Jan 17th

Finite dimensional Hilbert space $\mathcal{H}$.

$u, v \in \mathcal{H}$ $\quad \langle u, v \rangle$ inner product

$\lambda \in \mathbb{C}$ $\quad \langle u, \lambda v \rangle = \lambda \langle u, v \rangle$

$\langle \lambda u, v \rangle = \bar{\lambda} \langle u, v \rangle$

complex conjugate.

Linear operators $\mathcal{H} \to \mathcal{H}'$: $L(\mathcal{H}, \mathcal{H}')$

$L(\mathcal{H}, \mathcal{H}) =: L(\mathcal{H})$

For an operator $S \in L(\mathcal{H}, \mathcal{H}')$, the adjoint S^* is defined by

$L(\mathcal{H}', \mathcal{H})$

$$\langle u', Su \rangle = \langle S^* u', u \rangle \quad \text{for all } u \in \mathcal{H}, u' \in \mathcal{H}'.$$

Important classes of operators $S \in L(\mathcal{H})$:

- S is unitary if $SS^* = S^*S = I$ — identity.
- S is Hermitian if $S^* = S$.
- S is positive, we write $S \in \mathrm{Pos}(\mathcal{H})$ if S is Hermitian and $\langle u, Su \rangle \geq 0$ for all $u \in \mathcal{H}$. $S \geq 0$
- S is an orthogonal projection if $S^2 = S = S^*$. Such an S is positive.

Bra-ket notation:

We identify $u \in \mathcal{H}$ with $|u\rangle \in L(\mathbb{C}, \mathcal{H})$ — ket

defined by $|u\rangle : \mathbb{C} \to \mathcal{H}$

$$\lambda \mapsto \lambda \cdot u.$$

The adjoint $|u\rangle^* \in L(\mathcal{H}, \mathbb{C})$ is denoted $\langle u|$ — bra

$$\langle u | : \mathcal{H} \to \mathbb{C}$$
$$v \mapsto \langle u, v \rangle$$

We have $\cdot$ $\underset{\langle u, v \rangle.}{\underset{\parallel}{\langle u | \cdot | v \rangle}} \in L(\mathbb{C}, \mathbb{C})$ identified with $\mathbb{C}$.

$\Rightarrow$ will denote inner product by $\langle u | v \rangle$.

$\cdot$ $|v\rangle\langle u| \in L(\mathcal{H})$

Ex: e_i is a basis of $\mathcal{H}$ then
orthonormal
then $I = \sum_i |e_i\rangle\langle e_i|$.

Rk: We will often use shorthand $|i\rangle$ for $|e_i\rangle$
$|x\rangle$ for $|e_x\rangle$
$\vdots$

Spectral decomposition

. For any Hermitian $S \in L(\mathcal{H})$, then exists an orthonormal basis of $\mathcal{H}$ $\{e_i\}$ s.t.

$$S = \sum_{i=1}^{\dim \mathcal{H}} \lambda_i |e_i\rangle\langle e_i|$$

with $\lambda_i \in \mathbb{R}$.

. In other words S written in ONB $\{e_i\}$ is diagonal

$$S = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_{\dim(\mathcal{H})} \end{pmatrix}$$

- S is positive iff $\lambda_i \geq 0 \quad \forall i$.
- For $f : \mathbb{R} \to \mathbb{C}$,

$$f(S) = \sum_i f(\lambda_i) |e_i\rangle\langle e_i|$$

Tensor products:

Multiple systems $A, B, C, \ldots \quad X, Y, \ldots$

Hilbert space $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_C$

Hilbert space for joint system: $\mathcal{H}_A \otimes \mathcal{H}_B$

- vector space spanned by $u \otimes v$ — bilinear.
  for $u \in \mathcal{H}_A, v \in \mathcal{H}_B$
- inner product: $\langle u' \otimes v' | u \otimes v \rangle = \langle u' | u \rangle \cdot \langle v' | v \rangle$
  and linear extension.

For $S \in L(\mathcal{H}_A, \mathcal{H}_A')$, $T \in L(\mathcal{H}_B, \mathcal{H}_B')$ define $S \otimes T$:

$$(S \otimes T)(\underset{\in \mathcal{H}_A}{u} \otimes \underset{\in \mathcal{H}_B}{v}) = (Su) \otimes (Tv),$$ and linear extension

$$\underbrace{L(\mathcal{H}_A, \mathcal{H}_A') \otimes L(\mathcal{H}_B, \mathcal{H}_B')}^{= \operatorname{span}\{S \otimes T\}}$$

We identify: $L(\mathcal{H}_A, \mathcal{H}_A') \otimes L(\mathcal{H}_B, \mathcal{H}_B')$ and $L(\mathcal{H}_A \otimes \mathcal{H}_B, \mathcal{H}_A' \otimes \mathcal{H}_B')$

In particular $|u\rangle \otimes |v\rangle = |u \otimes v\rangle$

---

fixed ON basis.

