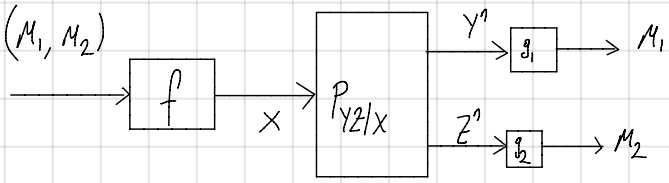
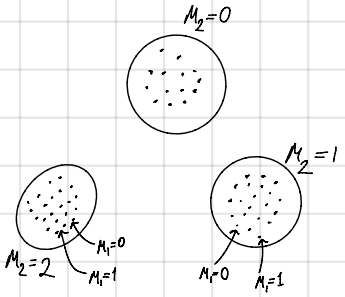
10/20/2016
Thursday

Broadcast Channel: (Cover 1972)



Capacity Region: an open problem.



↳ Better receiver decodes both.

Superposition Code:

Cluster codewords specified by "auxiliary" R.V.

Choose: P_{UX}: First layer: $C_U = \{U^n(m_2)\}_{m_2=1}^{2^{nR_2}}$ $\quad U^n(m_2) \sim \prod_{\text{indep.}} P_U$

Second layer: $C_X(m_2) = \{X^n(m_1)\}_{m_1=1}^{2^{nR_1}}$ $\quad X^n(m_1) \sim \prod_{i=1}^{n} P_{X|U_i(m_2)}$

These are conditionally indep. given U^n

↳ cond. indep. given $U^n(m_2)$

Transmit: $X^n(m_1, m_2) = X^n(m_1)$ from $C_X(m_2)$

Decoder 1: Find unique (m_1', m_2') s.t. $(X^n(m_1', m_2'), Y^n) \in T_\varepsilon^{(n)}$

Decoder 2: Find unique m_2' s.t. $(U^n(m_2'), Z^n) \in T_\varepsilon^{(n)}$

w.r.t. $P_{XU}\, P_{YZ|X}$ $\quad (U - X - (Y, Z))$

Error: Assume $(1,1)$ is transmitted.

Error 1: $(X^n(1,1), Y^n) \notin T_\varepsilon^{(n)}$ or $(U^n(1), Z^n) \notin T_\varepsilon^{(n)}$

Negligible because $P[(U^n(1), X^n(1,1), Y^n, Z^n) \in T_\varepsilon^{(n)}] \to 1$

Error 2: (Decoder 1): A.) $\exists m_2' \neq 1$, m_1' s.t. $(X^n(m_1', m_2'), Y^n) \in T_\varepsilon^{(n)}$

B.) $\exists m_1' \neq 1$ s.t. $(X^n(m_1', 1), Y^n) \in T_\varepsilon^{(n)}$

$$\mathbb{P}[\text{error 2.A}] \leq 2^{n(R_1+R_2)} \cdot 2^{-n(I(X;Y)-2\varepsilon)}$$

$$\mathbb{P}[\text{error 2.B}] \leq 2^{nR_1} \cdot 2^{-n(I(X;Y|U)-2\varepsilon)}$$

Error 3 (Decoder 2): $\exists m_2' \neq 1$ s.t. $(U^n(m_2'), Z^n) \in T_\varepsilon^{(n)}$

$$\mathbb{P}[\text{error 3}) \leq 2^{nR_2} \cdot 2^{-n(I(U,Z)-2\varepsilon)}$$

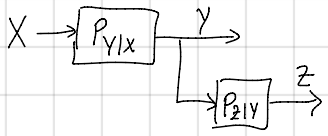
Achievable rates

$$R_1 \leq I(X;Y|U) \qquad (1)$$

$$R_2 \leq I(U;Z) \qquad (2)$$

$$R_1+R_2 \leq I(X;Y) \qquad (3)$$

Degraded: $P_{YZ|X} = P_{Y|X} P_{Z|Y}$ i.e. $X-Y-Z$ for an P_X



In this case: $I(X;Y) \geq I(X;Z)$

(1) and (2) $\Rightarrow$ (3)

$\rightsquigarrow R_1+R_2 \leq I(X;Y|U) + I(U,Z)$

$\leq I(X;Y|U) + I(U;Z)$

$= I(U,X;Y)$

$= I(X;Y)$

So for degraded case we need

$$R_1 \leq I(X;Y|U) \qquad (1)$$

$$R_2 \leq I(U;Z) \qquad (2)$$

~~$R_1+R_2 \leq I(X;Y)$ (3)~~ Automatic!

Cover's Conjecture: This, i.e. $C = \left\{ (R_1, R_2) : \begin{array}{l} \exists P_{X,U} \text{ s.t.} \\ R_1 \le I(X;Y|U) \\ R_2 \le I(U;Y) \\ |\mathcal{U}| \le \min\{|\mathcal{X}||\mathcal{Y}|, |\mathcal{Z}|\} + 1 \end{array} \right\}$ is optimal for degraded BC.

