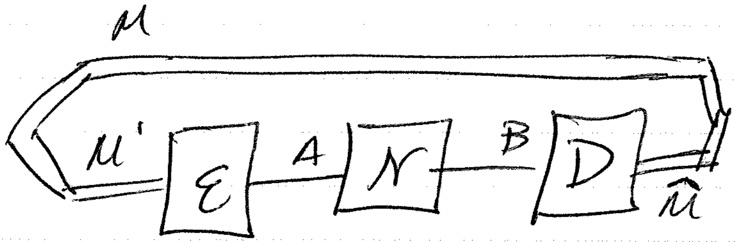
Lecture 27

(1)

- now let's discuss unassisted classical communication.

- we begin w/ the oneshot setting



Initial state is

$$\overline{\Phi}^{p}_{MM'} = \sum_{m \in M} p(m) \, |m\rangle\langle m|_M \otimes |m\rangle\langle m|_{M'}$$

Final state is

$$\omega^{p}_{M\hat{M}} = \left(\mathcal{D}_{B \to \hat{M}} \circ \mathcal{N}_{A \to B} \circ \mathcal{E}_{M' \to A}\right)\left(\overline{\Phi}^{p}_{MM'}\right)$$

Since encoding channel acts on classical register M', we can define

$$\mathcal{E}_{M' \to A}\left(|m\rangle\langle m|_{M'}\right) = \rho^{m}_{A}$$

Also, decoder $\mathcal{D}_{B\to\hat{\mathcal{M}}}$ is a measurement channel & so can be written as

$$\mathcal{D}_{B\to\hat{\mathcal{M}}}(\tau_B) = \sum_{\hat{m}\in\mathcal{M}} \mathrm{Tr}[\Lambda_B^{\hat{m}} \tau_B] |\hat{m}\rangle\langle\hat{m}|_{\hat{\mathcal{M}}}$$

$\Rightarrow$

$$\omega^p_{\mathcal{M}\hat{\mathcal{M}}} = \sum_{m,\hat{m}\in\mathcal{M}} p(m) |m\rangle\langle m|_{\mathcal{M}} \otimes q(\hat{m}|m) |\hat{m}\rangle\langle\hat{m}|_{\hat{\mathcal{M}}}$$

where

$$q(\hat{m}|m) = \mathrm{Tr}[\Lambda_B^{\hat{m}} \mathcal{N}_{A\to B}(\rho_A^m)]$$

Similar definitions as before:

$$p_{err}(m) = 1 - q(m|m)$$

$$p^*_{err} = \max_{m\in\mathcal{M}} p_{err}(m)$$

An $(|M|, \varepsilon)$ classical comm. protocol sends $|M|$ messages such that $p^*_{err} \leq \varepsilon$.

One-shot classical capacity:

$$C^{\varepsilon}(N) = \sup_{(M, \xi, D)} \{ \log_2 |M| : p^*_{err} \leq \varepsilon \}$$

goal is to establish an upper bound and a lower bound.

Let's start w/ upper bound

$$C^{\varepsilon}(N) \leq \chi_H^{\varepsilon}(N)$$

hypothesis testing Holevo information

$$\chi_H^{\varepsilon}(N) = \sup_{\{p(x), \rho_A^x\}} I_H^{\varepsilon}(X;B)_{\tau} \quad \tau_{XB} = \sum_x p(x) |x\rangle\langle x|_X \otimes [N(\rho^x)]_B$$

Consider that $p_{err}^* \leq \varepsilon$

$\Rightarrow \quad p_{avg} = \frac{1}{|M|}\sum_m p_{err}(m) \leq \varepsilon$ 4

By the same reasoning used for EA classical comm. upper bound, we conclude that

$$\log_2 |M| \leq I_H^\varepsilon(M;\hat{M})_\omega$$

where $\omega_{M\hat{M}} = \omega^p_{M\hat{M}}$ w/ $\underline{p}$ uniform

From data processing under decoding channel

$$\Rightarrow I_H^\varepsilon(M;\hat{M})_\omega \leq I_H^\varepsilon(M;B)_\theta$$

where

$$\theta_{MB} = \frac{1}{|M|}\sum_m |m\rangle\langle m|_M \otimes N_{A\to B}(\rho_A^m)$$

