# Lecture 1



<u>Plan:</u> I. Fundamentals

II. Classical Comm. over Q. Channels

III. Quantum Comm. over Q. Channels

IV. Approximate Quantum Markov Chains + Conditional Mutual Information

---

Density operators describe quantum states

$\rho$ is a density operator acting on Hilbert space

if $\rho \geq 0$ + $\mathrm{Tr}\{\rho\} = 1$

all eigenvalues are non-negative

probability normalization condition

generalizes notion of probability distribution

arises from two perspectives:

1) if we have imperfect knowledge of a pure state, i.e., ensemble
$\{p(x), |\psi_x\rangle\} \Rightarrow \rho = \sum_x p(x) |\psi_x\rangle\langle\psi_x|$

2) as reduction of a pure state on a larger system

so from lack of information
or lack of access
in standard linear quantum mechanics, can
treat these the same way

"proper" + "improper" mixtures

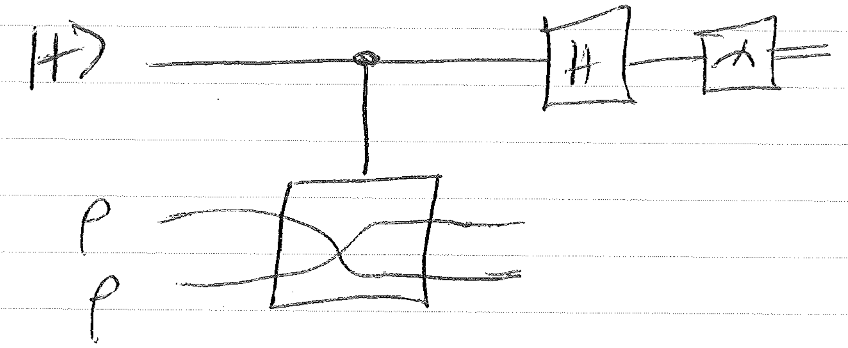
---

quantum states acting on a
tensor-product Hilbert space $H_A \otimes H_B$
are "bipartite." Think of Alice
possessing one system + Bob
another. They are "distinguishable
particles" or have distinguishable
degrees of freedom.

quantum state is ~~[illegible]~~ pure
if density operator is rank one
i.e., $\rho = |\psi\rangle\langle\psi|$ for some
unit vector $|\psi\rangle$

can test this by computing purity
$\mathrm{Tr}\{\rho^2\}$ if $=1$ then pure
+ $<1 \Rightarrow$ mixed

Exercise: Show how the following quantum circuit can be used to estimate purity




$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$|0\rangle\langle 0| \otimes I \otimes I \; + \; |1\rangle\langle 1| \otimes \text{SWAP}$$

$$H = |0\rangle\langle +| + |1\rangle\langle -|$$

Take an axiomatic approach to quantum evolutions. A quantum channel has a quantum input & quantum output.

Examples: ① unitary evolution (closed system $U = e^{-iHt}$

$$\rho \to U \rho U^{+} \quad \text{for some unitary } U$$

Notice: input is quantum state ⇒ output is quantum state

2) Interaction w/ bath

$$U_{SB} = e^{-iH_{SB}t}$$

where $H_{SB} = H_S \otimes I_B + I_S \otimes H_B + H_{SB}^{int}$

$$\rho_S \rightarrow \rho_S \otimes \tau_B$$

$$\rightarrow U_{SB}(\rho_S \otimes \tau_B) U_{SB}^{\dagger}$$

$$\rightarrow \mathrm{Tr}_B\{U_{SB}(\rho_S \otimes \tau_B) U_{SB}^{\dagger}\}$$

---

What are the axioms?

I. Channel $\mathcal{N}$ should be <u>convex linear</u>

$$\mathcal{N}(p\rho + (1-p)\sigma) = p\mathcal{N}(\rho) + (1-p)\mathcal{N}(\sigma)$$

Why? one could have experiments where $\rho$ & $\sigma$ chosen randomly according to $(p, 1-p)$.

Without telling another, who measures their experimental data would be described by $\mathcal{N}(p\rho + (1-p)\sigma)$.

Later this info. could be revealed, in which case the data would be given by $p\mathcal{N}(\rho) + (1-p)\mathcal{N}(\sigma)$

These two should be consistent!

extend this to full linearity

<u>other arguments</u>: Nonlinear evolutions would allow for signaling, or solving computational problems believed to be intractable.

