

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

C : V の部分線型空間のとき

C : **線型符号**と呼ぶ

線型符号の不変量

$k := \dim_{F_q} \mathcal{C} : \mathcal{C}$ の F_q 上の次元

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

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

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

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

$\longrightarrow \underline{[n, k, d]\text{-符号}}$

線型符号の不変量

$$R := \frac{k}{n} : \underline{\text{伝送レート}}$$

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

→ R, δ : 共に大きくしたい (相反する要求)

線型符号の表示

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

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

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

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

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

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

符号語の生成 (符号化)

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

: \mathcal{C} の生成行列

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

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

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

符号語の検査

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

$$\pi_C : V \longrightarrow V/C \simeq F_q^{n-k} : \text{標準射影}$$

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

符号語の検査

$$\begin{aligned}\varphi_A : V = \mathbf{F}_q^n &\longrightarrow \mathbf{F}_q^{n-k} \\ \mathbf{y} &\longmapsto \mathbf{y}A\end{aligned}$$

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

通常、

転置行列 $H = A^T \in M(n-k, n; \mathbf{F}_q)$ で表示
: \mathcal{C} の パリティ検査行列

(parity-check matrix)

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

復号 (誤り訂正)

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

$\mathbf{y}H^T$: \mathbf{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？

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

復号 (誤り訂正)

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

に注意

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

→ 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

$\iff f$: 線型同型で距離を保つ

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

d : **Hamming** 距離の場合には、

$\iff f$: 線型同型で重みを保つ

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

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
 $\cdots \text{Aut}(V, d)$

$\text{Aut}(V, d)$ 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)

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

符号の同値

符号 $C, C' \subset V$ が 同値

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

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

$$G = (I_k | P), \quad H = (-P^T | I_{n-k})$$
$$(P \in M(k, n - k; \mathbf{F}_q), GH^T = O)$$

このとき、

$$\varphi_G : \mathbf{F}_q^k \xrightarrow{\sim} \mathcal{C} \subset V = \mathbf{F}_q^n$$
$$\mathbf{s} = (s_1, \dots, s_k) \longmapsto \mathbf{s}G = (\mathbf{s} | \mathbf{s}P)$$

(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 $GH^T = 0$ となるような) G を求めよ。
- (3) $w(e) = 1$ なる $e \in F_2^7$ 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 $y \in F_2^7$ 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。

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

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

符号語の例：

情報語 $s = (1 \ 0 \ 0 \ 1)$

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

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

e	eH^T
e_1	(1 1 1)
e_2	(1 1 0)
e_3	(1 0 1)
e_4	(0 1 0)
e_5	(1 0 0)
e_6	(0 1 0)
e_7	(0 0 1)

符号語 $x = (1 0 0 1 1 0 0)$ が
1箇所誤って

$$y = (1 0 \mathbf{1} 1 1 0 0)$$

と受信されたとせよ。

$$yH^T = (1 0 1) = e_3H^T$$

→ $y - e_3 = (1 0 \mathbf{0} 1 1 0 0)$ が正しい符号語

→ 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 → 線型符号

もっと“対称性”が高いと良いのでは？

“対称性” → 符号の自己同型

符号の自己同型

$$\mathcal{C} : \text{符号} \subset V = \mathbf{F}_q^n$$

$f : \mathcal{C}$ の 自己同型

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

その全体は群を成す $\dots \text{Aut}(\mathcal{C})$

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

符号の自己同型

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

特に、 $q = 2$ のときは、

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

→ 対称群の有限体上の線型表現の問題に

典型的な場合:

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

... 巡回符号 (cyclic code)