# Lecture 20



3/17/2011

Error Analysis:

$$\overline{p_e} \equiv \frac{1}{|\mathcal{M}|}\sum_{m=1}^{|\mathcal{M}|} \mathrm{Tr}\{(I - \Lambda_m^{B^n})\, \sigma_{x^n(m)}^{B^n}\}$$

Since $\mathrm{Tr}\{\Pi_{\sigma,\delta}^{B^n}\, \sigma_{x^n}^{B^n}\} \geq 1-\epsilon$

$$\overline{p_e} \leq \frac{1}{|\mathcal{M}|}\sum_{m=1}^{|\mathcal{M}|} \mathrm{Tr}\{(I - \Lambda_m^{B^n})\, \Pi_{\sigma,\delta}^{B^n}\, \sigma_{x^n(m)}^{B^n}\, \Pi_{\sigma,\delta}^{B^n}\} + 2\sqrt{\epsilon} \qquad (*)$$

Now we need Hayashi-Nagaoka:

$$I - (S+T)^{-1/2} S (S+T)^{-1/2} \leq$$

$$2(I-S) + 4T \qquad \text{for } 0 \leq S \leq I, \; T \geq 0$$

(can prove this)

Set $S = \Pi_{\sigma_{x^n(m)},\delta}^{B^n|x^n}$

$T = \sum_{m' \neq m} \Pi_{\sigma_{x^n(m')},\delta}^{B^n|x^n}$

Since $\Pi_{\sigma,\delta}^{B^n}\, \sigma_{x^n(m)}^{B^n}\, \Pi_{\sigma,\delta}^{B^n} \geq 0$, we have

$$(*) \leq \frac{1}{|\mathcal{M}|}\sum_{m=1}^{|\mathcal{M}|} \Big[ 2\,\mathrm{Tr}\{(I - \Pi_{\sigma_{x^n(m)},\delta}^{B^n|x^n})\, \Pi_{\sigma,\delta}^{B^n}\, \sigma_{x^n(m)}^{B^n}\, \Pi_{\sigma,\delta}^{B^n}\}$$
$$+ 4\,\mathrm{Tr}\{\sum_{m'\neq m} \Pi_{\sigma_{x^n(m')},\delta}^{B^n|x^n}\, \Pi\, \sigma_{x^n(m)}^{B^n}\, \Pi^{B^n}\}\Big]$$
$$+ 2\sqrt{\epsilon} \qquad (**)$$

3/17/2011



Consider 1st term:

$$\mathrm{Tr}\left\{\left(I - \Pi^{B^n|X^n}_{\sigma_{x^n(m)},\delta}\right)\Pi^{B^n}_{\sigma,\delta}\,\sigma^{B^n}_{x^n(m)}\,\Pi^{B^n}_{\sigma,\delta}\right\}$$

Again, since $\mathrm{Tr}\left\{\Pi^{B^n}_{\sigma,\delta}\,\sigma^{B^n}_{x^n(m)}\right\} \geq 1-\epsilon$,

the above is less than

$$\mathrm{Tr}\left\{\left(I - \Pi^{B^n|X^n}_{\sigma_{x^n(m)},\delta}\right)\sigma^{B^n}_{x^n(m)}\right\} + 2\sqrt{\epsilon}$$

$$\leq \underset{\substack{\uparrow \\ \text{by conditional typicality}}}{\epsilon} + 2\sqrt{\epsilon}$$

So,

$$(**) \leq 2(\epsilon + 2\sqrt{\epsilon}) + \frac{4}{|M|}\underbrace{\sum_{m=1}^{|M|}\sum_{m'\neq m}\mathrm{Tr}\left\{\Pi^{B^n|X^n}_{\sigma_{x^n(m')},\delta}\,\Pi^{B^n}_{\sigma,\delta}\,\sigma^{B^n}_{x^n(m)}\,\Pi^{B^n}_{\sigma,\delta}\right\}}_{\text{can't really do much of anything w/ this term in the general case}}$$

invoke the random coding argument!

3/17/2011



Consider the expectation of the average error probability over the random choice of code

$$\mathbb{E}_{X'^n}\{\bar{p}_e\} \leq 2(\epsilon + 2\sqrt{\epsilon})$$

$$+ \frac{4}{|\mathcal{M}|} \mathbb{E}_{X'^n}\left\{ \sum_{m=1}^{|\mathcal{M}|} \sum_{m' \neq m} \mathrm{Tr}\left\{ \Pi^{B^n|X^n}_{\sigma_{X^n(m')},\delta} \Pi^{B^n}_{\sigma,\delta} \sigma^{B^n}_{X^n(m)} \Pi^{B^n}_{\sigma,\delta} \right\} \right\}$$

