12/08/2016
Thursday

Wyner-Ziv Achievability:

Choose $\bar{P}_{U|X}$ s.t. $R < I(U;X|Y) = I(U;X) - I(U;Y)$

$$R' \in \left(I(U;X) - R,\ I(U;Y)\right)$$

$$\Rightarrow R + R' > I(U;X)$$

$$R' < I(U;Y)$$

Codebook $\{U^n(m,m')\} \sim \bar{P}_U$

<u>Standart Method:</u>

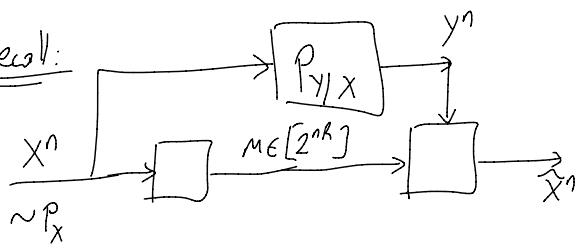
success w.h.p. because $R+R' > I(U;X)$

Encoder finds (m,m') s.t. $(U^n(m,m'), X^n) \in T_\varepsilon^{(n)}$, send m

Decoder finds unique m'' s.t. $(U^n(m,m''), Y^n) \in T_{\varepsilon'}^{(n)}$

received m. $\varepsilon' > \varepsilon$

<u>Recall:</u>



ASIDE:

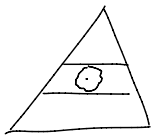
$P_{UXY} = P_{UX} P_{Y|X}$

$U - X - Y$

$(U^n, X^n) \in T$ $\overset{?}{\Longrightarrow}$ $(U^n, X^n, Y^n) \in T$

$(X^n, Y^n) \in T$

NO!



Analysis: If encoder works properly, $(u^n(m,m'), X^n) \in T_\varepsilon^{(n)}$,

$$Y^n \sim \bar{P}_{Y^n|X^n=x^n} = \bar{P}_{Y^n|X^n=x^n,\, U^n=u^n(m,m')} \implies (u^n(m,m'),\, x^n,\, Y^n) \in T_{\varepsilon'}^{(n)} \text{ w.h.p. as } n\to\infty$$

$U - X - Y$

One technical complication: $\forall m'' \neq m'$: We want $\mathbb{P}[u^n(m,m''), Y^n) \in T_{\varepsilon'}^{(n)}]$ small $2^{-nI(U;X)}$

chosen by encoder

If indep. then easy

but Encoder look at all $u^n \in \mathcal{C}_u$ so they are not independent

But we'll do LE and not worry about this technicality at all.

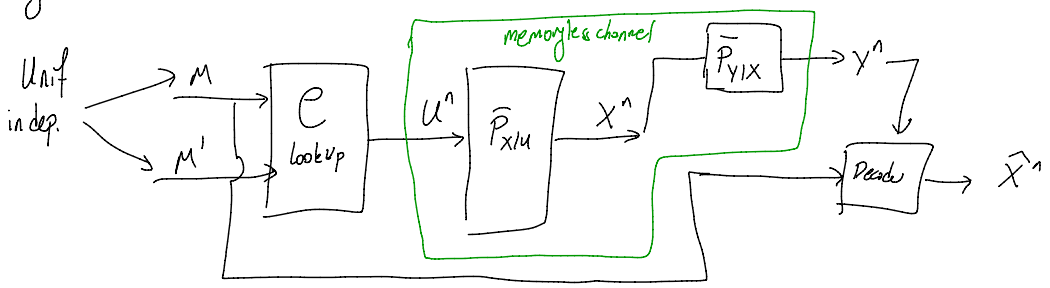
<u>LE Proof:</u>

<u>Encoder</u> uses LE on pairs (m,m') and sends m.

<u>Decoder</u> looks at $\{u^n(m,m'')\}_{m''=1}^{2^{nR'}}$

↳ Decodes m' using any good channel decoder

Analysis: Ideal distr. (due to SCL)



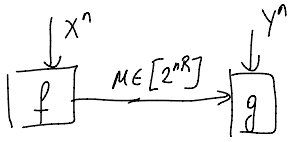
→ This is a channel coding problem. Codebook is iid $\sim \bar{P}_U$ (as used to achieve capacity)

→ See Eva's paper for certain details.

