Lecture : Formal definitions

Def 1 (Block code): An (n, M) block code is a subset $\mathcal{C} \subseteq \mathcal{X}^n$ with $|\mathcal{C}| = M$.

$n \downarrow$ Blocklength

We hence have rate $R = \frac{\log M}{n}$.

Egs: (i) Rate of repetition code $\mathcal{C} = \{000, 111\}$ is $1/3$ and $\mathcal{C}$ is a $(3,2)$ block code.

(ii) Rate of single parity-check code $\mathcal{C} \subseteq \{0,1\}^n$ is ? and it is a $(\_\_, \_\_)$ block code.

(Recall): From basic communication theory, for a given noisy channel $W = \left(P(\underline{y}|\underline{c}) : \underline{c} \in \mathcal{C}, \underline{y} \in \mathcal{X}^n\right)$, the decoder that minimizes the error probability is the "maximum a-posteriori probability" (MAP) decoder:

$$\hat{\underline{c}} = \arg\max_{\underline{c} \in \mathcal{C}} P(\underline{c} | \underline{y}).$$

HW①: Provide / read up a proof of this fact.

Now, suppose that $\underline{c} \sim \text{Unif}(\mathcal{C})$. Then,

$$\hat{\underline{c}} = \underset{\underline{c} \in \mathcal{C}}{\operatorname{argmax}} \frac{P(\underline{y}|\underline{c})P(\underline{c})}{P(\underline{y})}$$

$$= \underset{\underline{c} \in \mathcal{C}}{\operatorname{argmax}} \underbrace{\frac{1}{M P(\underline{y})}}_{\text{constant!}} \cdot P(\underline{y}|\underline{c}) = \underset{\underline{c} \in \mathcal{C}}{\operatorname{argmax}} P(\underline{y}|\underline{c})$$

$\triangleq$ ML decoder ("maximum likelihood").

<u>What is ML decoding for the BSC</u> ?

For a fixed $\underline{c} \in \mathcal{C}$ and any $\underline{y} \in \{0,1\}^n$,

$$P(\underline{y}|\underline{c}) = p^{d(\underline{c},\underline{y})} (1-p)^{n-d(\underline{c},\underline{y})},$$

where $d(\underline{c},\underline{y}) = d(\underline{y},\underline{c}) \triangleq d$ is the "Hamming distance" b/w $\underline{c}$ and $\underline{y}$,

i.e., the # positions where $\underline{c}$ & $\underline{y}$ differ.

Hence, $ML(\underline{y}) = \underset{\underline{c} \in \mathcal{C}}{\operatorname{argmax}} P(\underline{y}|\underline{c}) = \underset{\underline{c} \in \mathcal{C}}{\operatorname{argmin}} d(\underline{c},\underline{y})$, when $p < 1/2$.

<u>Lemma 1</u> : $d(\cdot,\cdot)$ is a metric over $\mathcal{X}^n$.

<u>Pf</u>: HW.

<u>Def 2</u> (Minimum distance): The minimum distance of a block code $\mathcal{C}$

$$d(\mathcal{C}) = d_{min}(\mathcal{C}) = \min_{\substack{\underline{c}_1, \underline{c}_2 \in \mathcal{C}, \\ \underline{c}_1 \neq \underline{c}_2}} d(\underline{c}_1, \underline{c}_2).$$

An (n, M) block code with min. dist. d is written as an (n, M, d) block code.

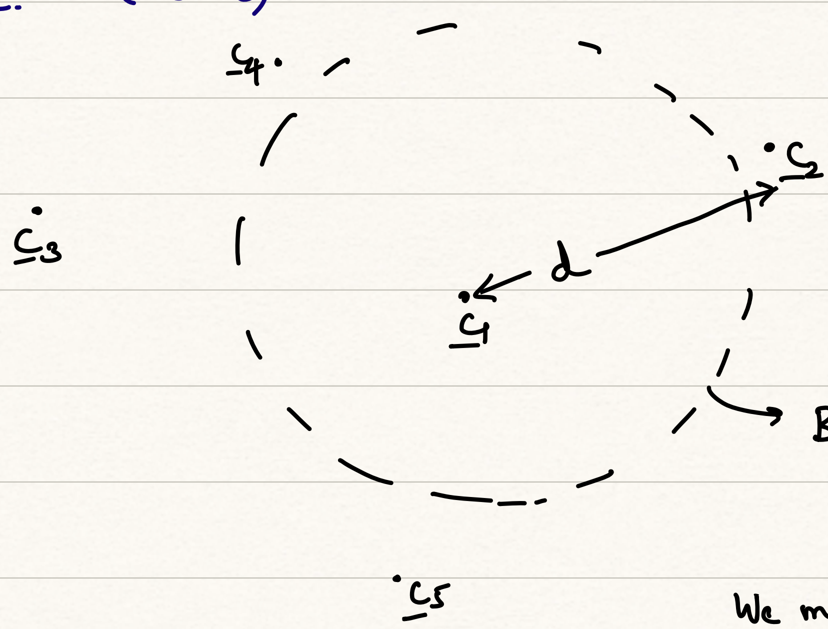
Error detection/correction tied to distance

Thm 1: For an (n, M, d) block code $\mathcal{C}$, $\exists$ a decoder that detects up to $d-1$ bit-flip errors.

