19/1 Recap (Tut)

$\mathcal{C} \rightarrow (n, M, d)$ Block code

$M \downarrow$ # codewords

$$d = \min_{\substack{c_1, c_2 \in \mathcal{C} \\ c_1 \neq c_2}} d_H(c_1, c_2)$$

$$d_H(c_1, c_2) = \sum_{i=1}^{n} \mathbb{1}_i$$

$$\mathbb{1} = \begin{cases} 1 & (c_1)_i \neq (c_2)_i \\ 0 & \text{o/w} \end{cases}$$

→ Properties

All 3 satisfied ⇒ Metric

1. $d_H(c_1, c_2) \geq 0$
2. Commutative
3. $d_H(c_1, c_2) \leq d_1(c_1, c_3) + d_1(c_1, c_2)$

A 1) Let us assume $\exists\, y \in F_2^7$: $d_H(y, c_1) = 1$

Hamming ⇒ (7, 16, 3) contradicts inference $d_H(y, c_2) = 1$

$\triangle$ ineq ⇒ $\boxed{d_H(c_1, c_2) \leq 1 + 1 \leq 2}$ → Cannot be True

Discrete Memoryless Ch

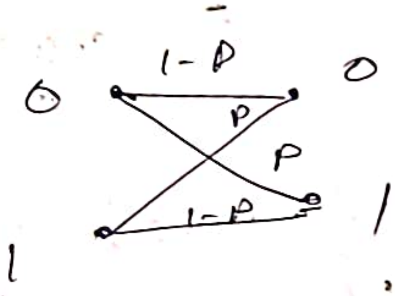
$x \in X \longrightarrow$ DMC $P(y/x) \longrightarrow y \in Y$

① BSC ② BEC ③ AWGN

DMC iff $\longrightarrow P(y/x) = \prod_{i=1}^{n} P(y_i/x_i)$

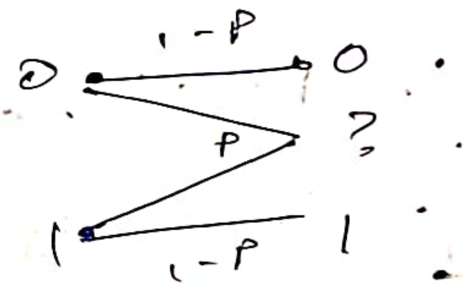
① BSC

$$P(y/x) = \begin{cases} p & ; x \neq y \\ 1-p & ; x = y \end{cases}$$



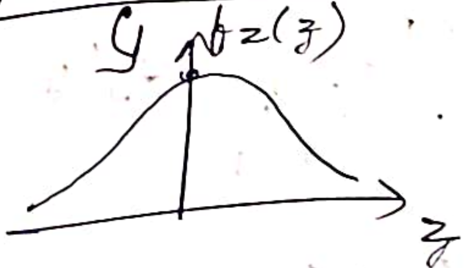
② BEC

$$P(y/x) = \begin{cases} p & ; x \neq y \\ 1-p & ; x = y \end{cases}$$



③ AWGN

$x \longrightarrow$ AWGN $Z \sim N(0, \sigma^2) \longrightarrow Y = x + Z$



$Y = x + Z$

$Y - x = Z$

$\rightarrow f(y/x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2}\left(\frac{y-x}{\sigma}\right)^2}$

MAP Decoder

$$P_e = P(\hat{c} \neq c / y)$$
$$= 1 - P(\hat{c} = c / y)$$

$$\hat{c} = \underset{\underline{c} \in \mathcal{C}}{\arg\max}\ P(\underline{c} / \underline{y})$$

$$= \underset{\underline{c} \in \mathcal{C}}{\arg\max}\ P(\underline{y} / \underline{c}) \cdot P(\underline{c})$$

[$P(\underline{y})$ is not relevant ∵ it is $\underset{\underline{c}}{\arg\max}$]

If code is uniformly coded,
then $P(\underline{c}) = \frac{1}{|\mathcal{C}|} = \frac{1}{M}$

