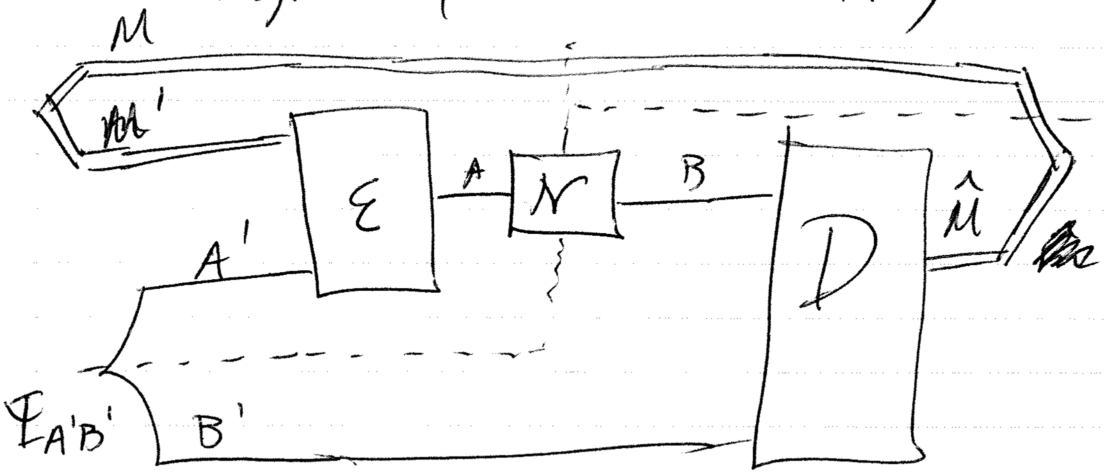
Lecture 25

Entanglement-assisted communication

Begin w/ one-shot setting



Initial state is

$$\overline{\Phi}^{p}_{MM'} \otimes \Psi_{A'B'}$$

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

Then encoding and decoding lead to final state

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

Note that decoder is a measurement channel

$$\mathcal{D}_{BB'\to\hat{M}}(\tau_{BB'}) = \sum_{\hat{m}\in\mathcal{M}} \mathrm{Tr}[\Lambda^{\hat{m}}_{BB'}\tau_{BB'}] \times |\hat{m}\rangle\langle\hat{m}|_{\hat{M}}$$

we can also define

$$\mathcal{E}^{m}_{A'\to A}(\cdot) = \mathcal{E}_{M'A'}(|m\rangle\langle m|_{M'} \otimes (\cdot))$$

& write the final state as

$$\omega^{p}_{M\hat{M}} = \sum_{m,\hat{m}\in\mathcal{M}} p(m)\,|m\rangle\langle m|_{M} \otimes \underbrace{\mathrm{Tr}[\Lambda^{\hat{m}}_{BB'}\,\mathcal{N}_{A\to B}(\mathcal{E}^{m}_{A'\to A}(\Phi_{A'B'}))]}\,|\hat{m}\rangle\langle\hat{m}|_{\hat{M}}.$$

Defining

$q(\hat{m}|m) =$

error prob. when sending message m is then

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

(prob. that decoded message does not equal transmitted one)

maximal error prob. of a code is then

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

A code is an $(|\mathcal{M}|, \varepsilon)$ code if $|\mathcal{M}|$ is # messages & $p^*_{err} \leq \varepsilon$.

- can prove that $p^*_{err} =$

$$\max_{p : \mathcal{M} \to [0,1]} \frac{1}{2} \left\| \Phi^p_{MM'} - \omega^p_{M\hat{M}} \right\|_1$$

one-shot EA capacity:

$$C^{\varepsilon}_{EA}(\mathcal{N}) = \sup_{(\mathcal{M},\Psi,\mathcal{E},\mathcal{D})} \left\{ \log_2 |\mathcal{M}| : p^*_{err}((\Psi,\mathcal{E},\mathcal{D});\mathcal{N}) \leq \varepsilon \right\}$$

---

our 1st goal is to establish an upper bound on $C^{\varepsilon}_{EA}(\mathcal{N})$

- Main idea is to substitute the actual channel $\mathcal{N}_{A\to B}$ w/ a useless channel $\mathcal{R}^{\sigma}_{A\to B}(\cdot) = \mathrm{Tr}[(\cdot)]\sigma_B$ & then compare these different protocols using hypothesis testing relative entropy.