$m' \neq m$ are different

By the way we chose the code, it means that $X^n(m')$ & $X^n(m)$ are independent

then $$= 2(\epsilon + 2\sqrt{\epsilon}) + \frac{4}{|\mathcal{M}|} \sum_{m=1}^{|\mathcal{M}|} \sum_{m' \neq m} \mathrm{Tr}\left\{ \mathbb{E}_{X'^n}\left\{ \Pi^{B^n|X^n}_{\sigma_{X^n(m')},\delta} \right\} \Pi^{B^n}_{\sigma,\delta} \mathbb{E}_{X'^n}\left\{ \sigma^{B^n}_{X^n(m)} \right\} \Pi^{B^n}_{\sigma,\delta} \right\}$$

Note that $\mathbb{E}_{X'^n}\{\sigma^{B^n}_{X^n}\} \leq [1-\epsilon]^{-1} \sigma^{\otimes n}$

then $$\leq 2(\epsilon + 2\sqrt{\epsilon}) + [1-\epsilon]^{-1} \frac{4}{|\mathcal{M}|} \sum_{m=1}^{|\mathcal{M}|} \sum_{m' \neq m} \mathrm{Tr}\left\{ \mathbb{E}_{X'^n}\left\{ \Pi^{B^n|X^n}_{\sigma_{X^n(m')},\delta} \right\} \Pi^{B^n}_{\sigma,\delta} \sigma^{\otimes n} \Pi^{B^n}_{\sigma,\delta} \right\}$$

3/17/2011



$$\leq 2(\epsilon + 2\sqrt{\epsilon}) +$$

$$[1-\epsilon]^{-1} \frac{4}{|\mathcal{M}|} \sum_{m=1}^{|\mathcal{M}|} \sum_{m' \neq m} \mathbb{E}_{X'^n} \{ \text{Tr} \{ \Pi^{B^n|X^n}_{\sigma_{X^n(m')},\delta} \cdot \Pi^{B^n}_{\sigma,\delta} \} \} 2^{-n[H(B)-\delta]}$$

Since $\Pi^{B^n}_{\sigma,\delta} \leq I$

$$\Rightarrow \Pi^{B^n|X^n}_{\sigma_{X^n(m')},\delta} \Pi^{B^n}_{\sigma,\delta} \Pi^{B^n|X^n}_{\sigma_{X^n(m')},\delta} \leq \Pi^{B^n|X^n}_{\sigma_{X^n(m')},\delta}$$

$\therefore$

$$\leq 2(\epsilon + 2\sqrt{\epsilon}) +$$

$$[1-\epsilon]^{-1} \frac{4}{|\mathcal{M}|} \sum_{m=1}^{|\mathcal{M}|} \sum_{m' \neq m} \mathbb{E}_{X'^n} \{ \text{Tr} \{ \Pi^{B^n|X^n}_{\sigma_{X^n(m')},\delta} \} \} 2^{-n[H(B)-\delta]}$$

$$\leq 2(\epsilon + 2\sqrt{\epsilon}) +$$

$$[1-\epsilon]^{-1} \frac{4}{|\mathcal{M}|} \sum_{m=1}^{|\mathcal{M}|} \sum_{m' \neq m} 2^{-n[H(B)-\delta]} \, 2^{n[H(B|X)+\delta]}$$

$$\leq 2(\epsilon + 2\sqrt{\epsilon}) +$$

$$[1-\epsilon]^{-1} 4 |\mathcal{M}| \, 2^{-n[I(X;B) - 2\delta]}$$

— Choose $|\mathcal{M}| = 2^{n(I(X;B) - 3\delta)}$ & bound becomes

$$2(\epsilon + 2\sqrt{\epsilon}) + [1-\epsilon]^{-1} 4 \cdot 2^{-n\delta}$$

which becomes arbitrarily small as $n \to \infty$

3/17/2011



- Since we have a good bound on expectation of average error prob., there must exist a particular code w/ its average error prob $\leq \epsilon'$
- By throwing away the worst half of the codewords, we have a code w/ maximal error prob $\leq 2\epsilon'$ w/ an asymptotically negligible loss in rate
- the rate is $\frac{\log_2 |\mathcal{M}|}{n} = I(X;B) - 3\delta$

Thus, the rate $I(X;B)$ is achievable.

we can get $\chi(\mathcal{N})$ by ~~choos~~ making codes from the ensemble that attains the maximum in

$$\chi(\mathcal{N}) = \max_{\rho^{XA}} I(X;B)$$

to achieve $\frac{1}{k}\chi(\mathcal{N}^{\otimes k})$, build codes for the channel $\chi(\mathcal{N}^{\otimes k})$ instead

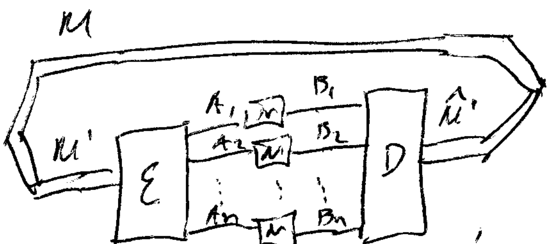
- this shows that $\lim_{k\to\infty} \frac{1}{k}\chi(\mathcal{N}^{\otimes k})$ is achievable

3/17/2011

## Converse Theorem

consider the task of common randomness generation instead.

