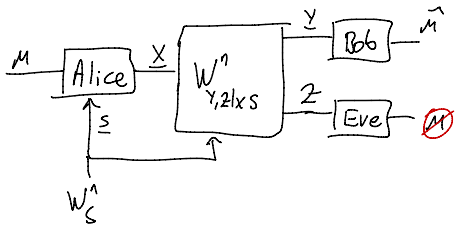
12/01/2016
Thursday

Gelfand-Pinsker WTC:



Product channel:

$$\mathbb{P}[\underline{Y}=\underline{y}, \underline{Z}=\underline{z} \mid \underline{X}=\underline{x}, \underline{S}=\underline{s})$$

$$= \prod_{i=1}^{n} W_{Y,Z|X,S}(y_i, z_i | x_i, s_i)$$

$$\triangleq W^n_{Y,Z|X,S}(\underline{y}, \underline{z} | \underline{x}, \underline{s})$$

Some additional Definitions:

Code = An (n,R) code C_n for the GP-WTC has

1) A message set: $\mathcal{M}_n \triangleq [1:2^{nR}]$

2) Encoder (stochastic): $f_n : \mathcal{M}_n \times S^n \longrightarrow \mathcal{P}(X^n)$ where $\mathcal{P}(X^n)$ is the set of all probability mass functions (PMFs) over X^n.

$P_{\underline{X}|M,\underline{S}}$ $\quad \underline{X} \sim P_{\underline{X}|M=m, S=\underline{s}}$

3) Decoder $\varphi_n : \mathcal{Y}^n \longrightarrow \hat{\mathcal{M}}_n$ where $\hat{\mathcal{M}}_n = \mathcal{M}_n \cup \{e\}$ $\quad e \notin \mathcal{M}_n$

- Induced Distribution: For any $P_M \in \mathcal{P}(\mathcal{M}_n)$ the induced distr. by an (n,R) code C_n is

$$P^{(C_n)}(\underline{S}\, M\, \underline{X}\, \underline{Y}\, \underline{Z}\, \hat{M}) = \underbrace{W^n_S(\underline{s})}_{P^{(C_n)}(s)} \underbrace{P_M(m)}_{P^{C_n}_{M|\underline{S}}} f_n(\underline{x}|m,\underline{s})\, W^n_{YZ|X,S}(\underline{y}, \underline{z} | \underline{x}, \underline{s})\, \mathbb{1}_{\{\hat{m}=\varphi_n(\underline{y})\}}$$

Average Error Probability: The average error probability of an (n,R) code c_n is defined as

$$e(c_n) = \frac{1}{|\mathcal{M}_n|} \sum_{m \in \mathcal{M}_n} e_m(c_n)$$

(We don't assume P_M is uniform we write this error because we would like to make discussion simpler)

where $e_m(c_n) \triangleq \mathbb{P}(\varphi_n(\underline{Y}) \neq m \mid M = m)$

Semantic Security: For any (n,R) c_n and $P_M \in \mathcal{P}(\mathcal{M}_n)$ define $\ell(c_n, P_M) = I_{P(c_n)}(M; Z)$

The semantic security metric for the GP-WTC under c_n is

$$\ell(c_n) = \max_{P_M \in \mathcal{P}(\mathcal{M}_n)} \ell(c_n, P_M)$$

Achievability: A rate R is achievable if for any $\varepsilon > 0$, there exists a sequence of (n,R) codes $\{c_n\}_{n \in \mathbb{N}}$ s.t. $\exists N \in \mathbb{N}$ $\forall n > N$ $e(c_n) < \varepsilon$ $\ell(c_n) < \varepsilon$

Result: Denote the semantic security capacity of the GP-WTC by C_{sem}. and for any $q_{U,V,X|S} : \mathcal{S} \to \mathcal{P}(\mathcal{U} \times \mathcal{V} \times \mathcal{X})$ define

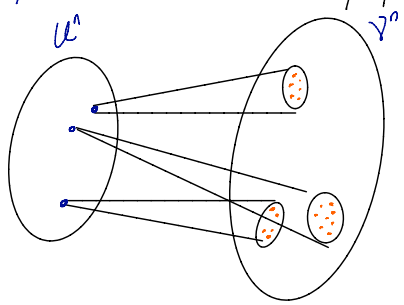
$$\min \begin{cases} I(V,Y|U) - I(V,Z|U), \\ I(U,V;Y) - I(U,V;S) \end{cases}$$

where the underlying joint distribution $W_S\, q_{UV\underline{X}|S}\, W_{Y,Z|\bar{X},S}$ $\quad ((Y,Z) - (X,S) - (U,V))$

A lower bound on C_{sem} is

$$C_{sem} \geq \max_{\substack{q_{UVX|S} \\ I(U|Y) - I(U;S) \geq 0}} R(q_{UVX|S}$$

Main Idea Behind the proof: We use a superposition code construction.