$\operatorname{Tr} S = \sum_i \langle e_i, S e_i \rangle$

Def: . A density operator ρ on $\mathcal{H}$ is a normalized positive operator on $\mathcal{H}$, i.e., $\rho \in \operatorname{Pos}(\mathcal{H})$ and $\operatorname{Tr}(\rho) = 1$.

- The set of density operators is denoted $S(\mathcal{H})$.
- ρ is said to be pure if $\operatorname{rank}(\rho) = 1$ $\Leftrightarrow$ $\rho = |\psi\rangle\langle\psi|$ $\psi \in \mathcal{H}$.
- $\rho = \frac{1}{\dim \mathcal{H}} \cdot I$ "maximally" mixed.

Density operator formalism:

- If a system is represented by a vector $|\psi\rangle$ (e.g. $\alpha|0\rangle + \beta|1\rangle$) Then the density operator ρ representing this system is given by $\rho = |\psi\rangle\langle\psi|$.

  e.g. $\rho = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{pmatrix}$ in the basis $\{|0\rangle, |1\rangle\}$.

- **Composition**: State of a composite system is given by density operators on $\mathcal{H}_A \otimes \mathcal{H}_B$ if individual state spaces are $\mathcal{H}_A$ and $\mathcal{H}_B$.

Independent: state of joint system is $\rho_A \otimes \rho_B$ if individual state are ρ_A and ρ_B.

Notation: $\mathcal{H}_A \longrightarrow A$.

(for short we call the Hilbert space A)

- Evolution: Isolated evolution of a subsystem A corresponds to a unitary on A. For a state ρ_{AB} on composite system $A \otimes B$ with evolution on A given by U_A and the B system unchanged:

$$\rho'_{AB} = (U_A \otimes I_B)\,\rho_{AB}\,(U_A^* \otimes I_B).$$

- **Measurement**: A measurement on subsystem A is defined by operators $\{M_x\}_{x\in\mathcal{X}}$ for some set $\mathcal{X}$, $M_x \in L(A)$ satisfying $\sum_{x\in\mathcal{X}} M_x^* M_x = I$

Prob of outcome x: $p(x) = \mathrm{Tr}(M_x \otimes I_B\, \rho_{AB}\, M_x^* \otimes I_B)$

Check: $\sum_x{}' p(x) = \sum_x{}' \mathrm{Tr}(M_x^* M_x \otimes I_B\, \rho_{AB}) = \mathrm{Tr}(\rho_{AB}) = 1.$

$\mathrm{Tr}(ST) = \mathrm{Tr}(TS)$.

Post-measurement state conditioned on x:

$$\rho'_{AB,x} = \frac{(M_x \otimes I_B)\,\rho_{AB}\,(M_x^* \otimes I_B)}{p(x)}.$$

• Special case: projective measurement

You might be used to special case

$M_x = P_x$ with P_x projector (ie $P_x^* = P_x = P_x^2$)

coming from the spectral decomposition of observable O

$$O = \sum_x{}' \, x \cdot P_x$$

A general measurement can model eg., a unitary followed by a projective measurement: U_A followed by $\{P_x\}_{x \in X}$

$$p(x) = \mathrm{Tr}\Big(\big(\underbrace{P_x U_A}_{M_x} \otimes I_B\big) \rho_{AB} \big(\underbrace{U_A P_x}_{M_x^*} \otimes I_B\big)\Big)$$

• Special case: POVM measurement.

Often, we are not interested in post-measurement state but only in the probability distribution $p(x)$.

$$p(x) = \mathrm{Tr}\big((M_x \otimes I_B) \rho_{AB} (M_x^* \otimes I_B)\big)$$

$$= \mathrm{Tr}\big(M_x^* M_x \otimes I \, \rho_{AB} \big)$$

We let $E_x = M_x^* M_x$.

↑ only need to know E_x to determine $p(x)$ and not M_x.

Def: A positive operator valued measure (POVM) on A is a family $\{E_x\}_{x\in X}$ of positive operators on A such that $\sum_{x\in X} E_x = I_A$

Probability of outcome $x = \mathrm{Tr}(E_x \rho)$.

Quantum channels

- General way of describing evolution of state of a system
- The Hilbert space can change: $A \longrightarrow B$. (forget a system, add a particle...)
- $\mathcal{E}$ should map $S(A)$ to $S(B)$

↖ density operators ↖ density operators.

Def: A quantum channel $\mathcal{E}$ is a linear map from $L(A)$ to $L(B)$ satisfying:

linear ↑ maps convex combinations
$\mathcal{E}(p\rho_0+(1-p)\rho_1)=p\mathcal{E}(\rho_0)+(1-p)\mathcal{E}(\rho_1)$

- Completely positive.

