15/1/2020

Lecture 3

(MAP Decoding, ML Decoding, Minimum distance of a block code)

Announcements

① Tomo (16th Jan) 10:30 am Tutorial

② Assignment 2 (graded) - Released on 16th Jan, Due on 22nd Jan, Discussion will be on 23rd Jan

Assignment 2 will be on linear Codes (Main material required to solve the assignment will be covered on Wednesday).

Block Codes (n - Blocklength or length of the code).

M - No. of Codewords in the Code.

Each codeword is an n-tuple over the Code alphabet $\mathbb{F}$.

Decoder: $\mathcal{D}: \mathbb{F}^n \rightarrow \mathbb{C}$.

$$P_e(\underline{c}) = \sum_{\underline{y}:\, D(\underline{y}) \neq \underline{c}} Pr\left[\underline{y} \,\middle|\, \underline{c}\right]$$

Average probability of error (Code & Decoder have to be specified).

$P_e(\underline{c})$ averaged over all possible codewords in the code

$$P_e = \sum_{c \in \mathbb{C}} P_e(\underline{c})\, Pr(\underline{c}).$$

Total probability Theorem

There is a decoder known as MAP Decoder. MAP stands for Maximum A-posteriori decoder which is optimum decoder for a given Code & Channel.

optimum decoder means that it minimizes the average probability of error.

$$P_e = \sum_{\underline{c} \in \mathbb{C}} \sum_{\underline{y} : \mathcal{D}(\underline{y}) \neq \underline{c}} P_r(\underline{y} | \underline{c}) P(\underline{c}).$$

Interchanging the summations.

$$= \sum_{\underline{y}} \sum_{\substack{\underline{c} \in \mathbb{C} : \\ \mathcal{D}(\underline{y}) \neq \underline{c}}} P_r(\underline{y} | \underline{c}) P(\underline{c}).$$

$$= \sum_{\underline{y}} \sum_{\substack{\underline{c} \in \mathbb{C} : \\ \mathcal{D}(\underline{y}) \neq \underline{c}}} P_r(\underline{c} | \underline{y}) P(\underline{y}).$$

$$= \sum_{\underline{y}} P(\underline{y}) \left(\sum_{\substack{\underline{c} \in \mathbb{C} : \\ \mathcal{D}(\underline{y}) \neq \underline{c}}} P(\underline{c} | \underline{y}). \right)$$

$\mathcal{D} : \mathbb{F}^n \to \mathbb{C}.$

$\mathcal{D}(\underline{y}) \to$

Optimum decoder has to minimize the sum $\forall \underline{y}$.

What choice of $\underline{c}$ minimizes the sum.

$$\left(\sum_{\substack{\underline{c} \in \mathbb{C} : \\ \mathcal{D}(\underline{y}) \neq \underline{c}}} P(\underline{c} | \underline{y}). \right)$$

$$\sum_{\substack{\underline{c} \in \mathbb{C} : \\ \mathcal{D}(\underline{y}) \neq \underline{c}}} P(\underline{c} | \underline{y}) = \sum_{\underline{c} \in \mathbb{C} : \underline{c} \neq \hat{\underline{c}}} P(\underline{c} | \underline{y}).$$

$$= \underbrace{\sum_{\underline{c} \in \mathbb{C}} P(\underline{c} | \underline{y})}_{\text{Does not depend on } \mathcal{D}} - P(\hat{\underline{c}} | \underline{y})$$

The term on the left is minimized if the second term on the right is maximized

$$\boxed{\hat{\underline{c}} = \arg\max_{\underline{c}\in\mathbb{C}} \Pr(\underline{c} \mid \underline{y})}$$

$\leftarrow$ MAP Decoding Rule.

$\hat{\underline{c}}$ is a function of $\underline{y}$.

$$\mathcal{D} : \mathbb{F}^n \to \mathbb{C}.$$
$$\underline{y} \to \hat{\underline{c}}.$$

$$\underline{c} \to \boxed{\text{channel}} \to \underline{y}$$

<u>Maximum Likelihood Decoder</u>
(ML Decoder)

$$\arg\max_{\underline{c}\in\mathbb{C}} \Pr(\underline{c} \mid \underline{y}) = \arg\max_{\underline{c}\in\mathbb{C}} \frac{\Pr(\underline{y} \mid \underline{c})\, P(\underline{c})}{P(\underline{y})}.$$

If $P(\underline{c}) = \overset{(1/M)}{\text{Constant}}$; which means that all codewords are equally likely.

$$\arg\max_{\underline{c}\in\mathbb{C}} \Pr(\underline{c} \mid \underline{y}) = \arg\max_{\underline{c}\in\mathbb{C}} \underbrace{\Pr(\underline{y} \mid \underline{c})}_{\text{Likelihood}}.$$

$$\boxed{\hat{\underline{c}} = \arg\max_{\underline{c} \in \mathbb{C}} P_r(\underline{y} | \underline{c})}.$$

↳ Maximum likelihood Decoder.