II. <u>Trace preserving</u>:

$$\mathrm{Tr}\{X\} = \mathrm{Tr}\{\mathcal{N}(X)\}$$

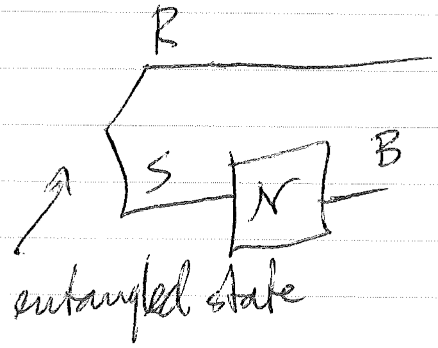
corresponds to probability conservation (quantum in to quantum out)

III. <u>Complete positivity</u>:

A map $\mathcal{N}$ is positive if

$\mathcal{N}(X) \geq 0$ ~~when~~ for all $X \geq 0$.

Not enough: demand that channel takes entangled input states to legitimate output states, i.e.




so demand that

$$(\mathrm{id}_R \otimes \mathcal{N}_S)(X_{RS}) \geq 0 \quad \forall X_{RS} \geq 0$$

$+$ $R$ of arbitrary size

can check complete positivity by checking whether

$$\left(\mathrm{id}_R \otimes \mathcal{N}_S\right)\left(\Phi_{RS}\right) \geq 0 \text{ where}$$

$$\Phi_{RS} = \frac{1}{d} \sum_{ij} |i\rangle\langle j|_R \otimes |i\rangle\langle j|_S$$

i.e. just check for $R$ same size as $S$.

These three sensible conditions imply the Choi-Kraus theorem:

Every linear CPTP map $\mathcal{N}$ (quantum channel) can be written as

$$\mathcal{N}(\rho) = \sum_x A_x \rho A_x^\dagger \quad \text{such that}$$

$$\sum_x A_x^\dagger A_x = I$$

linearity implies $\mathcal{N}(\rho) = \sum_x A_x \rho B_x^\dagger$ for any choice of $\{A_x, B_x\}$

CP implies $B_x = A_x \ \forall x$

TP implies $\sum_x A_x^\dagger A_x = I$

won't prove this theorem but the main idea is to work w/ Choi matrix

<u>Special example:</u> Measurement channel

Choose Kraus operators to be

$$\{ |x\rangle\langle i| A_x \}$$ where $\{|x\rangle\}$, $\{|i\rangle\}$ O.N. &

Then $$\sum_x A_x^\dagger A_x = I$$

$$\mathcal{M}(\rho) = \sum_{x,i} |x\rangle\langle i| A_x \, \rho A_x^\dagger |i\rangle\langle x|$$

$$= \sum_x \operatorname{Tr}\{A_x \rho A_x^\dagger\} |x\rangle\langle x|$$

$$= \sum_x \operatorname{Tr}\{\underbrace{A_x^\dagger A_x}_{\Lambda_x} \rho\} |x\rangle\langle x|$$

set $\{\Lambda_x\}$ is called POVM

for positive operator valued measure,

b/c $\Lambda_x \geq 0 \ \forall x$ & $\sum_x \Lambda_x = I$

Every measurement can be understood as a quantum to classical channel.

Every state & channel can be purified, meaning that we can find a pure state on a larger system or a unitary channel that simulates the originals after partial trace.

For state $\rho_S = \sum_x p(x) |x\rangle\langle x|$, purification is

$|\psi\rangle_{RS} = \sum_x \sqrt{p(x)}\, |x\rangle_R |x\rangle_S$ & can check that $\mathrm{Tr}_R\{|\psi\rangle\langle\psi|_{RS}\} = \rho_S$

purifications are not unique. Notice that we can place any isometry $U$ (i.e., $U^\dagger U = I$) acting on reference system $R$:

$$\mathrm{Tr}_R\{U_R |\psi\rangle\langle\psi|_{RS} U_R^\dagger\} =$$

$$\mathrm{Tr}_R\{U_R^\dagger U_R |\psi\rangle\langle\psi|_{RS}\}$$

$$= \mathrm{Tr}\{I_R |\psi\rangle\langle\psi|_{RS}\} = \rho_S$$

How to purify a quantum channel?

Given a set of Kraus operators $\{A_k\}$ form the following linear map:

$$U_{S\to BE} \equiv \sum_k A_k \otimes |k\rangle_E$$ where $\{|k\rangle\}$ is O.N. basis

takes $|\psi\rangle \longrightarrow \sum_k A_k |\psi\rangle \otimes |k\rangle_E$

this is an isometry b/c (length preserving)

$U^\dagger U = I_S$

Consider that $U^\dagger U = \left(\sum_j A_j^\dagger \otimes \langle j|_E\right)\left(\sum_k A_k \otimes |k\rangle_E\right)$

$$= \sum_{j,k} A_j^\dagger A_k \otimes \langle j|k\rangle$$

$$= \sum_k A_k^\dagger A_k = I_S$$

this is an isometric extension of a quantum channel in the sense that

$$\mathcal{N}(\rho) = \mathrm{Tr}_E \left\{ U_{S\to BE}\, \rho_S\, U_{S\to BE}^\dagger \right\}$$