We begin w/ a lemma

Let $\Phi_{MM'} = \frac{1}{|M|} \sum_{m \in M} |m\rangle\langle m|_M \otimes |m\rangle\langle m|_{M'}$

Define the comparator test

$\{\Pi_{MM'}, I_{MM'} - \Pi_{MM'}\}$

where

$\Pi_{MM'} = \sum_{m \in M} |m\rangle\langle m|_M \otimes |m\rangle\langle m|_{M'}$

Suppose that $\omega_{MM'}$ is a state ~~#~~ such that $\omega_M = \frac{I_M}{|M|} = \pi_M$

& $\mathrm{Tr}[\Pi_{MM'} \omega_{MM'}] \geq 1 - \varepsilon$.

Then

$\log_2 |M| \leq I_H^\varepsilon (M; M')_\omega$

where I_H^ε is the hypothesis testing mutual information, defined for ρ_{AB} as

$$I_H^{\varepsilon}(A;B)_\rho = \min_{\sigma_B} D_H^{\varepsilon}(\rho_{AB} \| \rho_A \otimes \sigma_B)$$

Proof: By assumption,

$$\mathrm{Tr}[\Pi_{MM'}\, \omega_{MM'}] \geq 1-\varepsilon$$

Now consider

$$\tau_{MM'} = \omega_M \otimes \sigma_{M'} = \pi_M \otimes \sigma_{M'}$$

Then

$$\mathrm{Tr}[\Pi_{MM'}\, \tau_{MM'}]$$

$$= \mathrm{Tr}[\Pi_{MM'}(\pi_M \otimes \sigma_{M'})]$$

$$= \frac{1}{|M|} \mathrm{Tr}[\Pi_{MM'}(I_M \otimes \sigma_{M'})]$$

$$= \frac{1}{|M|} \mathrm{Tr}[\mathrm{Tr}_M[\Pi_{MM'}]\, \sigma_{M'}]$$

$$= \frac{1}{|M|} \mathrm{Tr}[I_{M'}\sigma_{M'}] = \frac{1}{|M|}$$

By using the definition of hypothesis testing relative entropy,

$$\log_2 |\mathcal{M}| = -\log_2 \mathrm{Tr}[\Pi_{MM'} \tau_{MM'}]$$
$$\leq D_H^{\varepsilon}(\omega_{MM'} \| \tau_{MM'})$$
$$= D_H^{\varepsilon}(\omega_{MM'} \| \omega_M \otimes \sigma_{M'})$$

inequality holds for arbitrary $\sigma_{M'}$

$\Rightarrow$ take infimum over $\sigma_{M'}$ & apply definition of HTMI to arrive @ claim.

Assumption for an $(|\mathcal{M}|, \varepsilon)$ protocol:

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

$$\Rightarrow 1 - \frac{1}{|\mathcal{M}|} \sum_m q(m|m) \leq \varepsilon$$

i.e., average error probability

can show that this implies that

$$\mathrm{Tr}[\Pi_{M\hat{M}}\, \omega_{M\hat{M}}] \geq 1-\varepsilon$$

final state of protocol.

& by the lemma

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

establishes a close link between communication & hypothesis testing.

Now data processing under decoding channel to get

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

$$\leq I_H^{\varepsilon}(M;BB')_{\theta}$$

where $\theta_{MBB'} = (\mathcal{N}_{A\to B} \circ \mathcal{E}_{M'A\to A})$
$(\Phi_{MM'} \otimes \Phi_{A'B'})$

Consider that

$$\theta_{MB'} = \mathrm{Tr}_B\left[(\mathcal{N}_{A\to B} \circ \mathcal{E}_{M'A'\to A})(\overline{\Phi}_{MM'} \otimes \Psi_{A'B'})\right]$$

$$= \mathrm{Tr}_{M'A'}\left[\overline{\Phi}_{MM'} \otimes \Psi_{A'B'}\right]$$

$$= \overline{\Phi}_M \otimes \Psi_{B'}$$

$$= \theta_M \otimes \theta_{B'}$$

$$\Rightarrow \quad I_H^\varepsilon(M;BB')_\theta$$

$$= \inf_{\sigma_{BB'}} D_H^\varepsilon(\theta_{MBB'} \| \theta_M \otimes \sigma_{BB'})$$