∵ $P(\underline{c})$ become constant, it can be neglected

$$\boxed{\Rightarrow \hat{c} = \arg\max P(\underline{y} / \underline{c})} \rightarrow \text{ML Decoder}$$

A3) $\hat{c} =$ "

$$P(\underline{y}/\underline{c}) = p^{d_H(\underline{y},\underline{c})} \cdot (1-p)^{n-d_H(\underline{y},\underline{c})}$$

$$= (1-p)^n \cdot \left(\frac{p}{1-p}\right)^{d_H(\underline{y},\underline{c})}$$

$$\hat{c} = \underset{c \in \mathcal{C}}{\arg\max}\ P(\underline{y} / \underline{c})$$

min H. dist. decoder.

$$\Rightarrow \boxed{\hat{c} = \underset{c \in \mathcal{C}}{\arg\min}\ d_H(\underline{y}, \underline{c})}$$

b) $(01010) \longrightarrow 00010$.

ML => uniform encoding

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

$\Rightarrow \underline{y} = (00010) \begin{cases} \to 00000 & 1 \\ \to 01010 & 1 \\ \to 10101 & 4 \\ \to 11111 & 4 \end{cases}$ d_H

$\left.\begin{matrix}1\\1\end{matrix}\right\}$ => 50% chance to get correctly decoded

---

A) for AWGN, $f(y/x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-y)^2}{2\sigma^2}}$

MAP $\Rightarrow \hat{c} = \arg\max_{\underline{c} \in \mathcal{C}} f_{Y/X}(y/x) \cdot P(\underline{c})$

uniformly distributed => Reduce to ML

$\Rightarrow \hat{c} = \arg\max_{\underline{c} \in \mathcal{C}} f_{Y/X}(y/x)$

$= \arg\max_{\underline{c} \in \mathcal{C}} \prod_{i=1}^{n} P(y_i/c_i)$

$= \frac{1}{(2\pi\sigma^2)^{n/2}} e^{-\frac{1}{2\sigma^2}\left[\underbrace{(x_1-y_1)^2 + (x_2-y_2)^2 \cdots + (x_n-y_n)^2}_{\text{minimize this}}\right]}$

We know $\|y - c\|^2 = \sum_{i=1}^{n} (y_i - c_i)^2$

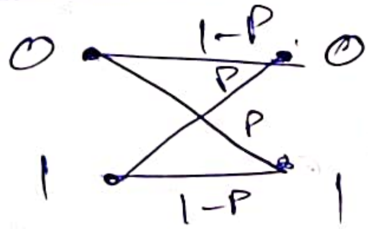
$$= (y_1^2 + y_2^2 \dots) + (c_1^2 + c_2^2 \dots)$$
$$- 2(y_1 c_1 + y_2 c_2 \dots)$$

Bipolar $\Rightarrow \{1, -1\}$

$$= \underbrace{n - 2\langle y, c \rangle}_{\text{to minimize this,}}$$

we max $\langle y, c \rangle$

i.e. $\underset{c \in \mathcal{C}}{\arg\max} \langle y, c \rangle$

A5) 

$$P_e(y/x) = \begin{cases} P ; & y \neq x \\ 1-P ; & y = x \end{cases}$$

~~For n length,~~ $\cancel{P_e = p^r (1-p)^{n-r}}$

Rep code $\Rightarrow k = 1,\ n,\ \cancel{d = \left\lfloor \frac{n-1}{2} \right\rfloor}$ $d_{min} = n$