  For $\rho\in \mathrm{Pos}(A)$, $\mathcal{E}(\rho)\in \mathrm{Pos}(B)$. (positive)

  For any Hilbert space R

  $\rho\in \mathrm{Pos}(A\otimes R)$ $(\mathcal{E}\otimes I_R)(\rho)\in \mathrm{Pos}(B\otimes R)$

  (completely positive)

  Identity on $L(R)$: "superoperator".

- Trace-preserving:

  For $T\in L(A)$, $\mathrm{Tr}(\mathcal{E}(T)) = \mathrm{Tr}(T)$

<u>Ex:</u> • $\mathcal{E} : L(A) \to L(A)$ $\quad U$ unitary on A

$$\mathcal{E}(T) = UTU^* \quad \text{for any } T \in L(A).$$

* Completely positive:

$$(\mathcal{E} \otimes I_R)(\rho) = (U \otimes I_R)\,\rho\,(U^* \otimes I_R) \geq 0$$

$$\Big[\langle v, (U \otimes I_R)\rho(U^* \otimes I_R) v\rangle$$
$$= \langle (U^* \otimes I_R)v, \rho\, U^* \otimes I_R v\rangle \geq 0\Big]$$

More generally, a map

$$\mathcal{E}(T) = STS^* \quad \text{for all } T$$

is completely positive.

* Trace preserving: $\mathrm{Tr}(UTU^*) = \mathrm{Tr}(U^*UT) = \mathrm{Tr}(T)$.

• Partial trace map. ← important example.

$\rho_{AB} \in S(A \otimes B)$ state of a composite system.

What is the state of system A on its own?

→ Should be a valid quantum channel, corresponds to "forgetting" B.

$$\mathrm{Tr}_B : L(A \otimes B) \longrightarrow L(A).$$

$$T \longmapsto \sum_b (I_A \otimes \langle b|)\, T\, (I_A \otimes |b\rangle)$$

where $\{|b\rangle\}_b$ forms a basis of B.

Note that $\mathrm{Tr}_B = \underbrace{I_A}_{\text{identity}: L(A)\to L(A)} \otimes \underbrace{\mathrm{Tr}}_{\text{map from } L(B)\to\mathbb{C}}$.

$$\mathrm{Tr}_B(\rho_A \otimes \rho_B) = \rho_A \cdot \mathrm{Tr}\,\rho_B = \rho_A \text{ if } \rho_B \in S(B).$$

Tr_B plays the role of taking the marginal distribution of a joint distribution.

$\{|a\rangle\}_a$ ONB of A

$\{|b\rangle\}_b$ ONB of B

$$\rho_{AB} = \sum_{a,b} P(a,b)\, |a\rangle\langle a| \otimes |b\rangle\langle b|$$

then $$\rho_A = \mathrm{Tr}_B\, \rho_{AB} = \sum_a \Big(\sum_b P(a,b)\Big) |a\rangle\langle a|$$

Check: Complete $\overset{\mathrm{CP}}{\shortparallel}$ positivity: $T \mapsto (I_A \otimes \langle b|)\, T\, (I_A \otimes |b\rangle)$ is CP

Sum of CP is CP.

- Trace-preserving: $\sum_b \mathrm{Tr}\big(I \otimes \langle b|\, T\, I \otimes |b\rangle\big) = \sum_b \mathrm{Tr}\big(I \otimes |b\rangle\langle b|\, T\big)$
$= \mathrm{Tr}(T)$.

- Measurements.

$\{M_x\}_{x\in X}$ $\quad \sum_x M_x^* M_x = I_A$.

Want the output of the channel to contain both the outcome x and the post measurement state.

Input: A $\qquad$ Output: $X \otimes A$ ← post measurement state.

↖ holds outcome $\dim X = |X|$.

fixed basis $\{|x\rangle\}_{x\in X}$

$$\mathcal{M} : L(A) \longrightarrow L(X \otimes A)$$

$$T \longmapsto \sum_{x \in X}' \underbrace{|x\rangle\langle x|}_{\text{operator on } X} \otimes \underbrace{M_x T M_x^*}_{\text{operator on } A}.$$

Check: • CP: $|x\rangle\langle x| \otimes M_x T M_x^* = \underbrace{(|x\rangle \otimes M_x)}_{L(A, X\otimes A)} T \underbrace{(\langle x| \otimes M_x^*)}_{\in L(X\otimes A, A)}$

$\Rightarrow$ same argument.