Key Agreement (no eavesdropper)

2 Nodes

One-direction of Communication



$$C_k = \max_{P_{U|X}} I(U;Y)$$

$$\underbrace{I(U;X) - I(U;Y)}_{I(U;X|Y)} \leq R$$

$\leftarrow$ $P_{U|X}$ implies markov chain $P_{U|X} \cdot P_{Y|U}$

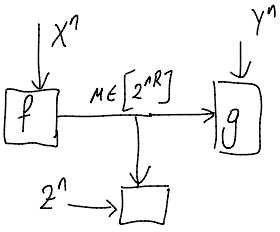
$\rightarrow$ Use Wyner-Ziv encoding, use "bin index" (M') as the key.

Recall:

$$\left.\begin{aligned} R &> I(V;X|Y) \\ R' &< I(U;Y) \end{aligned}\right\} \Rightarrow \text{Let } R' \approx I(U;Y)$$

With LE, $M \perp\!\!\!\perp M'$ under Q.

$\rightarrow$ Key agreement with observation Z at eavesdropper.



No rate limit
(Ahlswede Csiszar)

$$C_k = \max_{P_{UV|X}} I(V;Y|U) - I(V;Z|U)$$

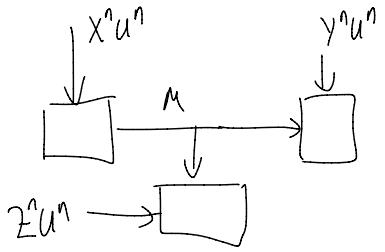
Achievability: First Consider $U = \emptyset$

$$C_k \geq \max_{P_{V|X}} I(V;Y) - I(V;Z)$$

$\rightsquigarrow$ Again, use Wyner-Ziv coding, LE makes this Wiretap channel.

Now, $U \neq \emptyset$. Encoder generates $U \sim \bar{P}_{U|X}$

Send U^n (don't worry about compression)



$$C_k \geq \max_{\substack{P_{V|XU} \\ P_{U|X}}} I(V;Y,U) - I(V;Z,U)$$

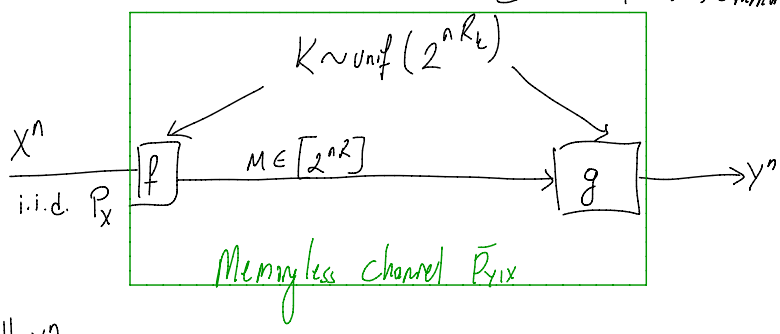
<u>with rate constraint</u> (Csiszar Narayan)

$$C_k = \max_{P_{UV|X}} I(V;Y|U) - I(V;Z|U)$$

$$\underbrace{I(U,V;X) - I(U,V;Y)}_{I(U,V;X|Y)} \leq R$$

superposition code.

← think of this as common randomness.



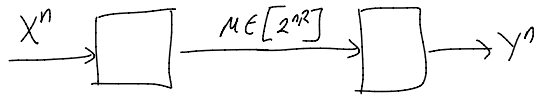
$K \perp\!\!\!\perp X^n$

"Distributed Channel Synthesis"

result of our system.

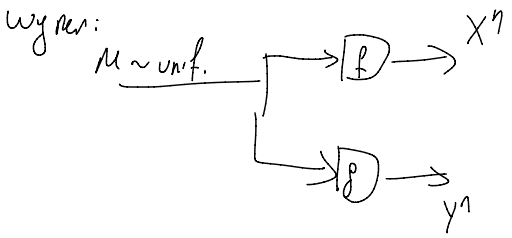
$$\| P_{X^n} P_{Y^n|X^n} - P_{X^n} \bar{P}^n_{Y|X} \|_{TV} < \varepsilon$$

$\rightsquigarrow$ First look at no Common Randomness



$R = I(X;Y)$?

wyner:



$$R \geq C_\omega(X,Y) = \min_{X-U-Y} I(X,Y;U)$$

Fix $\bar{P}_{U|XY}$

which give $\bar{P}_{UXY}$

s.t. $X-U-Y$

code book $\sim P_U$