Now take sup over input ~~ens~~ ensembles to get $I_H^\varepsilon(M;B)_\theta \leq \chi_H^\varepsilon(N)$

$$\Rightarrow \log_2 |\mathcal{M}| \leq \chi_H^\varepsilon(\mathcal{N})$$

Since this is an upper bound for every $(|\mathcal{M}|, \varepsilon)$ protocol, we conclude that

$$C^\varepsilon(\mathcal{N}) \leq \chi_H^\varepsilon(\mathcal{N})$$

Note that

$$\chi_H^\varepsilon(\mathcal{N}) = \sup_{\rho_{MA}} \inf_{\sigma_B} D_H^\varepsilon(\mathcal{N}_{A\to B}(\rho_{MA}) \| \mathcal{R}^\sigma_{A\to B}(\rho_{MA}))$$

replacer channel

this upper bound involves a comparison in HTRE of cq state generated by the actual channel & the most useless one.

By similar techniques as before, we get the bounds

$$C^{\varepsilon}(\mathcal{N}) \leq \frac{1}{1-\varepsilon}\left(\chi(\mathcal{N}) + h_2(\varepsilon)\right)$$

$$C^{\varepsilon}(\mathcal{N}) \leq \tilde{\chi}_{\alpha}(\mathcal{N}) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right)$$

$$\forall \alpha > 1$$

Asymptotic capacity defined as

$$C(\mathcal{N}) = \inf_{\varepsilon\in(0,1)} \liminf_{n\to\infty} \frac{1}{n} C^{\varepsilon}(\mathcal{N}^{\otimes n})$$

Strong converse capacity

$$\tilde{C}(\mathcal{N}) = \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} \frac{1}{n} C^{\varepsilon}(\mathcal{N}^{\otimes n})$$

- A channel is entanglement-breaking (EB) if $\mathcal{N}_{A\to B}(\rho_{RA})$ is separable for every bipartite input ρ_{RA}.

- Can show that $\mathcal{N}_{A\to B}$ is EB iff Choi op $\Gamma^{\mathcal{N}}_{RB}$ is a separable operator.

- Can also show the following additivity relations:

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

Also

$$\tilde{\chi}_\alpha(\mathcal{N}\otimes\mathcal{M}) = \tilde{\chi}_\alpha(\mathcal{N}) + \tilde{\chi}_\alpha(\mathcal{M})$$

$\forall \alpha > 1$

where $\mathcal{N}$ is EB + $\mathcal{M}$ is arbitrary can now use def's + upper bounds to get

$$\frac{C^{\varepsilon}(N^{\otimes n})}{n} \leq \frac{1}{1-\varepsilon}\left[\frac{\chi(N^{\otimes n})}{n} + \frac{h_2(\varepsilon)}{n}\right]$$

define $\chi^{reg}(N) = \lim_{n\to\infty} \frac{1}{n}\chi(N^{\otimes n})$

take lim $n\to\infty$

$$\liminf_{n\to\infty} \quad \leq \frac{1}{1-\varepsilon}\chi^{reg}(N)$$

now $\varepsilon \to 0$ to get

$$C(N) \leq \chi^{reg}(N)$$

for EB channels

$$\chi^{reg}(N) = \chi(N)$$

for strong converse for EB channels:

$$\frac{C^{\varepsilon}(\mathcal{N}^{\otimes n})}{n} \leq \frac{1}{n}\tilde{\chi}_{\alpha}(\mathcal{N}^{\otimes n}) + \frac{\alpha}{n(\alpha-1)}\log\left(\frac{1}{1-\varepsilon}\right)$$

$$\text{'} \quad = \tilde{\chi}_{\alpha}(\mathcal{N}) + \text{''}$$

take $n \to \infty$ limit

$$\Rightarrow \quad \liminf_{n\to\infty} \frac{C^{\varepsilon}(\mathcal{N}^{\otimes n})}{n} \leq \tilde{\chi}_{\alpha}(\mathcal{N})$$