• Trace-preserving:

$$\mathrm{Tr}\left(\sum_x' |x\rangle\langle x| \otimes M_x T M_x^*\right) \overset{\mathrm{Tr}(|x\rangle\langle x|) = 1.}{\underset{\mathrm{Tr}(S\otimes T) = \mathrm{Tr}(S)\cdot\mathrm{Tr}(T).}{=}} \sum_x' \mathrm{Tr}(M_x^* M_x T) \overset{\sum_x M_x^* M_x = I.}{=} \mathrm{Tr}(T)$$

Can check that this models the measurement.

$$\mathcal{M}(\rho_A) = \sum_{x\in X}' \underbrace{\mathrm{Tr}(M_x \rho_A M_x^*)}_{\text{prob of outcome } x} |x\rangle\langle x| \otimes \underbrace{\frac{M_x \rho_A M_x^*}{\mathrm{Tr}(M_x \rho_A M_x^*)}}_{\text{post-measurement state conditioned on } x.}$$

Rk: Such a state is called a classical-quantum state.
(cq state)

i.e. of the form

$$\rho_{XA} = \sum_{x\in X}' P_X(x)\, |x\rangle\langle x| \otimes \rho_A^x$$

$\{|x\rangle\}$ fixed basis, ρ_A^x density operator.

Distance measures between states

Def: The trace distance between two states ρ and σ in $S(A)$ is defined by

$$\Delta(\rho,\sigma) = \frac{1}{2}\underbrace{\|\rho-\sigma\|_1}_{\sum_i |\lambda_i|,\ \lambda_i \text{ eigenvalues of } \rho-\sigma} = \frac{1}{2}\mathrm{Tr}|\rho-\sigma| .$$

Rk: - $\Delta(\rho,\rho)=0$, $\Delta(\rho,\sigma) \leq \frac{1}{2}(\|\rho\|_1+\|\sigma\|_1) = 1$.

- Invariant under unitary

$$\Delta(U\rho U^*, U\sigma U^*) = \Delta(\rho,\sigma)$$

- For $\rho = \sum_a P(a)|a\rangle\langle a|$

$$\sigma = \sum_a Q(a)|a\rangle\langle a|$$

$$\Delta(\rho,\sigma) = \underbrace{\frac{1}{2}\sum_a |P(a)-Q(a)|}_{\text{called total variation distance between } P \text{ and } Q}$$

- Data processing ← important property for any distance measure.

$\mathcal{E}$ quantum channel

$$\Delta(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \leq \Delta(\rho,\sigma)$$

Operational interpretation: distinguishing states.

Hypotheses System A is either in:

$$H_0 : \rho_0 \qquad\qquad H_1 : \rho_1$$

Question: Minimum probability of error?

Strategy given by a POVM: $\underset{\Downarrow}{E_0}$, $\underset{\Downarrow}{E_1}$

$\qquad H_0 \qquad H_1$

Prior: H_0 with probability $1/2$.
$\qquad H_1$ with probability $1/2$.

$$\text{Error probability} = \frac{1}{2}\underbrace{\mathrm{Tr}(E_1\rho_0)}_{\substack{\text{state is } \rho_0 \\ \text{but we wrongly say } H_1 \\ \text{“Type I” error}}} + \frac{1}{2}\underbrace{\mathrm{Tr}(E_0\rho_1)}_{\substack{\text{state is } \rho_1 \\ \text{but wrongly say } H_0 \\ \text{“Type II” error}}}$$

Often H_0 and H_1 play asymetric role.

Proposition: The minimum error probability over all possible strategies is

$$\frac{1}{2} - \frac{1}{2}\Delta(\rho_0, \rho_1).$$

Rk: Hypothesis testing can also be considered in different regimes e.g. fix Type I error $\leq \varepsilon$ and minimize Type II error.

(also called divergence). 24/04/2023

Def: The hypothesis testing relative entropy with parameter $\varepsilon \in [0,1)$ is defined by

$$D_H^\varepsilon(\rho \| \sigma) = \max_{\substack{0 \le E \le I \\ \operatorname{Tr}(E\rho) \ge 1-\varepsilon}} -\log \operatorname{Tr}(E\sigma)$$

E corresponds to E_0, $E_1 = I - E_0 = I - E$.

Rk:
- $D_H^\varepsilon(\rho\|\sigma) \in [0,+\infty]$.
- $2^{-D_H^\varepsilon(\rho\|\sigma)}$ is the minimum Type II error if Type I error $\le \varepsilon$.
- For $\varepsilon = 1$, $D_H^1(\rho\|\sigma) = +\infty$ (not interesting).
- For $\varepsilon = 0$, $D_H^0(\rho\|\sigma) = -\log \operatorname{Tr}(\Pi_\rho \sigma)$

  where $\Pi_\rho :=$ projection onto the support of ρ

  $:= \sum'_{i : \lambda_i \neq 0} |e_i\rangle\langle e_i|$ where $\underset{\text{eigendecomposition}}{\rho = \sum'_i \lambda_i |e_i\rangle\langle e_i|}$.
- For $\rho = \sigma$, $D_H^\varepsilon(\rho\|\rho) = -\log(1-\varepsilon)$.