Why true? $\rho \rightarrow U_{S\to BE}\, \rho_S\, U^\dagger_{S\to BE}$

$$= \sum_{k,j} A_k \rho A_j^\dagger \otimes |k\rangle\langle j|_E$$

Now trace over environment:

$$Tr_E\{\cdot\} = \sum_{k,j} A_k \rho A_j^\dagger \langle j|k\rangle_E$$

$$= \sum_k A_k \rho A_k^\dagger = \mathcal{N}(\rho)$$

Any isometric ~~ext~~ extension has freedom for choice of environment. I.e., let $V_{E\to E'}$ be an isometry, so that $V^\dagger_{E\to E'} V_{E\to E'}$

Consider that

$$Tr_{E'}\{V_{E\to E'} U_{S\to BE}\, \rho_S\, U^\dagger_{S\to BE} V^\dagger_{E\to E'}\}$$

$$= Tr_E\{V^\dagger V\; U_{S\to BE}\, \rho_S\, U^\dagger_{S\to BE}\}$$

$$= Tr_E\{U_{S\to BE}\, \rho_S\, U^\dagger_{S\to BE}\} = \mathcal{N}(\rho)$$

Any isometry can be realized by tensoring in an ancilla of sufficient size & applying a unitary, i.e., suppose unitary is $\sum_k A_k \otimes |k\rangle\langle 0|_E$ & other entries are filled in to make a unitary

Then $\rho_S \to \rho_S \otimes |0\rangle\langle 0|_E$

$$\to U(\rho_S \otimes |0\rangle\langle 0|_E)U^\dagger$$

$$= \left(\sum_k A_k \otimes |k\rangle\langle 0|_E\right)\left(\rho_S \otimes |0\rangle\langle 0|_E\right)\left(\sum_{k'} A_{k'}^\dagger \otimes |0\rangle\langle k'|_E\right)$$

$$= \sum_{k,k'} A_k \rho A_{k'}^\dagger \otimes |k\rangle\langle k'|_E$$

---

Classical-quantum states

- In a bipartite system, one might be classical & the other quantum

Such a state is called classical-quantum and is in one-to-one correspondence w/ an ensemble. It has the following form:

$\sum_x p(x) \, |x\rangle\langle x|_X \otimes \rho_B^x$ where

$p(x)$ is a prob. dist., $\{|x\rangle\}$ is an O.N. basis, & $\{\rho_B^x\}$ is a set of quantum states.

could be the result of applying a measurement channel to one share of a bipartite state.

Given $\rho_{AB}$ & measurement channel

$$\mathcal{M}_{A\to X}(\cdot) = \sum_x \mathrm{Tr}\{\Lambda^x(\cdot)\} |x\rangle\langle x|_X ,$$

consider that

$$\mathcal{M}_{A\to X}(\rho_{AB}) = \sum_x \mathrm{Tr}_A\{\Lambda^x_A \rho_{AB}\} |x\rangle\langle x|_X$$

$$= \sum_x p(x) |x\rangle\langle x|_X \otimes \rho^x_B$$

$$p(x) = \mathrm{Tr}\{\Lambda^x_A \rho_{AB}\}$$

$$\rho^x_B = \frac{\mathrm{Tr}_A\{\Lambda^x_A \rho_{AB}\}}{p(x)}$$

This is the state of an apparatus & the B system after the measurement has occurred.

## Quantifying uncertainty

An important measure is the quantum relative entropy, "mother of all entropies"

Given a quantum state $\rho$ & a positive semidefinite operator $\sigma$ (which could be a quantum state)

$$D(\rho\|\sigma) = \begin{cases} \mathrm{Tr}\{\rho[\log\rho - \log\sigma]\} & \text{if } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \\ \infty & \text{else} \end{cases}$$

$\mathrm{supp}(\rho)$ is the subspace ~~where~~ spanned by eigenvectors of $\rho$ w/ non-zero eigenvalues (same for $\sigma$)

This definition is consistent w/ the following limit

$$\lim_{\varepsilon \searrow 0} D(\rho\|\sigma + \varepsilon I)$$

i.e., for all $\varepsilon > 0$ $\sigma + \varepsilon I$ always has full support (is invertible)

Example: $\rho = |0\rangle\langle 0|$

$\sigma = |1\rangle\langle 1|$

$$D(\rho\|\sigma) = \infty$$

$$D(\rho\|\sigma + \varepsilon I) =$$

$$= \mathrm{Tr}\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \left( \log \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \log \begin{bmatrix} \varepsilon & 0 \\ 0 & 1+\varepsilon \end{bmatrix} \right) \right\}$$

$$= \mathrm{Tr}\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \left( \begin{bmatrix} \log 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} \log \varepsilon & 0 \\ 0 & \log(1+\varepsilon) \end{bmatrix} \right) \right\}$$

$$= -\mathrm{Tr}\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \log \varepsilon & 0 \\ 0 & \log(1+\varepsilon) \end{bmatrix} \right\} = -\log \varepsilon$$

$$\to \infty \quad \text{as } \varepsilon \searrow 0$$

Most important property of $D(\rho\|\sigma)$

Monotonicity w/ respect to quantum channels:

