

誤り訂正符号の性能を表すには

- 符号長 n (当座固定)
- 符号語数 $M := \#C$ (大きいほど良い)
- 最小距離 d (大きいほど良い)

「 $M \rightarrow$ 大」と「 $d \rightarrow$ 大」とは
相反する要求!!

問題: n, d を固定した時の M の上限は ?

符号語数の評価

問題: n, d を固定した時の M の上限は ?

d : 設計距離

$$A_q(n, d) := \max\{M \mid \exists \mathcal{C} : q \text{ 元 } (n, M, d)\text{-符号}\}$$

→ n, d と $q := \#T$ とで評価する

Hamming の球充填上界

(sphere-packing bound)

$q := \#T$ のとき、

$(n, M, 2t + 1)$ -符号が存在

$$\implies M \left(\sum_{k=0}^t \binom{n}{k} (q-1)^k \right) \leq q^n$$

従って、

$$A_q(n, d) \left(\sum_{k=0}^t \binom{n}{k} (q-1)^k \right) \leq q^n \quad (t = \lfloor \frac{d-1}{2} \rfloor)$$

Gilbert-Varshamov の下界

$q := \#T$ のとき、

$$A_q(n, d) \left(\sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k \right) \geq q^n$$

即ち、

$$M \left(\sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k \right) \leq q^n \\ \implies (n, M, d)\text{-符号が存在}$$

問題: n, d を固定した時の M の上限は ?

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 $d = d(\mathcal{C}) = \min\{w(\mathbf{x}) | \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq 0\}$

$\longrightarrow [n, k, d]\text{-符号}$

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

多数決符号 (反復符号, repetition code)

$$n = 2t + 1, V = \mathbf{F}_q^n$$

1 つの文字を n 回繰返して送信

$$\mathcal{C} = \{(x, x, \dots, x) \mid x \in \mathbf{F}_q\} \subset V$$

$$\mathbf{v} = (1, 1, \dots, 1) \text{ とすれば、 } \mathcal{C} = \mathbf{F}_q \mathbf{v}$$

- 符号長 $n = \dim_{\mathbf{F}_q} V$
- 情報長 $k = \dim_{\mathbf{F}_q} \mathcal{C} = 1$
- 最小距離 $d = n$ (t 個までの誤りを訂正可)

パリティ検査符号 (parity-check code)

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

$$\mathcal{C} = \left\{ \mathbf{x} = (x_1, x_2, \dots, x_n) \mid \sum_{i=1}^n x_i = 0 \right\} \subset V$$

- 符号長 $n = \dim_{\mathbf{F}_q} V$
- 情報長 $k = \dim_{\mathbf{F}_q} \mathcal{C} = n - 1$
- 最小距離 $d = 2$
(誤り検出のみで訂正能力なし)

拡大符号 (extended code)

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

$\mathcal{C} : [n, k, d]$ -符号 $\subset V$ に対して

$$\bar{\mathcal{C}} := \left\{ (x_1, \dots, x_n, x_{n+1}) \mid \begin{array}{l} (x_1, \dots, x_n) \in \mathcal{C} \\ \sum_{i=1}^{n+1} x_i = 0 \end{array} \right\}$$

$: \mathcal{C}$ の**拡大符号** $\subset \mathbf{F}_q^{n+1}$

$\bar{\mathcal{C}} : [n + 1, k, d]$ -符号