  $\simeq 0$ if ε small.
- For ρ and σ having orthogonal supports, i.e., $\rho\sigma = 0$

  $D_H^\varepsilon(\rho\|\sigma) = +\infty$

Announcements:

* Please send an email to omar.fawzi@ens-lyon.fr if you're planning to take the course
* Evaluation will be

  Paper presentation + report
  &
  One homework near the end.
* You are encouraged to prepare the problems you couldn't cover in tutorial for the following time.

Jan 25th

Further remarks about $D_H^\varepsilon(\rho\|\sigma)$

- In general, no closed form expression but it

$$\min_{0\le E\le I} \mathrm{Tr}(E\sigma) \quad \text{subject to } \mathrm{Tr}(E\rho)\ge 1-\varepsilon$$

is a convex optimization program, more specifically it is a semi-definite program.
can be computed efficiently for small dimension.

- Classical case $\rho = \sum_{x\in\mathcal{X}} P(x)\,|x\rangle\langle x|$

$$\sigma = \sum_{x\in\mathcal{X}} Q(x)\,|x\rangle\langle x|.$$

A natural test:

For sample x, compute $\underbrace{\frac{P(x)}{Q(x)}}$ → If ≥ 1 output "P"; If ≤ 1 output "Q"

called likelihood ratio.

Prop: D_H^ε satisfies the data processing inequality
i.e. for any quantum channel $\mathcal{E}$, we have

$$D_H^\varepsilon(\mathcal{E}(\rho)\,\|\,\mathcal{E}(\sigma)) \le D_H^\varepsilon(\rho\|\sigma)$$

Proof: Very intuitive: If I have a strategy to distinguish $\mathcal{E}(\rho)$ from $\mathcal{E}(\sigma)$, can distinguish ρ and σ by first applying $\mathcal{E}$ then the strategy.

Let E be such that

$$D_H^\varepsilon(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)) = -\log \operatorname{Tr}(E\mathcal{E}(\sigma)) \text{ and } \operatorname{Tr}(E\mathcal{E}(\rho)) \geq 1-\varepsilon$$

Note that $L(\mathcal{H})$ is itself a Hilbert space with inner product $\langle S,T\rangle = \operatorname{Tr}(S^*T)$.

So $\mathcal{E} \in L(L(\mathcal{H}))$ has an adjoint denoted $\mathcal{E}^*$, it satisfies:

$$\operatorname{Tr}(E\,\mathcal{E}(\sigma)) \underset{\uparrow}{=} \operatorname{Tr}(E^*\mathcal{E}(\sigma)) = \operatorname{Tr}(\mathcal{E}^*(E)\sigma)$$

E is Hermitian

and $\operatorname{Tr}(E\mathcal{E}(\rho)) = \operatorname{Tr}(\mathcal{E}^*(E)\rho)$

Fact: $\mathcal{E}$ completely positive $\iff$ $\mathcal{E}^*$ completely positive.

$\mathcal{E}$ trace preserving $\iff$ $\mathcal{E}^*$ is unital i.e. $\mathcal{E}^*(I) = I$.

As a result, $\mathcal{E}^*(E)$ satisfies

$$0 = \mathcal{E}^*(0) \leq \mathcal{E}^*(E) \leq \mathcal{E}^*(I) = I.$$

and it is a feasible solution for the program for $D_H^\varepsilon(\rho\|\sigma)$

So $D_H^\varepsilon(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)) \leq D_H^\varepsilon(\rho\|\sigma)$ ■

Special states of interest: $\rho^{\otimes n}$, $\sigma^{\otimes n}$ with $n \to \infty$.

<u>Th</u> (Quantum Stein Lemma)

Let $\varepsilon \in (0,1)$ and $\rho, \sigma \in S(A)$.

Then

$$\lim_{n\to\infty} \frac{1}{n} D_H^{\varepsilon}\left(\rho^{\otimes n} \| \sigma^{\otimes n}\right) = D(\rho\|\sigma).$$

The quantum relative entropy

Will give proof sketch.

<u>Def</u>: For $\rho \in S(A)$, $\sigma \in Pos(A)$ where A is a finite dimensional Hilbert space, the quantum relative entropy is defined by:

(ρ state but σ not necessarily normalized)

$\mathrm{supp}(\rho) = \mathrm{Span}\{|e_i\rangle : \lambda_i \neq 0\}$ if $\rho = \sum_i \lambda_i |e_i\rangle\langle e_i|$

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

Rk: * $\log\rho = \sum_i' (\log\lambda_i) |e_i\rangle\langle e_i|$ for $\rho = \sum_i' \lambda_i |e_i\rangle\langle e_i|$, $\lambda_i \neq 0$.

