each line.

$\longrightarrow$ **No two vectors are colinear.**

$\longrightarrow$ **A linearly dependent system of h_i's consists of at least 3 vectors.**

$H := (h_1 \cdots h_n) \in M(c, n; F_q)$

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

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

Hamming 符号 (Hamming codes)

$c \geq 1$

of the lines in $F_q{}^c$ through the origin

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

Choose a direction vector h_i for each line.

$\longrightarrow$ **No two vectors are colinear.**

$\longrightarrow$ **A linearly dependent system of h_i's consists of at least 3 vectors.**

$H := (h_1 \cdots h_n) \in M(c, n; F_q)$

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

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

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 $\mathrm{GH}^{\mathsf{T}} = \mathrm{O}$ 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、そのシンドローム $e\mathrm{H}^{\mathsf{T}}$ 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、シンドローム $y\mathrm{H}^{\mathsf{T}}$ 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.

$\longrightarrow$ Use mathematical structures (symmetry) of $V = \mathrm{T}^{\mathrm{n}}$

invariant under translation (平行移動で不変)
$\longrightarrow$ 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”

$\cdots$ automorphisms of a code
(符号の自己同型)

符号の自己同型 (automorphisms of a code)

To be more efficient, more “symmetric” !!

“symmetry of a code”

$\cdots$ automorphisms of a code

(符号の自己同型)

等距離線型自己同型 (linear isometry)

$\mathrm{V} = (\mathrm{V}, \mathrm{d})$: a metric linear space
(距離付き線型空間)

$\mathrm{f} : \mathrm{V} \longrightarrow \mathrm{V}$: a **linear isometry**
(**等距離線型自己同型**, **isometric linear autom.**)

$\Longleftrightarrow$ f : a linear autom. preserving distances
$(\mathrm{d}(\mathrm{f}(\boldsymbol{x}), \mathrm{f}(\boldsymbol{y})) = \mathrm{f}(\boldsymbol{x}, \boldsymbol{y}))$

For d : Hamming distance,
$\Longleftrightarrow$ f : a linear autom. preserving weights
$(w(\mathrm{f}(\boldsymbol{x})) = w(\boldsymbol{x}))$

等距離線型自己同型 (linear isometry)

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

$\mathrm{Aut}(\mathrm{V}, \mathrm{d})$ **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)**

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

符号の同値 (equivalence of codes)

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

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

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** $\subset V = \mathbf{F}_q{}^n$

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

$$\overset{\leftarrow}{\Longleftrightarrow} \mathrm{f} \in \mathrm{Aut}(V, \mathrm{d}) \text{ s.t. } \mathrm{f}(\mathcal{C}) = \mathcal{C}$$

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

: $\mathcal{C}$ **の自己同型群**

(the automorphism group of $\mathcal{C}$**)**

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

符号の自己同型 (automorphisms of a code)

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

In particular, when $q = 2$,

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

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

A typical case:

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

$\cdots$ 巡回符号 (cyclic codes)

符号の自己同型 (automorphisms of a code)

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

In particular, when $q = 2$**,**

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

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

A typical case:

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

$\cdots$ **巡回符号 (cyclic codes)**

符号の自己同型 (automorphisms of a code)

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

In particular, when $q = 2$**,**

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

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

A typical case:

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

$\cdots$ **巡回符号 (cyclic codes)**