$\hookrightarrow (n, 2, n$ [redacted] $)$

$$t_c = \left\lfloor \frac{n-1}{2} \right\rfloor, \quad t_d = n-1$$

$$P_e = \sum_{i = t_c + 1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

$\therefore P_e = \sum_{i=0}^{i=n-t-1} \binom{n}{i} (1-p)^i \, p^{n-i}$

For odd $\rightarrow i = \frac{n-1}{2}$

For even $\rightarrow \frac{n-1}{2} - 1$

---

6) $V_2(x, n, t) = \{ y : d_H(x, y) \leq t \}$

$|V_2(x, n, t)| = ?$

$= \sum_{i=0}^{t} \binom{n}{i}$

Tut 2

Linear code $\longrightarrow \mathcal{C} \rightarrow (n, k, d)$ — subspace of $\mathbb{F}_2^n$

$$= \{ mG \; \forall m \in \mathbb{F}_2^k \}$$

- Rank $(G) = k$ ($\because$ k lin ind rows)

$G = [A \mid B]$

$A^{-1}G = [I \mid A^{-1}B] = [I \mid P]$

$G' = [I \mid P]$

- $\dim(C) = k = \text{rank}(G) \longrightarrow |\mathcal{C}| = 2^k$, $\boxed{\dim(C) = \log_2 |\mathcal{C}|}$

~~$d_{H,\min}(x, y) = w_H(x) + w_H(y)$~~

- $d_{H,\min} = w_{H,\min}$ for LBC.

A1) $\mathcal{C} \rightarrow (n, k)$

M1

$c = (m_1 \ldots m_i \ldots m_k)$ $\begin{bmatrix} \cdots & j\text{th} & \\ & 0 & \\ & 1 \leftarrow i\text{th} & \\ & 0 & \end{bmatrix} = (c_1 \ldots c_j \ldots c_n)$

$m_i = 1$ (say)

$k-1$ other bits

only one 1 in this row by RT.

fixing ~~ith~~ $m_i = 1$

$\Rightarrow c_j = 1$ always.

$\Rightarrow 2^{k-1}$ possible codewords

M2

$\mathcal{C}_0 = \{ c \in \mathcal{C} \mid c_i = 0 \}$, $\mathcal{C}_1 = \{ c \in \mathcal{C} \mid c_i = 1 \}$

$|\mathcal{C}_0| + |\mathcal{C}_1| = |\mathcal{C}| = 2^k$. (Prove $|\mathcal{C}_0| = |\mathcal{C}_1|$

3) $n = 8$

$k = 4$

$G = [I \mid P]$

$c = m \cdot G$

$\vdots$ rord

$$\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$$

$$\text{Ans} \Rightarrow \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \Rightarrow$$

$\cancel{10010110}$

4) $C_1 \Rightarrow (n_1, k_1, d_1)$

$C_2 \Rightarrow (n_2, k_2, d_2)$

$$C = \{(u|v) : u \in C_1, v \in C_2\} \longrightarrow (2n, k, d)$$

$$n = n_1 + n_2 = 2n$$

$$k = \log_2 |C|$$

for ~~each~~ each u, $\exists$ 2^{k_2} vs

Also, $\exists$ 2^{k_1} u values

$\Rightarrow$ Total c.w $= 2^{k_1 + k_2}$

$$k = k_1 + k_2$$

$$d = \min(d_1, d_2)$$

5) $C_1 \to (n, k_1, d_1)$
$C_2 \to (n, k_2, d_2)$

$C = \{ u \mid u+v \}$

$n = 2n$

$k = k_1 + k_2$

~~$d_{min} = (d_1, d_2)$~~

$d_{min} = (2d_1, d_2)$

Proof
$C = (c_1 \mid c_1 + c_2 ; \dots)$
$\to$ Plotkin construction

[Can also be ~~used~~ proved using G_1 & G_2]

$C_1 \to \quad G \to [\, I_{k_1 \times k_1} \mid P_{k_1 \times n-k_1}]$

$C_2 \to \quad G \to [\, I_{k_2 \times k_2} \mid P_{k_2 \times n-k_2}]$

$C = (m_1 G_1 \mid m_1 G_1 + m_2 G_2)$

$\Rightarrow C = [m_1 \;\; m_2] \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix} \to (k_1 + k_2 \times 2n)$

$\Rightarrow k$ proved