* Classical case, i.e. ρ and σ commute

$$\rho = \sum_x' P(x) |x\rangle\langle x|, \quad \sigma = \sum_x Q(x) |x\rangle\langle x|.$$

$$D(\rho\|\sigma) = \underbrace{\sum_x' P(x) \log\frac{P(x)}{Q(x)}}_{\text{called relative entropy or Kullback-Leibler divergence}}$$

Quantum relative entropy can be seen as a noncommutative generalization of KL divergence (there are others as well)

<u>Th</u> (Properties of the quantum relative entropy)

- We have $D(\rho \| \sigma) \geq 0$ for $\rho, \sigma \in S(A)$ with equality iff $\rho = \sigma$.
- Data processing for D: for a quantum channel $\mathcal{E}$

$$D(\mathcal{E}(\rho) \| \mathcal{E}(\sigma)) \leq D(\rho \| \sigma)$$

We skip the proof, proof of data processing not easy.

D can be used to define entropies

<u>Def:</u> For a state $\rho_{AB} \in S(A \otimes B)$ we define

- $H(A)_\rho := -D(\rho_A \| I_A)$

entropy

sign.

not normalized.

Recall $\rho_A = \mathrm{Tr}_B \rho_{AB}$

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

conditional entropy

von Neumann entropies.

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

mutual information

Properties in TD.

Proof of Stein lemma:

Will only give elements. See references for full proofs.

Recall $\lim_{n\to\infty} \frac{1}{n} D_H^{\varepsilon}(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho\|\sigma)$

* Achievability: $\geq$ (have to give a strategy)

Will restrict to case where $\boxed{\rho \text{ and } \sigma \text{ commute}}$.

$\rho = \sum_x P(x) |x\rangle\langle x|$ $\qquad$ $\sigma = \sum_x Q(x) |x\rangle\langle x|$.

$$\rho^{\otimes n} = \sum_{x_1 \cdots x_n} P(x_1)\cdots P(x_n) |x_1\rangle\langle x_1| \otimes \cdots \otimes |x_n\rangle\langle x_n|$$

$$\sigma^{\otimes n} = \sum_{x_1 \cdots x_n} Q(x_1)\cdots Q(x_n) |x_1\rangle\langle x_1| \otimes \cdots \otimes |x_n\rangle\langle x_n|.$$

Will define a test for this hypothesis testing problem.

Given $X_1, \ldots, X_n$

Compute $R = \dfrac{P(X_1)P(X_2)\cdots P(X_n)}{Q(X_1)Q(X_2)\cdots Q(X_n)}$

If $\frac{1}{n}\log R \geq D(P\|Q) - \delta$

Return "Samples from P".

Else Return "Samples from Q".

$\delta > 0$ is a parameter, will let $\delta \to 0$ at the end.

In quantum notation corresponds to:

$$E = \sum_{x_1 \cdots x_n : \frac{P(x_1)\cdots P(x_n)}{Q(x_1)\cdots Q(x_n)} \geq 2^{n(D(P\|Q)-\delta)}} |x_1 \cdots x_n\rangle\langle x_1 \cdots x_n|$$

it clearly depends on n

Analysis of this test.

* If samples are from P. (Hypothesis 0)

$$\mathbb{P}_{X_1 \dots X_n \sim P} \left\{ \frac{1}{n} \log R \geq D(P\|Q) - \delta \right\} \quad \left(= \mathrm{Tr}(E_{\ell}^{\otimes n}) \right)$$

$$= \mathbb{P}\left\{ \frac{1}{n} \sum_{i=1}^{n} \log \frac{P(X_i)}{Q(X_i)} \geq D(P\|Q) - \delta \right\}$$

But $\mathbb{E}_{X_i \sim P}\left\{ \log \frac{P(X_i)}{Q(X_i)} \right\} = \sum_x P(x) \log \frac{P(x)}{Q(x)} = D(P\|Q)$.

So by the law of large numbers

$$\xrightarrow[n \to \infty]{} 1$$

The constraint $\mathrm{Tr}(E_{\ell}^{\otimes n}) \geq 1 - \varepsilon$ satisfied for large enough n.

* If samples are from Q. (Hypothesis 1)

$$\underbrace{\mathbb{P}_{X_1 \dots X_n \sim Q} \left\{ \frac{1}{n} \log R \geq D(P\|Q) - \delta \right\}}_{= \mathrm{Tr}(E_{\sigma}^{\otimes n})} = \sum_{x_1, \dots, x_n}' Q(x_1) \dots Q(x_n)$$

$$\frac{1}{n} \sum_i' \log \frac{P(x_i)}{Q(x_i)} \geq \left(D(P\|Q) - \delta \right)$$

$$= \sum_{x_1 \dots x_n}' Q(x_1) \dots Q(x_n).$$

$$Q(x_1) \dots Q(x_n) \leq 2^{-n(D(P\|Q) - \delta)} P(x_1) \dots P(x_n)$$

$$\leq 2^{-n(D(P\|Q) - \delta)} \sum_{x_1 \dots x_n}' P(x_1) \dots P(x_n)$$

$$\leq 2^{-n(D(P\|Q) - \delta)}$$

So
$$-\log \mathrm{Tr}(E\sigma^{\otimes n}) \geq n\left(D(P\|Q)-\delta\right)$$
and $\frac{1}{n} D_H^{\varepsilon}\left(\rho^{\otimes n} \| \sigma^{\otimes n}\right) \geq D(P\|Q) - \delta$

for large enough n.