ML Decoder is same as MAP Decoder if codewords are equally likely.

→ ML Decoding is said to be optimum

Example of ML Decoding applied to the case of BSC with cross over probability p.

$$\boxed{P_r(\underline{y} | \underline{c}) = p^d \cdot (1-p)^{n-d}.}$$

$d_H(\underline{y}, \underline{c}) = d$. $\triangleq$ Hamming distance between $\underline{y}$ and $\underline{c}$.

<u>Ex:</u> $\underline{y} = 1\,0\,1\,1\,1\,0$.
$\underline{c} = 0\,1\,1\,0\,1\,0$. → $d_H(\underline{y}, \underline{c}) = 3$.

→ Given a received vector $\underline{y}$.

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

$$= \arg\max_{\underline{c} \in \mathbb{C}} p^d (1-p)^{n-d} = \arg\max_{\underline{c} \in \mathbb{C}} (1-p)^n \left(\frac{p}{1-p}\right)^d$$

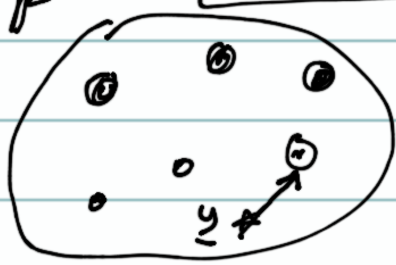
If $\frac{p}{1-p} \leq 1$, i.e, $p \leq \frac{1}{2}$;

then $\hat{\underline{c}} = \arg\max\limits_{\underline{c} \in \mathbb{C}} (1-p)^n \left(\frac{p}{1-p}\right)^d$.

d has to be minimized.

$$\boxed{\hat{\underline{c}} = \arg\min_{\underline{c} \in \mathbb{C}} d_H(\underline{y}, \underline{c})}$$

$\mathbb{F}^n$



$\mathbb{C} \subseteq \mathbb{F}^n$

↳ ML decoding is equivalent to <u>Minimum distance decoding</u>

By distance, we mean Hamming distance.

<u>Hamming Distance</u>

Hamming distance between two vectors $\underline{x}$ and $\underline{y} \in \mathbb{F}^n$. is the no. of positions / coordinates in which $\underline{x}$ and $\underline{y}$ differ.

$$\begin{array}{ll} \underline{x} & 1\,0\,2\,1\,1\,0. \\ \underline{y} & 0\,0\,1\,0\,1\,0 \end{array} \quad d_H(\underline{x}, \underline{y}) = 3.$$

Properties:-

① $d_H(\underline{x}, \underline{y}) \geq 0$. (Positive)

② $d_H(\underline{x}, \underline{y}) = d_H(\underline{y}, \underline{x})$. (Symmetric).

③. $d_H(\underline{x}, \underline{z}) \leq d_H(\underline{x}, \underline{y}) + d_H(\underline{y}, \underline{z})$. (Triangle Inequality).

# of flips from $\underline{x}$ to $\underline{y}$ → $\underline{y}$ → # of flips from $\underline{y}$ to $\underline{z}$

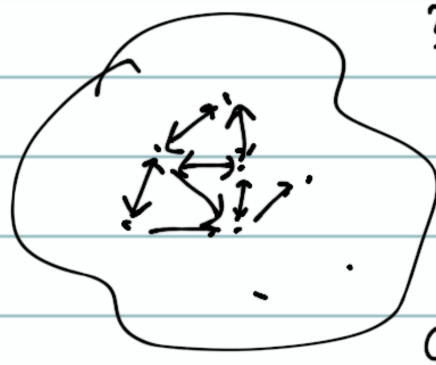
$\underline{x}$ → # of flips → $\underline{z}$. ← Some flips have to be undone

Parameter of a Block Code.

Minimum Distance of a Block Code.

Defn:-

$$d(\mathbb{C}) = d_{min}(\mathbb{C}) = \min_{\substack{\underline{x}, \underline{y} \in \mathbb{C}: \\ \underline{x} \neq \underline{y}}} d_H(\underline{x}, \underline{y}).$$



(n, M) block Code

(n, M, d) block Code.

d = minimum distance of the block code.

