線型符号

符号語数 M の大きい符号を
組織的に構成するには、

$\mathcal{C}$ の元がなるべく “均等に” 分布する
のが望ましい

$\longrightarrow V = T^n$ の持つ数理構造 (対称性) を利用
$\cdots$ **線型符号**

線型符号

$T = F_q$: 有限体にとる

$V = {F_q}^n$: F_q 上の線型空間の構造を持つ
(和・スカラ倍がある)

$\mathcal{C}$: V の部分線型空間のとき

$\mathcal{C}$: **線型符号 (linear code)** と呼ぶ

有限体 (finite field)

Z/nZ : n で割った余りの等しい整数は同一視

$\longrightarrow$ 環の構造を持つ (加減乗が出来る)

Z/nZ : 体 (四則演算が出来る)

$\Updownarrow$

p : 素数

$F_p := Z/pZ$: p 元体

有限体 (finite field)

$q = p^m$: 素数冪 (p : 素数) に対して

q 個の元から成る有限体が存在

$\longrightarrow \boldsymbol{F}_q, GF(q)$ と書く

構成:

$f(X) \in \boldsymbol{F}_p[X]$: $\boldsymbol{F}_p$ 上の m 次既約多項式

$K := \boldsymbol{F}_p[X]/(f)$ とすると、

K は体で、 $\dim_{\boldsymbol{F}_p} K = m \qquad \longrightarrow \#K = q$

有限体上の線型空間

有限体 F_q 上でも、R や C 上と同様に、
線型代数が出来る (基底・次元・などなど)

$T = \boldsymbol{F}_q$ **: 有限体**

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

$\mathcal{C} \subset V$ **: 部分線型空間となるものを考える**

- $\mathbf{0} \in \mathcal{C}$
- $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C} \Longrightarrow \boldsymbol{x} + \boldsymbol{y} \in \mathcal{C}$
- $\boldsymbol{x} \in \mathcal{C}, a \in \boldsymbol{F}_q \Longrightarrow a\boldsymbol{x} \in \mathcal{C}$

線型符号 (再掲)

$T = F_q$: 有限体にとる

$V = F_q^{\,n}$: 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 (linear code)** と呼ぶ

線型符号の不変量

符号語長 $n = \dim_{\boldsymbol{F}_q} V$

$k := \dim_{\boldsymbol{F}_q} \mathcal{C}$ **：** $\mathcal{C}$ **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 $d = d(\mathcal{C}) = \min\{w(\boldsymbol{x}) \,|\, \boldsymbol{x} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{0}\}$

$\longrightarrow$ $[n, k, d]$**-符号**

Hamming 距離 (再掲)

$V = T^n$ 上に次で定まる距離

$$d : V \times V \longrightarrow \boldsymbol{R}$$

を V 上の Hamming 距離 (distance) と呼ぶ：

$\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in V$ に対し、

$$d(\boldsymbol{x}, \boldsymbol{y}) := \#\{i | x_i \neq y_i\}$$

線型符号の不変量

- **符号長** $n = \dim_{\boldsymbol{F}_q} V$ **(当座固定)**
- **情報長** $k = \dim_{\boldsymbol{F}_q} \mathcal{C}$ **(大きいほど良い)**
- **最小距離** d **(大きいほど良い)**

$R := \dfrac{k}{n}$ **：伝送レート**

$\delta := \dfrac{d}{n}$ **：相対最小距離**

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

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**

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

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

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

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

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)

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

パリティ検査行列と最小距離

H : 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**)

復号 (誤り訂正)

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

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**

等距離線型自己同型

$V = (V, d)$：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

$V = (V, d)$ **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)

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

符号の同値

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

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

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**

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**

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 h_i を 1 本づつ選ぶと
どの 2 本も同一直線上にない
$\longrightarrow$ 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** $\longrightarrow d = 3, t = 1$

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 h_i を 1 本づつ選ぶと
どの 2 本も同一直線上にない
$\longrightarrow$ 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 $\longrightarrow d = 3, t = 1$

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 h_i を 1 本づつ選ぶと
どの 2 本も同一直線上にない
$\longrightarrow$ h_i 達の線型従属系は最小 3 本

$H := (h_1 \cdots h_n)$

C : H をパリティ検査行列とする符号

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

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** $\longrightarrow d = 3, t = 1$

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。