誤り訂正性能 (the ability of error-correction)

$\mathcal{C}$: a block code (等長符号) $\subset V = \mathrm{T}^{\mathrm{n}}$

- the code-word length (符号長) n
  (temporarily fix)
- the number of code-words (符号語数)
  $\mathrm{M} := \#\mathcal{C}$ (larger, better)
- the number of correctable errors t
  (larger, better)

But in general,

"larger M" and "larger t"

are conflicting requests !!

誤りの訂正 (Error-correction)

符号 $\mathcal{C} \subset V = \mathrm{T}^n$ で、

- **受信語 $y \notin \mathcal{C}$ によって誤り検出**
  Detect an error if $y \notin \mathrm{Im}\mathcal{C}^*$.
- **y に “一番近い” $x \in \mathcal{C}$ が正しい、**
  として誤り訂正
  Guess the “nearest” $x \in \mathrm{Im}\mathcal{C}^*$ to y
  as the correct word.
  $\longrightarrow$ What is “nearest” ?

$\longrightarrow$ Introduce a “metric” into V
(Hamming metric, usually)

Hamming 距離 (Hamming distance)

Hamming distance on $V = T^n$

$$d : V \times V \longrightarrow \mathbf{R}_{\geq 0}$$

is defined as follows:

for $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in V$**,**

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

誤り訂正性能 (the ability of error-correction)

$\mathcal{C} \subset V = T^n$

n 箇所のうち何箇所違っても訂正できるか？
(How many errors can one correct ?)

$=$ 距離が幾ら以内なら訂正できるか？
(Within what distance can one correct ?)

uniquely correctable for t errors

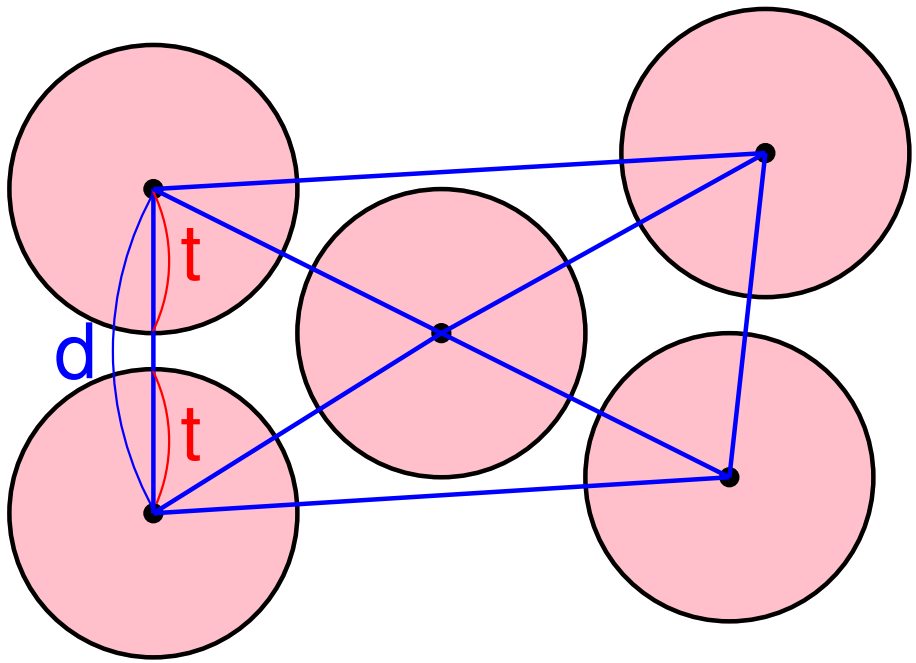
$\Longleftrightarrow$ for any $y \in V$,
at most one $x \in \mathcal{C}$ satisfies $d(x, y) \leq t$
$(\#\{x \in \mathcal{C} | d(x, y) \leq t\} \leq 1)$

誤り訂正性能 (the ability of error-correction)

$\mathrm{d} := \min\{\mathrm{d}(\boldsymbol{x}, \boldsymbol{x}') | \boldsymbol{x}, \boldsymbol{x}' \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{x}'\}$

: $\mathcal{C}$ の**最小距離 (minimum distance)**

t-error-correctable if $\mathrm{d} \geq 2\mathrm{t}+1 \longrightarrow \mathrm{t} = \left\lfloor \dfrac{\mathrm{d}-1}{2} \right\rfloor$



誤り訂正性能 (the ability of error-correction)

- the code-word length (符号長) n
  (temporarily fix)
- the number of code-words (符号語数)
  $\mathrm{M} := \#\mathcal{C}$ (larger, better)
- the number of correctable errors t
  (larger, better)

$\longrightarrow$ Error-correctability t can be seen
from the minimum distance d !!

誤り訂正性能 (the ability of error-correction)

- the code-word length (符号長) n
  (temporarily fix)
- the number of code-words (符号語数)
  $M := \#\mathcal{C}$ (larger, better)
- the **minimum distance** (**最小距離**) d
  (larger, better)

$\longrightarrow$ (n, M, d)-**code**

誤り訂正性能 (the ability of error-correction)

- the code-word length (符号長) n
  (temporarily fix)
- the number of code-words (符号語数)
  $\mathrm{M} := \#\mathcal{C}$ (larger, better)
- the **minimum distance** (**最小距離**) d
  (larger, better)

"larger M" and "larger d" are conflicting !!

What is the supremum of M for fixed n, d ?