Examples of Codes

① n-fold repetition. $\rightarrow (n, 2, n)$

② Simple parity check code. $\rightarrow (n, 2^{n-1}, 2)$

③ (7,4) Hamming Code. $\rightarrow (7, 2^4, 3)$

$\rightarrow$ Minimum distance of a code determines the error detection capability & error correction capability.

Error Detection

Consider a (n, M, d) block code $\mathbb{C}$

Claim: There is a decoder $\mathcal{D}$ for the code $\mathbb{C}$ which can detect upto $(d-1)$ errors.

Proof:

$$\mathcal{D}(\underline{y}) = \begin{cases} \underline{y} & \text{if } \underline{y} \in \mathbb{C}. \\ \text{Error} & \text{otherwise}. \end{cases}$$

$\underline{c} \longrightarrow \underline{y}$ s.t. $d_H(\underline{y}, \underline{c}) \leq d-1$

If $d_H(\underline{y}, \underline{c}) \neq 0$ & $d_H(\underline{y}, \underline{c}) \leq d-1$, then $\underline{y} \notin \mathbb{C}$.

Error Correction

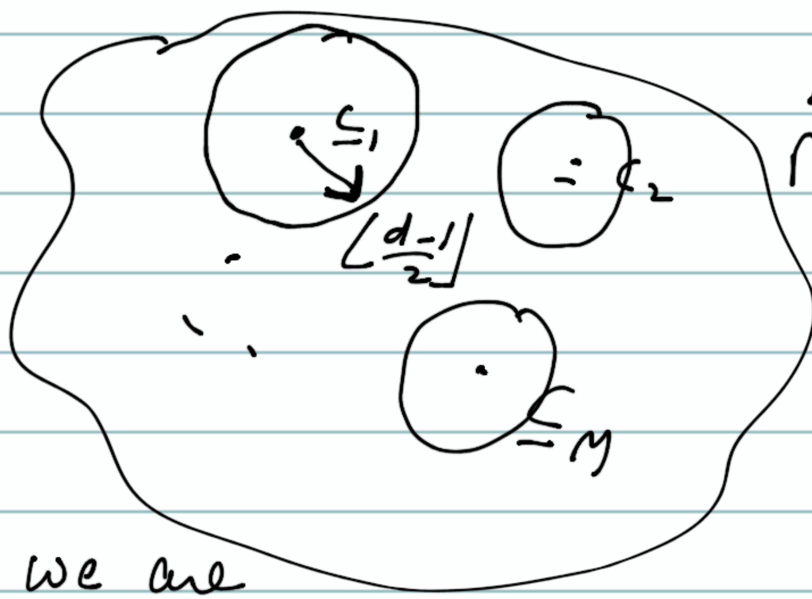
Consider a (n, M, d) block code $\mathbb{C}$.

Claim: There is a decoder for $\mathbb{C}$ that corrects upto $\lfloor \frac{d-1}{2} \rfloor$ errors.

Proof: Decoder is minimum distance decoder.

$$D(\underline{y}) = \arg\min_{\underline{c} \in \mathbb{C}} d_H(\underline{y}, \underline{c}).$$

$\lfloor x \rfloor$ = largest integer less than or equal to x.



$$B\left(\underline{c}_i, \left\lfloor \frac{d-1}{2} \right\rfloor\right) \cap B\left(\underline{c}_j, \left\lfloor \frac{d-1}{2} \right\rfloor\right) = \phi.$$

Ball that we are drawing around each codeword is a Hamming ball.

$$B(\underline{c}, t) = \{ \underline{y} \in \mathbb{F}^n : d_H(\underline{y}, \underline{c}) \le t \}$$

$$d_H(\underline{c}_i, \underline{c}_j) \geq d$$

$$\underline{y} \in B(\underline{c}_i, \lfloor \tfrac{d-1}{2} \rfloor)$$

$$d_H(\underline{y}, \underline{c}_i) \leq \lfloor \tfrac{d-1}{2} \rfloor.$$

$$d \leq d_H(\underline{c}_i, \underline{c}_j) \leq d_H(\underline{y}, \underline{c}_i) + d_H(\underline{y}, \underline{c}_j).$$

$$d_H(\underline{y}, \underline{c}_j) \geq d - \lfloor \tfrac{d-1}{2} \rfloor.$$

$$> \lfloor \tfrac{d-1}{2} \rfloor$$

$$\underline{y} \notin B(\underline{c}_j, \lfloor \tfrac{d-1}{2} \rfloor).$$

All the Hamming balls are disjoint.