Works for any $\delta > 0$ so we have
$$\lim_{n\to\infty} \frac{1}{n} D_H^{\varepsilon}\left(\rho^{\otimes n} \| \sigma^{\otimes n}\right) \geq D(P\|Q).$$

* Converse:

Will only prove
$$\lim_{\varepsilon \to 0} \lim_{n\to\infty} \frac{1}{n} D_H^{\varepsilon}\left(\rho^{\otimes n} \| \sigma^{\otimes n}\right) \leq D(\rho\|\sigma)$$

General quantum case

The statement is that it holds for any $\varepsilon \in (0,1)$

Let E be such that $\mathrm{Tr}(E\rho^{\otimes n}) \geq 1-\varepsilon$.

We apply the data processing inequality for the quantum channel
$$\mathcal{E} : L(A^{\otimes n}) \longrightarrow L(\mathbb{C}^2)$$
$$T \longmapsto |0\rangle\langle 0| \mathrm{Tr}(ET) + |1\rangle\langle 1| \mathrm{Tr}((\mathbb{1}-E)T).$$

$$\mathcal{E}(\rho^{\otimes n}) = |0\rangle\langle 0| \mathrm{Tr}(E\rho^{\otimes n}) + |1\rangle\langle 1| \left(1 - \mathrm{Tr}(E\rho^{\otimes n})\right)$$
$$\mathcal{E}(\sigma^{\otimes n}) = |0\rangle\langle 0| \mathrm{Tr}(E\sigma^{\otimes n}) + |1\rangle\langle 1| \left(1 - \mathrm{Tr}(E\sigma^{\otimes n})\right)$$

We have on one side:

- $D(\rho^{\otimes n} \| \sigma^{\otimes n}) = \mathrm{Tr}(\rho^{\otimes n} \log \rho^{\otimes n}) - \mathrm{Tr}(\rho^{\otimes n} \log \sigma^{\otimes n})$

Note that if $\rho = \sum_x' \lambda_x |x\rangle\langle x|$ for a basis $\{|x\rangle\}$

$$\rho^{\otimes n} = \sum_{x_1 \cdots x_n}' \lambda_{x_1} \lambda_{x_2} \cdots \lambda_{x_n} |x_1 \cdots x_n\rangle\langle x_1 \cdots x_n|$$

$$\log(\rho^{\otimes n}) = \sum_{x_1 \cdots x_n}' \sum_{i=1}^{n}{}' \log \lambda_i \, |x_1 \cdots x_n\rangle\langle x_1 \cdots x_n|$$

$$= \sum_{i=1}^{n}{}' I_{A_1} \otimes \cdots \otimes I_{A_{i-1}} \otimes (\log \rho_{A_i}) \otimes I_{A_{i+1}} \otimes \cdots \otimes I_{A_n}$$

So $\mathrm{Tr}(\rho^{\otimes n} \log \rho^{\otimes n}) = n \mathrm{Tr}(\rho \log \rho)$

and $D(\rho^{\otimes n} \| \sigma^{\otimes n}) = n D(\rho \| \sigma)$.

- But

data processing

$$D(\rho^{\otimes n} \| \sigma^{\otimes n}) \geq D(\mathcal{E}(\rho^{\otimes n}) \| \mathcal{E}(\sigma^{\otimes n}))$$

$$= \mathrm{Tr}(E\rho^{\otimes n}) \log \frac{\mathrm{Tr}(E\rho^{\otimes n})}{\mathrm{Tr}(E\sigma^{\otimes n})} + (1 - \mathrm{Tr}(E\rho^{\otimes n})) \log \left(\frac{1 - \mathrm{Tr}(E\rho^{\otimes n})}{1 - \mathrm{Tr}(E\sigma^{\otimes n})} \right)$$

$$\geq -1 - \mathrm{Tr}(E\rho^{\otimes n}) \log \mathrm{Tr}(E\sigma^{\otimes n})$$

elementary inequalities

So $-\log \mathrm{Tr}(E\sigma^{\otimes n}) \leq \dfrac{n D(\rho\|\sigma) + 1}{\mathrm{Tr}(E\rho^{\otimes n})} \leq \dfrac{n D(\rho\|\sigma) + 1}{1 - \varepsilon}$

$$\frac{1}{n} D_H^{\varepsilon}(\rho^{\otimes n} \| \sigma^{\otimes n}) \leq \frac{D(\rho\|\sigma)}{1-\varepsilon} + \frac{1}{(1-\varepsilon) \cdot n}$$

letting $n \to \infty$ then $\varepsilon \to 0$, we get the desired result. ⊠

Rk: • D_H^ε is called a "one-shot entropy" measure as it has an operational interpretation for any states. Many others: H_{min}^ε $\leftarrow$ Cryptography.
$\vdots$
"worst case" entropy.