符号語数の評価
(Estimation of the number of code-words)

What is the supremum of M for fixed n, d ?

d : **designed distance (設計距離)**

$$A_{\mathrm{q}}(\mathrm{n}, \mathrm{d}) := \max\{\mathrm{M} \mid \exists \mathcal{C} : \mathrm{q}\text{-}\textbf{ary } (\mathrm{n}, \mathrm{M}, \mathrm{d})\text{-}\textbf{code}\}$$

$\longrightarrow$ **Estimate** $A_{\mathrm{q}}(\mathrm{n}, \mathrm{d})$ **with** n, d **and** $\mathrm{q} := \#\mathsf{T}$

符号語数の評価

(Estimation of the number of code-words)

Hamming 距離で “半径 t の球” の元の個数は ?
(How many points
does “a ball of radius t” have
in Hamming distance ?)

$$B(x,t) := \{y \in V \mid d(x,y) \le t\}$$

: 中心 x, 半径 t の球体

$$\#B(x,t) = \sum_{k=0}^{t} \binom{n}{k} (q-1)^k ?$$

符号語数の評価

(Estimation of the number of code-words)

Hamming 距離で “半径 t の球” の元の個数は ?
(How many points
does “a ball of radius t” have
in Hamming distance ?)

$$B(x,t) := \{y \in V \mid d(x,y) \le t\}$$

: 中心 x, 半径 t の球体

$$\#B(x,t) = \sum_{k=0}^{t} \binom{n}{k} (q-1)^k$$

Hamming の球充填上界 (sphere-packing bound)

$q := \#\mathsf{T}$

$\exists \mathcal{C}$: $(n, M, 2t+1)$-**code**

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

Hence,

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

Gilbert-Varshamov の下界
(Gilbert-Varshamov bound)

$q := \#T$

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

i.e.

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

$$\Longrightarrow \exists \mathcal{C} : (n, M, d)\text{-code}$$

What is the supremum of M for fixed n, d ?

To construct a code with large M systematically,

it is better that

the code-words of $\mathcal{C}$ are distributed as "equally" as possible.

$\longrightarrow$ **Use mathematical structures (symmetry) of $\mathrm{V} = \mathrm{T}^{\mathrm{n}}$**

$\cdots$ **linear codes (線型符号)**

線型符号 (linear codes)

$\mathsf{T} = \mathsf{F}_q$: a finite field (有限体)

$V = \mathsf{F}_q{}^n$: a linear space over F_q

$\cdots$ 和・スカラ倍がある

(equipped with sum and scalar multiplication)

$\mathcal{C}$: 線型符号 (linear code)

$\overset{\leftarrow}{\Longleftrightarrow}$ $\mathcal{C}$ is a subspace of V

有限体 (finite fields)

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

$\longrightarrow$ 環 (ring) の構造を持つ (加減乗が出来る)

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

$\Updownarrow$

$n = p$: 素数 (prime number)

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$: p 元体 (the field of p elements)

有限体 (finite fields)

$q = p^m$: **素数冪** (p : **素数**) **に対して**

q **個の元から成る有限体が存在**

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

構成:

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

$K := \mathbf{F}_p[X]/(f)$ **とすると、**

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

有限体上の線型空間

(Linear spaces over finite fields)

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**

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

- $0 \in \mathcal{C}$
- $x, y \in \mathcal{C} \Longrightarrow x + y \in \mathcal{C}$
- $x \in \mathcal{C}, a \in F_q \Longrightarrow ax \in \mathcal{C}$

線型符号 (linear codes) (再掲)

$\mathsf{T} = \mathsf{F}_q$: a finite field (有限体)

$V = \mathsf{F}_q{}^n$: a linear space over F_q

$\cdots$ 和・スカラ倍がある

(equipped with sum and scalar multiplication)

$\mathcal{C}$: 線型符号 (linear code)

$\overset{\leftarrow}{\Longleftrightarrow}$ $\mathcal{C}$ is a subspace of V

線型符号の不変量 (invariants of linear codes)

the code-word length (符号語長) $n = \dim_{\mathbf{F}_q} V$

the dimension (次元) $k := \dim_{\mathbf{F}_q} \mathcal{C}$ **over** $\mathbf{F}_q$

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

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

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

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

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

Hamming 距離 (Hamming distance)

Hamming distance on $V = T^n$

$$d : V \times V \longrightarrow \mathbf{R}_{\geq 0}$$

is defined as follows:

for $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in V$**,**

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

線型符号の不変量 (invariants of linear codes)

- the code-word length (符号長) $n = \dim_{\mathbf{F}_q} V$ (temporarily fix)
- the dimension (次元)$k = \dim_{\mathbf{F}_q} \mathcal{C}$ (larger, better)
- the minimum distance(最小距離) d (larger, better)

$R := \dfrac{k}{n}$: transmission rate (伝送レート)

$\delta := \dfrac{d}{n}$: relative minimum distance (相対最小距離)

$\longrightarrow R, \delta$: both larger (conflicting request)

線型符号の例 (examples of linear codes)

- 多数決符号 (反復符号) (repetition code)
- パリティ検査符号 (parity-check code)
  (誤り検出のみ, only error-detection)
- Hamming code

多数決符号 (反復符号, repetition code)

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

Send each symbol n times repeatedly.

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

$\mathcal{C} = \mathbf{F}_q \boldsymbol{v}$ **with** $\boldsymbol{v} = (1, 1, \ldots, 1)$

- **符号長** $n = \dim_{\mathbf{F}_q} V$
- **次元** $k = \dim_{\mathbf{F}_q} \mathcal{C} = 1$
- **最小距離** $d = n$ **(**t**-error correction)**

パリティ検査符号 (parity-check code)

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

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

- **符号長** $n = \dim_{\mathbf{F}_q} V$
- **次元** $k = \dim_{\mathbf{F}_q} \mathcal{C} = n - 1$
- **最小距離** $d = 2$
  (only error-detection, no error-correction)