$\forall \alpha > 1$

take $\alpha \to 1$ limit

$$\Rightarrow \quad \text{''} \leq \chi(\mathcal{N})$$

$$\Rightarrow \quad \tilde{C}(\mathcal{N}) \leq \chi(\mathcal{N})$$

Lower bound

$$C^{\varepsilon}(\mathcal{N}) \geq \bar{\chi}_H^{\varepsilon/2-\eta}(\mathcal{N}) - \log_2\left(\frac{4\varepsilon}{\eta^2}\right)$$

for $\varepsilon \in (0,1)$ & $\eta \in (0, \varepsilon/2)$

where

$$\bar{\chi}_H^{\delta}(\mathcal{N}) = \sup_{\rho_{XA}} D_H^{\varepsilon}(\omega_{XB} \| \omega_X \otimes \omega_B)$$

where $\omega_{XB} = \mathcal{N}_{A \to B}(\rho_{XA})$

basic idea is to use position-based coding again

Idea is to allow Alice + Bob access to shared randomness before comm. begins:

$$\rho_{XB'} = \sum_x r(x)\, |x\rangle\langle x|_X \otimes |x\rangle\langle x|_{B'}$$

where r is a prob. dist.

Then they share the state

$\rho_{XB'}^{\otimes |M|}$

If Alice wants to send message m, she transmits the mth X system through a cq channel $x \to \rho_A^x$ + then system A through channel $N_{A\to B}$

reduced state for Bob is then

$$\tau^m = \rho_{B_1'} \otimes \cdots \otimes \rho_{B_{m-1}'} \otimes \mathcal{N}_{A\to B}(\rho_{AB_m'}) \otimes \rho_{B_{m+1}'} \otimes \cdots \otimes \rho_{B_{|M'|}'}$$

where $\rho_{B_i'} = \sum_x r(x) |x\rangle\langle x|$

& $\rho_{AB_m'} = \sum_x p(x) |x\rangle\langle x|_{B_m'} \otimes \rho_A^x$

we are then in the same setting as before, w/ position-based coding

$\Rightarrow \exists$ scheme such that

$p_{err}(m) \leq \varepsilon \quad \forall m \in M'$

w/

$$\log|M'| = I_H^{\varepsilon-\eta}(B';B)_\xi - \log_2\left(\frac{4\varepsilon}{\eta^2}\right)$$

where $\xi_{B'B} = \mathcal{N}_{A\to B}(\rho_{AB'})$

We now would like to remove the shared randomness.

First consider that

$$\overline{p_{err}} = \frac{1}{|\mathcal{M}'|} \sum_{m \in \mathcal{M}'} p_{err}(m) \leq \varepsilon$$

Observe that $\mathcal{N}_{A \to B}(\rho_{A'B'})$ & $\rho_{B'} \otimes \mathcal{N}_{A \to B}(\rho_{A'})$ are cq states

$\Rightarrow$

$$\mathrm{Tr}[\Lambda_{BB'} \mathcal{N}_{A \to B}(\rho_{A'B'})]$$

$$= \sum_x r(x) \, \mathrm{Tr}[\Lambda_{B'B} (|x\rangle\langle x|_{B'} \otimes \rho^x_B)]$$

$$= \sum_x r(x) \, \mathrm{Tr}[M^x_B \rho^x_B]$$

where $M^x_B = \langle x|_{B'} \Lambda_{B'B} |x\rangle_{B'}$

& setting $\bar{\rho}_B = \sum_x p(x) \rho_B^x$

$$\Rightarrow \mathrm{Tr}\left[\Lambda_{B'B}\left(\rho_{B'} \otimes \mathcal{N}_{A\to B}(\rho_{A'})\right)\right]$$

$$= \sum_x r(x) \,\mathrm{Tr}\left[\Lambda_{B'B}\left(|x\rangle\langle x|_{B'} \otimes \bar{\rho}_B\right)\right]$$

$$= \sum_x r(x) \,\mathrm{Tr}\left[M^x \bar{\rho}_B\right]$$

$\Rightarrow$ optimal meas. op. for

$$D_H^{\varepsilon-n}\left(\mathcal{N}_{A\to B}(\rho_{A'B'}) \,\|\, \rho_{B'} \otimes \mathcal{N}_{A\to B}(\rho_{A'})\right)$$

has the form

$$\Lambda^*_{B'B} = \sum_x |x\rangle\langle x|_{B'} \otimes M_B^x$$

Recall we implemented measurements in position-based coding as projectors

$\Pi_{B'BR}$.

