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 $M := \#\mathcal{C}$ (大きいほど良い)**
- **最小距離 d (大きいほど良い)**

「$M \longrightarrow$ 大」と「$d \longrightarrow$ 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**

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

$$\longrightarrow n, d \text{ と } q := \#T \text{ とで評価する}$$

Hamming の球充填上界 (sphere-packing bound)

$q := \#T$ のとき、

$(n, M, 2t+1)$-符号が存在

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

従って、

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

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、

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

$$\Longrightarrow (n,M,d)\text{-}\textbf{符号が存在}$$

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、

$\mathcal{C}$ 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

$T = \boldsymbol{F}_q$: 有限体にとる

$V = \boldsymbol{F}_q{}^n$: 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)

$T = \boldsymbol{F}_q$: 有限体にとる

$V = \boldsymbol{F}_q^{\,n}$: 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 $d = d(\mathcal{C}) = \min\{w(\boldsymbol{x}) | \boldsymbol{x} \in \mathcal{C}, \boldsymbol{x} \neq 0\}$

$\longrightarrow$ $[n, k, d]$**-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**

多数決符号 (反復符号, repetition code)

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

1 つの文字を n 回繰返して送信

$\mathcal{C} = \{(x, x, \ldots, x) | x \in \boldsymbol{F}_q\} \subset V$

$\boldsymbol{v} = (1, 1, \ldots, 1)$ とすれば、$\mathcal{C} = \boldsymbol{F}_q \boldsymbol{v}$

- 符号長 $n = \dim_{\boldsymbol{F}_q} V$
- 情報長 $k = \dim_{\boldsymbol{F}_q} \mathcal{C} = 1$
- 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)

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

$$\mathcal{C} = \left\{ \boldsymbol{x} = (x_1, x_2, \ldots, x_n) \,\middle|\, \sum_{i=1}^{n} x_i = 0 \right\} \subset V$$

- **符号長** $n = \dim_{\boldsymbol{F}_q} V$
- **情報長** $k = \dim_{\boldsymbol{F}_q} \mathcal{C} = n - 1$
- **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)

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

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

$$\overline{\mathcal{C}} := \left\{ (x_1,\ldots,x_n,x_{n+1}) \;\middle|\; \begin{array}{c} (x_1,\ldots,x_n) \in \mathcal{C} \\ \sum_{i=1}^{n+1} x_i = 0 \end{array} \right\}$$

: $\mathcal{C}$ の拡大符号 $\subset \boldsymbol{F}_q{}^{n+1}$

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