Gallager Proved this conjecture. (1974)

Converse:

$\exists$ enc.-dec. s.t. they achieve ε error $\forall \varepsilon > 0$

$$nR_1 = H(M_1)$$

$$= I(M_1; Y^n) + H(M_1|Y^n) \quad \text{(Fano)}$$

$$\le I(M_1; Y^n | M_2) \quad M_1 \perp\!\!\!\perp M_2$$

$$\le I(X^n; Y^n | M_2) \quad \text{D.P.I.}$$

$$= \sum_{i=1}^{n} I(X^n; Y_i | M_2, Y^{i-1}) \quad \leftarrow (M_2 Y^{i-1} X^{i-1} X_{i+1}^n) - X_i - Y_i$$

$$= \sum_{i=1}^{n} I(X^n; Y_i | M_2, Y^{i-1})$$

$$nR_2 = H(M_2)$$

$$= I(M_2; Z^n) + H(M_2|Z^n) \quad \text{(Fano)}$$

$$= \sum I(M_2; Z_i | Z^{i-1})$$

$$\le \sum I(M_2, \cancel{Z^{i-1}}, Y^{i-1}; Z_i)$$

$$= \sum I(M_2, Y^{i-1}; Z_i)$$

Define $T \sim \text{Unif}\{1, \dots, n\}$

↳ Random Time:

$$nR_1 \le n I(X_T; Y_T | M_2 Y^{T-1}, T) + \text{Fano}$$

$$= n I(X; Y|U) + \text{Fano}$$

$U = (M_2, Y^{T-1}, T)$

$X = X_T$

$Y = Y_T$

$Z = Z_T$

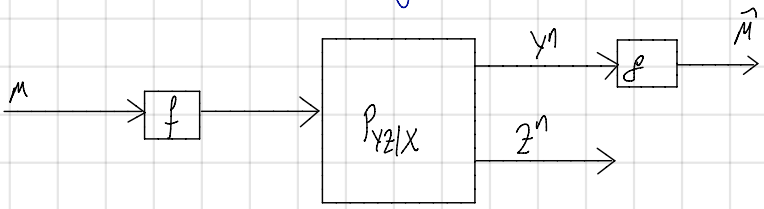
$$nR_2 \le n I(M_2 Y^{T-1}; Z_T | T) + \text{Fano}$$

$$\le n I(M_2 Y^{T-1} T; Z_T) + \text{Fano}$$

$$= n I(U, Z) + \text{Fano}$$

Check $P_{YZ|XU}$ of construction matches $P_{YZ|X}$ of channel

Wiretap Channel: (Wyner 1975)



Two goals: 1.) Reliable Communication

2.) Z^n contains nearly no info about M (i.e. Perfect secrecy)

Achievability: $\forall \varepsilon > 0$ $\exists n, f, g$ s.t.

$$\mathbb{P}[M \neq \hat{M}] < \varepsilon$$

$$\frac{1}{n} I(M, Z^n) < \varepsilon \qquad \text{(now called weak secrecy)}$$

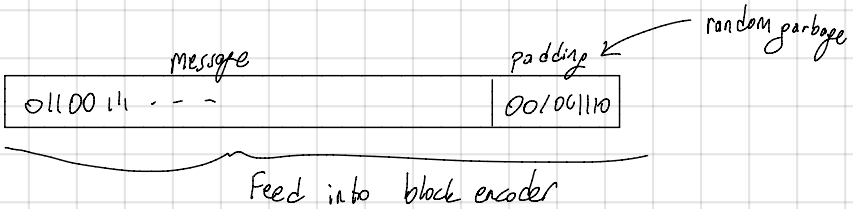
"Secrecy capacity": Sup of achievable rates

Wyner's Thm: For degraded channels

$$C_s = \max_{P_X} \left(I(X;Y) - I(X;Z) \right) = \max_{P_X} I(X;Y|Z)$$

Achievability proof: Some encoding as point to point channel.

Main idea: Pad to message with random bits



Wyner's Analysis:

Let $R < I(X;Y) - I(X;Z)$ for some P_X

Let $R_s \in (I(X;Z) - \varepsilon, I(X;Z))$

↳

Notice

$$R + R_p < I(X;Y)$$

Random codebook: $C = \{X^n(m, m_p)\}_{m=1}^{2^{nR}}{}_{m_p=1}^{2^{nR_p}} \sim \prod P_X$

Decoding: From prev. proofs, $\exists f$ s.t. $P[M \neq \hat{M}] < \varepsilon$ when n large

Secrecy: Notice that M_p is decodable from M and Z^n.

$\exists f_2$ for eavesdropper s.t. $P[M_p \neq f_2(M, Z^n)] \in \varepsilon'$

$M \times Z^n \longrightarrow \hat{M}_p$ $\Rightarrow H(M_p | M Z^n) \leq \varepsilon' n R + 1$ (Fano)

$$I(M, M_p; Z^n) = \boxed{I(M, Z^n)} + I(M_p; Z^n | M)$$

$\vdots$

$n I(X, Z)$ → to be explained.

$I(M_p; Z^n | M) = H(M_p | M) - H(M_p | Z^n)$

$H(M_p | M) = H(M_p) = nR_p$

$H(M_p | Z^n)$ small