$$\leq \inf_{\sigma_B} D_H^\varepsilon(\theta_{MBB'} \| \theta_M \otimes \sigma_B \otimes \theta_{B'})$$

$$= \text{''} \quad D_H^\varepsilon(\theta_{MBB'} \| \theta_{MB'} \otimes \sigma_B)$$

$$= I_H^\varepsilon(MB';B)_\theta$$

$$\leq \sup_{\rho_{SA}} I_H^\varepsilon(S;B)_\xi$$

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

suffices to optimize over pure states ψ_{SA} w/ $S \simeq A$

$$\Rightarrow \log_2 |\mathcal{M}| \leq I_H^{\varepsilon}(\mathcal{N}) := \sup_{\psi_{SA}} I_H^{\varepsilon}(S;B)_{\rho}$$

where $\rho_{SB} = \mathcal{N}_{A\to B}(\psi_{SA})$

$\Rightarrow$ final bound on one-shot EA capacity

$$C_{EA}^{\varepsilon}(\mathcal{N}) \leq I_H^{\varepsilon}(\mathcal{N})$$

one-shot mutual information of channel.

By applying $D_H^{\varepsilon}(\rho\|\sigma) \leq D_{\alpha}(\rho\|\sigma) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right)$

$\Rightarrow$

$$C_{EA}^{\varepsilon}(\mathcal{N}) \leq \widetilde{I}_{\alpha}(\mathcal{N}) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right)$$

By using

$$D_H^{\varepsilon}(\rho\|\sigma) \leq \frac{1}{1-\varepsilon}\Big(D(\rho\|\sigma) + h_2(\varepsilon) + \varepsilon \log_2 \mathrm{Tr}[\sigma]\Big)$$

we also get

$$C_{EA}^{\varepsilon}(\mathcal{N}) \leq \frac{1}{1-\varepsilon}\Big(I(\mathcal{N}) + h_2(\varepsilon)\Big)$$

where $I(\mathcal{N}) = \sup_{\psi_{RA}} I(R;B)_{\omega}$

w/ $\omega_{RB} = \mathcal{N}_{A\to B}(\psi_{RA})$

Asymptotic capacity is defined as

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

& strong converse capacity as

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

$C_{EA}(\mathcal{N}) \leq \tilde{C}_{EA}(\mathcal{N})$ always holds

Let us 1st bound

$C_{EA}(\mathcal{N})$ from above by $I(\mathcal{N})$

using the weak-converse bound we have that

$$\frac{1}{n} C_{EA}^{\varepsilon}(\mathcal{N}^{\otimes n}) \leq \frac{1}{1-\varepsilon}\left(\frac{I(\mathcal{N}^{\otimes n})}{n} + \frac{h_2(\varepsilon)}{n}\right)$$

Let us prove that $\frac{I(\mathcal{N}^{\otimes n})}{n} = I(\mathcal{N})$

Follows from

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

+ induction

We always have $I(\mathcal{N}\otimes\mathcal{M}) \geq I(\mathcal{N}) + I(\mathcal{M})$

Now for opposite inequality

$$I(\mathcal{N}\otimes\mathcal{M}) = \sup_{\psi_{RA_1A_2}} I(R;B_1B_2)_\omega$$

$$\omega_{RB_1B_2} = (\mathcal{N}_{A_1\to B_1} \otimes \mathcal{M}_{A_2\to B_2})(\psi_{RA_1A_2})$$

Consider that

$$I(R;B_1B_2)_\omega =$$

$$I(R;B_1)_\omega + I(R;B_2|B_1)_\omega$$

$$\leq I(R;B_1)_\omega + I(RB_1;B_2)_\omega$$

$$\leq I(\mathcal{N}) + I(\mathcal{M})$$

Finishing off we get

$$\frac{1}{n} C_{EA}^{\varepsilon}(\mathcal{N}^{\otimes n}) \leq \frac{1}{1-\varepsilon}\left(I(\mathcal{N}) + \frac{h_2(\varepsilon)}{n}\right)$$

then ~~lim~~ $n\to\infty$ & $\varepsilon \to 0$ gives upper bound can also get the strong converse by using previous upper bound + the fact that

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

$$\forall\, \alpha > 1$$