

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、

C の元がなるべく “均等に” 分布する
のが望ましい

→ $V = T^n$ の持つ数理構造 (対称性) を利用
… 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)

C : V の部分線型空間のとき

C : 線型符号 (linear code) と呼ぶ

有限体 (finite field)

$\mathbb{Z}/n\mathbb{Z}$: n で割った余りの等しい整数は同一視

→ 環の構造を持つ (加減乗が出来る)

$\mathbb{Z}/n\mathbb{Z}$: 体 (四則演算が出来る)



p : 素数

$F_p := \mathbb{Z}/p\mathbb{Z}$: 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

→ $F_q, GF(q)$ と書く

構成:

$f(X) \in F_p[X]$: F_p 上の m 次既約多項式

$K := F_p[X]/(f)$ とすると、

K は体で、 $\dim_{F_p} K = m$ → $\#K = q$

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)

$T = F_q$: 有限体

$V = F_q^n$: F_q 上の線型空間の構造を持つ

$C \subset V$: 部分線型空間となるものを考える

- $0 \in C$
- $x, y \in C \implies x + y \in C$
- $x \in C, a \in F_q \implies ax \in C$

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

C : V の部分線型空間のとき

C : 線型符号 (**linear code**) と呼ぶ

線型符号の不変量

符号語長 $n = \dim_{F_q} V$

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

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

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

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

最小距離 $d = d(\mathcal{C}) = \min\{w(\mathbf{x}) | \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq \mathbf{0}\}$
 $\longrightarrow [n, k, d]\text{-符号}$

Hamming 距離 (再掲)

$V = T^n$ 上に次で定まる距離

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

を V 上の **Hamming 距離 (distance)** と呼ぶ :

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

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

線型符号の不変量

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

$$R := \frac{k}{n} : \text{伝送レート}$$

$$\delta := \frac{d}{n} : \text{相対最小距離}$$

→ R, δ : 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

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

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

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

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

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

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

符号語の検査

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

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

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

符号語の検査

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

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

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

通常、

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

: \mathcal{C} のパリティ検査行列

(parity-check matrix)

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

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)

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

$\mathbf{y}H^T$: \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

$$\iff f : \text{線型自己同型で距離を保つ} \\ (d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}))$$

d : **Hamming** 距離の場合には、

$$\iff f : \text{線型自己同型で重みを保つ} \\ (w(f(\mathbf{x})) = w(\mathbf{x}))$$

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

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

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

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

Hamming 符号

$$c \geq 1$$

$$F_q^c \text{ 内で原点を通る直線の本数 } n = \frac{q^c - 1}{q - 1}$$

ここから方向ベクトル h_i を 1 本ずつ選ぶと
どの 2 本も同一直線上にない
→ 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

… **Hamming 符号** → $d = 3, t = 1$

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 $e \in F_2^7$ 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。