Notice

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

Random Codebook: $\mathcal{C} = \left\{ X^n(m, m_g) \right\}_{m=1}^{2^{nR}} \ {}_{m_g=1}^{2^{nR_g}} \sim \prod P_X$

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

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

$\exists g_2$ for eavesdropper s.t. $\mathbb{P}[M_g \neq g_2(M, Z^n)] \leq \varepsilon'$

$\mathcal{M} \times Z^n \longrightarrow \hat{\mathcal{M}}_g \qquad \Rightarrow H(M_g | M Z^n) \leqslant \varepsilon' n R + 1$ (fano)

$$I(M, M_g; Z^n) = \boxed{I(M, Z^n)} + \underbrace{I(M_g; Z^n | M)}_{\underbrace{H(M_g|M)}_{\underbrace{H(M_g)}_{nR_g}} - \underbrace{H(M_g|Z^n)}_{\text{small}}}$$

$$\leq nI(X,Z)$$

to be explained.

10/25/2016
Tuesday

Converse: Wiretap channel (Degraded)

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

Z

We want to show:

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

Z

Assume n, f, g at rate R satisfy $\mathbb{P}[M \neq \hat{M}] \leq \varepsilon$ (ε arbitrarily small)

$\frac{1}{n} I(M; Z^n) \leq \varepsilon \rightarrow$ (secrecy requirement)

$$P_{Y^n Z^n | X^n} = \prod P_{YZ|X}$$

$$nR = H(M)$$

$$= I(M;Y^n) + H(M|Y^n)$$ Fano will handle

$$\leq \underbrace{I(M;Y^n) - I(M;Z^n)}\ + n\varepsilon + H(M|Y^n)$$

$$= I(M;Y^n|Z^n) \quad \text{(because it's degraded)}$$

$$\leq I(X^n;Y^n|Z^n) \quad (\text{D.P.I}) \quad (M - X^n - Y^n - Z^n)$$

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

$$= \sum_{i=1}^{n} I(X_i;Y_i|Z^n, Y^{i-1}) \leftarrow \left((Z^{i-1} Z_{i+1}^n Y^{i-1} X^{i-1} X_{i+1}^n) - (Z_i X_i) - Y_i\right)$$ because of memoryless channel

$$\leq \sum_{i=1}^{n} I(X_i;Y_i|Z_i) \quad \left(\text{recall } I(A;B) \geq I(A;B|C) \quad A-B-C\right)$$

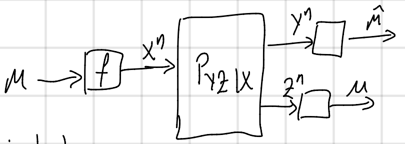
$$= n\, I(X_T;Y_T|Z_T,T)$$

$$\leq n\, I(X_T;Y_T|Z_T) \quad T - X_T - Y_T - Z_T \quad \text{(because of memoryless channel)}$$

Complete solution: Csiszar – Körner

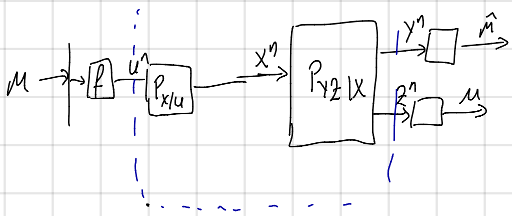
Thm: $C_S = \max_{P_{XU}} \left(I(U;Y) - I(U;Z)\right)$ wrt $P_{XU} P_{YZ|X}$

$U - X - (YZ)$



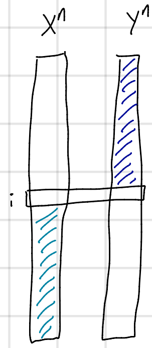
(instead do

new channel



$P_{YZ|U}$ ← Achievability follows from Weiner's proof!

Converse of the complete solution by Csiszar-Körner



Csizsár's sum:

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

proof: Add $I(X_{i+1}^n ; Y^{i-1} | U)$ to both sides

$$\Rightarrow \quad lhs = \sum_{i=1}^{n} I(X_{i+1}^n ; Y^i | U)$$

$$rhs = \sum_{i=1}^{n} I(X_i^n ; Y^{i-1} | U)$$

$$lhs - rhs = \sum_{i=1}^{n} \left(I(X_{i+1}^n ; Y^{i-1} | U) - I(X_i^n ; Y^{i-1} | U) \right)$$

Telescopes

$$= I(X_{n+1}^n ; \cancel{Y^n} | U) - I(\cancel{X^n} ; Y^0 | U)$$

0 $\qquad$ 0

$$= 0 \quad \checkmark$$

proof of the converse

$$nR = \underbrace{I(M; Y^n) - I(M; Z^n)}_{\text{not degraded, cannot combine.}} + n\varepsilon + \text{Fano}$$

$$= \sum_{i=1}^{n} I(M; Y_i | Y^{i-1}) - I(M; Z_i | Z_{i+1}^n)$$ (Chain rule in the first, reversed chain rule in second)

$$= \sum_{i=1}^{n} I(M, Z_{i+1}^n ; Y_i | Y^{i-1}) - I(M, Y^{i-1} ; Z_i | Z_{i+1}^n)$$ (Csiszar's sum identity)

↳ $\sum I(Z_{i+1}^n, Y_i | Y^{i-1}, M) = \sum I(Y^{i-1}; Z_i | Z_{i+1}^n, M)$

$$= \sum_{i=1}^{n} I(M; Y_i | Y^{i-1}, Z_{i+1}^n) - I(M; Z_i | Y^{i-1} Z_{i+1}^n)$$ (Again Csiszar's identity)

Let $V_i = (Y^{i-1}, Z_{i+1}^n)$ $\qquad X = X_T \qquad Z = Z_T$

$U_i = (M, V_i)$ $\qquad Y = Y_T \qquad U = U_T \qquad V = V_T, T$

Go to next page

$= n\, I(M, Y_T \mid Y^{T-1}, Z_{T+1}^{n}, T) - n\, I(M; Z_T \mid Y^{T-1}, Z_{T-1}^{n}, T)$

$= n\, I(U; Y \mid V) - n\, I(U; Z \mid V)$

$\leq n. \max I(u_i; Y \mid V=v) - I(U; Z \mid V=v)$

Consider $P_{UXYZ|V=v}$ satisfies thm statement

<u>Check</u>: cond. on V

$U - X - YZ$

$P_{YZ|X}$ matches channel.