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$$

$\forall$ quantum channels $\mathcal{N}$

This inequality is so important that it can be regarded as a "law of quantum information theory." Essentially all fundamental limits can be derived from it. One can even argue the second law of thermodynamics from it.

proof is considered difficult, but a variety of approaches are known, including

1) limit of Renyi entropies

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \mathrm{Tr}\{\rho^\alpha \sigma^{1-\alpha}\}$$

& Lieb concavity theorem.

2) quantum hypothesis testing -

relate $D(\rho\|\sigma)$ to how well we can distinguish $\rho$ from $\sigma$.

Basic idea: If noise $N$ is applied to both $\rho$ + $\sigma$, then we cannot distinguish them as well, so $D(\rho\|\sigma)$ goes down.

3) use operator convexity of $-t\log t$ & some mathematical tricks

$$\Rightarrow \quad D(\rho\|\sigma) \geq 0 \quad \text{if } \underbrace{\mathrm{Tr}\{\rho\}}_{=p} \geq \underbrace{\mathrm{Tr}\{\sigma\}}_{=q}$$

Channel can be "trace out" channel

$$\Rightarrow D(\rho\|\sigma) \geq D(\mathrm{Tr}\{\rho\}\|\mathrm{Tr}\{\sigma\}) =$$

$$p(\log p - \log q) = p\log\frac{p}{q} \geq 0 \quad \text{if } p \geq q$$

Relative entropy as "mother entropy"

**Check:** (exercise)

$$-D(\rho \| I) = -\mathrm{Tr}\{\rho \log \rho\} = H(\rho)$$

Von Neumann entropy

$$-D(\rho_{AB} \| I_A \otimes \rho_B) = H(\rho_{AB}) - H(\rho_B)$$
$$= H(A|B)_\rho$$

conditional entropy

$$D(\rho_{AB} \| \rho_A \otimes \rho_B) = H(\rho_A) + H(\rho_B) - H(\rho_{AB})$$
$$= I(A;B)_\rho$$

quantum mutual information
"how far is $\rho_{AB}$ from being a product state?"

More interesting: conditional quantum mutual information

$$D(\rho_{ABC} \| \exp\{\log \rho_{AC} + \log \rho_{BC} - \log \rho_C\})$$
$$= H(AC)_\rho + H(BC)_\rho - H(C)_\rho - H(ABC)_\rho$$
$$\equiv I(A;B|C)_\rho$$

conditional quantum mutual information

$I(A;B|C) \geq 0$ known as strong subadditivity of entropy these entropies all receive meaning (physical or operational) in the context of quantum communication protocols. will focus on this in later lectures...

entropic uncertainty relation w/ quantum side information:

Given is a bipartite state $\rho_{AB}$

Alice performs one of two measurement channels on her system

$$\mathcal{M}^{x}_{A\to X}(\cdot) = \sum_{x} \operatorname{Tr}\{\Lambda^{x}_{A}(\cdot)\} |x\rangle\langle x|_X$$

$$\mathcal{M}^{z}_{A\to Z}(\cdot) = \sum_{z} \operatorname{Tr}\{\Gamma^{z}_{A}(\cdot)\} |z\rangle\langle z|_Z$$

Let $\varphi_{XB} = \mathcal{M}^{x}_{A\to X}(\rho_{AB})$

$\omega_{ZB} = \mathcal{M}^{z}_{A\to Z}(\rho_{AB})$

Bob should then try to guess which outcome Alice gets, after learning which measurement she performed.

Can quantify Bob's uncertainty about outcome w/ conditional entropy:

$H(X|B)_\sigma$ "How uncertain is Bob about outcome X given his quantum system B?"

$H(X|B)_\sigma + H(Z|B)_\omega$ ← sum of these uncertainties

- might not always be possible to make both be simultaneously zero.

it is known that

$$H(X|B)_\sigma + H(Z|B)_\omega \geq -\log c + H(A|B)_\rho$$

$c =$ "overlap of measurements" (incompatibility of measurements)

$$= \max_{x,z} \left[ \lambda_{max} \left( \sqrt{\Lambda^x} \sqrt{\Gamma^z} \right) \right]^2$$

technical condition: at least one of $\{\Lambda^x\}$ or $\{\Gamma^z\}$ should be a rank-one measurement

$H(A|B)$ - conditional entropy

- can be negative for entangled states

When is the inequality saturated?