→ U index is a padding (decoy)

→ V layer encoder padding + message

→ All the secrecy comes from V.

Strong soft-covering lemma for superposition codes:

→ This is a key tool for the (both reliability and security) for our superposition coding scheme for GP-WTC.

→ Setup: Fix $q_{UV} \in \mathcal{P}(\mathcal{U} \times \mathcal{V})$ and a channel $q_{W|U,V}$.

Let $\mathcal{B}_U \triangleq \{\underline{U}(i)\}_{i \in \mathcal{I}_n}$ where $\mathcal{I}_n \triangleq [1 : 2^{nR_1}]$ be a collection of $|\mathcal{I}_n|$ random vectors of length n iid $\sim q_U^n$

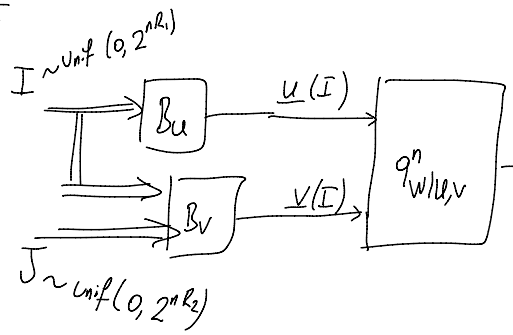
Denote a realization of $\mathcal{B}_U$ by $\mathcal{B}_U \triangleq \{\underline{u}(i)\}_{i \in \mathcal{I}_n}$

→ Fix $\mathcal{B}_U = \{\underline{u}(i)\}_{i \in \mathcal{I}_n}$, and each $i \in \mathcal{I}_n$, let $\mathcal{B}_V(i) = \{\underline{V}(i,j)\}_{j \in \mathcal{J}_n}$ where $\mathcal{J}_n = [1 : 2^{nR_2}]$ is a random outer layer code book with $\underline{V}(i,j) \sim \prod_{k=1}^{n} q_{V|U}(\cdot \mid u_k(i))$ indep. of all the other V-codewords

- Denoting a realization of $\mathcal{B}_V(i)$ by $\mathcal{B}(i)$

$\mathbb{P}(\mathcal{B}_U = \mathcal{B}, \mathcal{B}_V(1) = \mathcal{B}_V(1), \mathcal{B}_V(2) = \mathcal{B}_V(2) \cdots \mathcal{B}_V(2^{nR_1}) = \mathcal{B}_V(2^{nR})$

Model



$\underline{W}$ ~ induced distr. that depends on the codebooks

$$P^{(B_n)}_{\underline{W}}(\underline{w}) = \sum_{i,j \in \mathcal{I}_n \times \mathcal{J}_n} \frac{1}{|\mathcal{I}_n|\,|\mathcal{J}_n|} q^n_{W|U,V}(\underline{w} \mid \underline{u}(i), \underline{v}(i,j))$$

- Induced distr.: Fixed superposition codebook B_n

$$P^{(B_n)}(i,j,u,v,w) = \frac{1}{|\mathcal{I}_n|}\frac{1}{|\mathcal{J}_n|}\mathbb{1}\{u = u(i)\}\,\mathbb{1}\{\underline{V} = v(i,j)\}\, q^n_{W|UV}(\underline{w} \mid \underline{u}, \underline{v})$$

Question: How large should R_1 and R_2 be in order to get $P^{B_n}_{W^n} \approx q^n_W$?

<u>Lemma:</u> For any coding distribution q_{UV} and $q_{W|U,V}$ where $|W| < \infty$ there exists $\delta_1, \delta_2 > 0$ s.t. for sufficiently large n

provided that

$$R_1 > I(U;W)$$
$$R_1 + R_2 > I(U,V;W)$$

$$\mathbb{P}_{B_n}\left(D(P^{(B_n)}_W \| q^n_W) > e^{-n\delta_1}\right) \leq e^{-e^{n\delta_2}}.$$