these now have the form

$$\Pi_{B'BR} = \sum_x |x\rangle\langle x|_{B'} \otimes \Pi^x_{BR}$$

where $\Pi^x_{BR} = (U^x_{BR})^\dagger (I_B \otimes |1\rangle\langle 1|_R) U^x_{BR}$

& $U^x_{BR} = \sqrt{I - M^x_B} \otimes I_R$

$\qquad + \sqrt{M^x_B} \otimes (|1\rangle\langle 0|_R - |0\rangle\langle 1|_R)$

$\Rightarrow$ measurement op's have the form

$$P_i = \sum_{x_1, \ldots, x_{m-1}} |\underline{x}\rangle\langle \underline{x}|_{B'_1 \cdots B'_{m-1}} \otimes P_i^{x_i}$$

where $P_i^{x_i} = \Pi^{x_i}_{BR_i}$

can write state τ^m as

$$\tau^m_{B'_1 \cdots B'_{m-1} B} = \sum_{x_1, \ldots, x_{m-1}} r(x_1) \cdots r(x_{m-1}) \, |\underline{x}\rangle\langle \underline{x}| \otimes \rho_B^{x_m}$$

& can write error prob. as

$$P_{err}(m) =$$

$$1 - \text{Tr}\left[P_m \hat{P}_{m-1} \cdots \hat{P}_1 \,\omega^m \hat{P}_1 \cdots \hat{P}_{m-1} P_m\right]$$

$$= \sum_{x_1, \ldots, x_{|\mathcal{M}'|}} r(x_1) \cdots r(x_{|\mathcal{M}'|}) \times$$

$$\left[1 - \text{Tr}\left[\Lambda_m^{x_m}\left(\rho_B^{x_m} \otimes |\underline{0}\rangle\langle\underline{0}|_{P_1^{|\mathcal{M}'|}}\right)\right]\right]$$

where

$$\Lambda_m^{x_m} = \hat{P}_1^{x_1} \cdots \hat{P}_{m-1}^{x_{m-1}} P_m^{x_m} \hat{P}_{m-1}^{x_{m-1}} \cdots \hat{P}_1^{x_1}$$

Basic idea from here

write avg. error prob. as

$$\frac{1}{|\mathcal{M}'|} \sum_m P_{err}(m)$$

$$= \sum_{x_1, \ldots, x_{|\mathcal{M}'|}} r(x_1) \cdots r(x_{|\mathcal{M}'|}) \times$$

$$\frac{1}{|\mathcal{M}'|} \sum_m \left[1 - \text{Tr}\left[\Lambda_m^{x_m}\left(\rho_B^{x_m} \otimes |\underline{0}\rangle\langle\underline{0}|\right)\right]\right]$$

$$\leq \varepsilon$$

where we switched sums

"Shannon trick"

Since expected error $\leq \varepsilon$

$\Rightarrow$ existence of symbols (codewords)

$x_1, \ldots, x_{|\mathcal{M}'|}$ such that

$$\frac{1}{|\mathcal{M}'|} \sum_m \left\{1 - \mathrm{Tr}\left[\Lambda_m^{x_m} \left(\rho_B^{x_m} \otimes |\underline{0}\rangle\langle\underline{0}|\right)\right]\right\} \leq \varepsilon$$

Now throw away worst half of codewords to get $\mathcal{M}$ such that

$$|\mathcal{M}| = \frac{|\mathcal{M}'|}{2}$$

$$1 - \mathrm{Tr}\left\{\Lambda_m^{x_m} \left(\rho_B^{x_m} \otimes |\underline{0}\rangle\langle\underline{0}|\right)\right\} \leq 2\varepsilon$$

$$\forall m \in \mathcal{M}$$

this is the code to use & # of bits transmitted is as stated before.