CR capacity has to be an upper bound on classical comm. capacity b/c a classical bit channel can always generate common randomness.




$$\left\| D^{B^n\to\hat{M}}\left(\mathcal{N}^{\otimes n}\left(\mathcal{E}^{M'\to A^n}\left(\overline{\Phi}^{MM'}\right)\right)\right) - \overline{\Phi}^{M\hat{M}}\right\|_1 \le \epsilon$$

where $\overline{\Phi}^{M\hat{M}} \equiv \frac{1}{|M|}\sum_{m=1}^{|M|} |m\rangle\langle m|^M \otimes |m\rangle\langle m|^{\hat{M}}$

If this holds for a good code, what is limit on rate?

rate of common randomness is

$$\frac{\log|M|}{n} = C$$

3/17/2011

$$nC = \log |M|$$
$$= H(M)_{\Phi} - H(M|\hat{M})_{\Phi}$$
$$= I(M;\hat{M})_{\Phi}$$
$$\leq I(M;\hat{M})_{\omega'} + n\epsilon' \quad \text{Alicki-Fannes'}$$
$$\leq I(M;B^n)_{\omega^*} + n\epsilon' \quad \text{(QDP)}$$

state $\omega$ is a classical quantum state of the form $\sum_m p(m)\,|m\rangle\langle m| \otimes \mathcal{N}(\rho_m)$

must have mutual info less than ~~optimal~~ rate

$$\leq \chi(\mathcal{N}^{\otimes n}) + n\epsilon'$$

$$\therefore \quad C \leq \frac{1}{n}\chi(\mathcal{N}^{\otimes n}) + \epsilon'$$

statement of classical capacity theorem

$$\sup\{C : C \text{ is achievable}\} = \lim_{k\to\infty} \frac{1}{k}\chi(\mathcal{N}^{\otimes k})$$

3/17/2011

In general, cannot compute capacity.

But suppose $\mathcal{N}$ is entanglement breaking so that

$$\mathcal{N}^{A\to B}(\rho^{A'A}) = \sum_y p(y)\, \sigma_y^{A'} \otimes \omega_y^{B}$$

for any entangled state $\rho^{A'A}$.

- Then we can show that $\chi(\mathcal{N})$ is capacity
- would like to prove additivity of $\chi$ in this case:

$$\chi(\mathcal{N}_1 \otimes \mathcal{N}_2) = \chi(\mathcal{N}_1) + \chi(\mathcal{N}_2)$$

$$\chi(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq \chi(\mathcal{N}_1) + \chi(\mathcal{N}_2) \text{ always holds}$$

let's prove $\chi(\mathcal{N}_1 \otimes \mathcal{N}_2) \leq \chi(\mathcal{N}_1) + \chi(\mathcal{N}_2)$

consider arbitrary state

$$\rho^{XA_1A_2} \equiv \sum_x p(x)\, |x\rangle\langle x|^X \otimes (\rho_x^{A_1A_2})$$

Inputting to tensor product channel gives

$$\rho^{XB_1B_2} = (\mathcal{N}_1^{A_1\to B_1} \otimes \mathcal{N}_2^{A_2\to B_2})(\rho^{XA_1A_2})$$

suppose $\mathcal{N}_2$ is entanglement breaking - Then

$$\rho^{XB_1B_2} = \sum_x p(x)\, |x\rangle\langle x|^X \otimes \sum_y p(y|x) \left[\mathcal{N}_1(\sigma_{y,x}) \otimes \omega_{y,x}^{B_2}\right]$$

can augment this state as

$$\rho^{XYB_1B_2} = \sum_{x,y} p(x)p(y|x)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes \mathcal{N}_1(\sigma_{y,x}) \otimes \omega_{y,x}^{B_2}$$

then

$$I(X;B_1B_2) = H(B_1B_2) - H(B_1B_2|X)$$

3/17/2011

$$\leq H(B_1) + H(B_2) - H(B_1 B_2 | X)$$

$$\leq H(B_1) + H(B_2) - H(B_1 B_2 | XY)$$

$$= H(B_1) + H(B_2) - H(B_1 | XY) - H(B_2 | XY)$$

$$= I(XY; B_1) + I(XY; B_2)$$

$$\leq \chi(N_1) + \chi(N_2)$$