This decoder obeys

$$\mathcal{D}(\underline{y}) = \begin{cases} \underline{y}, & \text{if } \underline{y} \in \mathcal{C}, \\ \text{ERROR}, & \text{o.w.} \end{cases}$$

Pf: (Picture)



Ball $B(\underline{c}_1, t)$ of radius t around $\underline{c}_1$.

$\cap\!|$

$\mathcal{X}^n$

We must have $B(\underline{c}_1, t) \cap \mathcal{C} = \{\underline{c}_1\}$, if $t \leq d-1$; else, contradiction

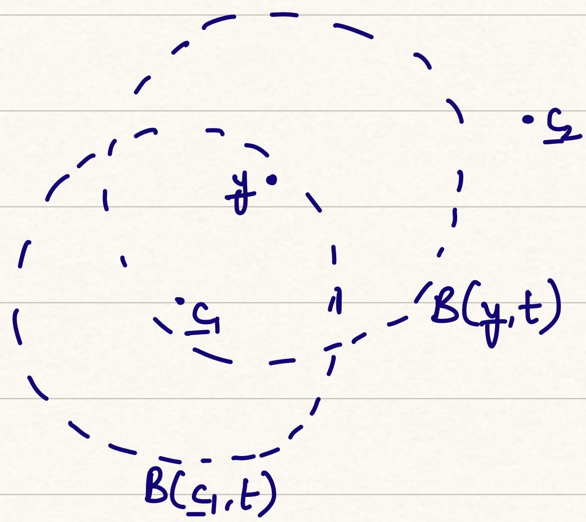
$\blacksquare$

Thm 2: For an (n, M, d) block code $\mathcal{C}$, $\exists$ a decoder that **corrects** $t \leq \lfloor \frac{d-1}{2} \rfloor$ bit-flip errors.

This decoder is the minimum distance decoder

$$\mathcal{D}(\underline{y}) = \underline{c}, \text{ if } B(\underline{y}, t) \cap \mathcal{C} = \{\underline{c}\}.$$

Pf: (Picture)



We cannot have $\underline{c}_2 \neq \underline{c}_1$ s.t. $\underline{c}_2 \in B(\underline{y}, t)$, as then

$$\begin{aligned} d(\underline{c}_1, \underline{c}_2) &\leq d(\underline{c}_1, \underline{y}) + d(\underline{c}_2, \underline{y}) \\ &\leq 2t \leq 2 \cdot \left\lfloor \frac{d-1}{2} \right\rfloor < d, \end{aligned}$$

a contradiction. ☒

An aside: Erasures are channel noise that behave as follows:

$$\underline{c} = (c_1, c_2, \cdots, c_{n-1}, c_n) \xrightarrow[\text{channel}]{\text{Erasure}} \underline{y} = (c_1, ?, c_3, \cdots, c_{n-1}, ?)$$

- Selected codeword symbols are replaced with a '?'.

Thm: For an (n, M, d) block code $\mathcal{C}$, there is a decoder that **corrects** up to $d-1$ erasures.

Pf: HW. (state a decoder and prove its erasure-correction property).

Addendum: Proof that the MAP decoder is optimal for minimizing error prob.
(23-1-26)

Given a channel W and an Encoder (Enc) (or equivalently, the code $\mathcal{C}$), we wish to identify a Decoder (Dec) that minimizes

$$P_{err}(\mathcal{C}) \triangleq \Pr[\hat{m} \neq m]$$

$$= \Pr[\mathrm{Dec}(\underline{y}) \neq \underline{c}]$$ [Assuming that Enc is a one-one map from $\mathcal{M}$ to $\mathcal{C}$]

$$= \sum_{\underline{c}, \underline{y} : D(\underline{y}) \neq \underline{c}} P(\underline{y}, \underline{c})$$ $[D \equiv \mathrm{Dec}]$

$$= \sum_{\underline{y}} P(\underline{y}) \sum_{\underline{c} : D(\underline{y}) \neq \underline{c}} P(\underline{c} | \underline{y}),$$

over D.

Clearly,

$$\arg\min_{D} P_{err}(\mathcal{C}) \text{ computes, for each } \underline{y},$$

[Think about this!]

$$\underset{D(\underline{y})}{\operatorname{argmin}} \sum_{\underline{c}:D(\underline{y})\neq\underline{c}} P(\underline{c}|\underline{y}) .$$

We thus obtain that for any fixed $\underline{y} \in \mathcal{Y}^n$, we must have

$$D(\underline{y}) = \max_{\underline{c}\in\mathcal{C}} P(\underline{c}|\underline{y}) .$$

(MAP estimator)