- The usual relative entropy D and corresponding von Neumann entropy H only has an operational interpretation in an iid (independent identically distributed) or average setting

Feb 8th.

Purification of a quantum state:

Prop: Any quantum state $|\psi\rangle \in A \otimes B$ can be written as

≥ 0 Schmidt coefficients

$$|\psi\rangle = \sum_i s_i |u_i\rangle_A \otimes |v_i\rangle_B$$

where $|u_i\rangle$ are eigenvectors of $Tr_B(|\psi\rangle\langle\psi|)$ and $|v_i\rangle$ are eigenvectors of $Tr_A(|\psi\rangle\langle\psi|)$ } unit norm & orthogonal

and s_i^2 are the eigenvalues of $Tr_A(|\psi\rangle\langle\psi|)$ and of $Tr_B(|\psi\rangle\langle\psi|)$

Same as the singular value decomposition using the isomorphism $\underbrace{|u\rangle\otimes|v\rangle}_{A\otimes B} \leftrightarrow \underbrace{|u\rangle\langle v|}_{L(B,A)}$

Consequence: If ρ_{AB} is pure, then ρ_A and ρ_B have the same non zero eigenvalue.

Prop: For any density operator $\rho_A \in S(A)$ and a Hilbert space B with $\dim B \geq \operatorname{rank}(\rho_A)$, there exists a state $\rho_{AB} \in S(A\otimes B)$ s.t.

* $Tr_B(\rho_{AB}) = \rho_A$.
* ρ_{AB} is pure.

Proof: Spectral decomposition $\rho_A = \sum_{i=1}^{r} \lambda_i |u_i\rangle\langle u_i|$, $r = \operatorname{rank}(\rho_A)$

Let $\{|v_i\rangle_B\}_{i=1,\dots,r}$ be r orthonormal vectors in B

Define $\rho_{AB} = |\psi\rangle\langle\psi|$

with $|\psi\rangle = \sum_{i=1}^{r} \sqrt{\lambda_i}\, |u_i\rangle_A \otimes |v_i\rangle_B$

$\text{rank}(\rho_{AB}) = 1$ by construction.

$$\text{Tr}_B\, \rho_{AB} = \sum_{i,i'=1}^{r} \sqrt{\lambda_i \lambda_{i'}}\, |u_i\rangle\langle u_{i'}|_A \otimes \underbrace{\text{Tr}\big(|v_i\rangle\langle v_{i'}|_B\big)}_{=\delta_{ii'}}$$

$$= \sum_{i=1}^{r} \lambda_i\, |u_i\rangle\langle u_i|_A = \rho_A \blacksquare$$

Another similarity measure for quantum states: Fidelity

For pure states $|\varphi\rangle$, $|\psi\rangle$, $|\langle\varphi|\psi\rangle|$ is a useful similarity measure. Fidelity generalizes it for density operators.

Def: The fidelity between ρ and $\sigma \in S(A)$ is defined by

$$F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1 = \text{Tr}\left(\sqrt{\sqrt{\sigma}\,\rho\sqrt{\sigma}}\right)$$

$$\|S\|_1 := \text{Tr}\left(\sqrt{S^* S}\right)$$

Rk: * If one of the states is pure, $\sigma = |\psi\rangle\langle\psi|$, then $F(\rho,\sigma) = \sqrt{\langle\psi|\rho|\psi\rangle}$

If ρ is also pure $\rho = |\varphi\rangle\langle\varphi|$, $F(\rho,\sigma) = |\langle\psi|\varphi\rangle|$

* $F(\rho,\rho) = 1$ and $F(\rho,\sigma) = 0$ if ρ & σ have orthogonal supports.

* If $\rho = \sum_i' P(i)\, |i\rangle\langle i|$, $\sigma = \sum_i' Q(i)\, |i\rangle\langle i|$

$$F(\rho,\sigma) = \sum_i' \sqrt{P(i)}\sqrt{Q(i)}$$

By Cauchy-Schwarz, easy to see $F(\rho,\sigma)=1 \Leftrightarrow \rho=\sigma$

* The fidelity does not have a direct operational meaning like trace distance but it is often very convenient to use.

<u>Th (Uhlmann)</u>

Let $\rho_A, \sigma_A \in S(A)$ and let B with $\dim B \geq \dim A$.
Then

$$F(\rho_A,\sigma_A) = \max_{\substack{\rho_{AB},\sigma_{AB} \\ \text{purifications of} \\ \rho_A,\sigma_A}} F(\rho_{AB},\sigma_{AB})$$

$\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$
$\sigma_{AB} = |\varphi\rangle\langle\varphi|_{AB}$ $\rightarrow$

$$= \max_{\substack{|\psi\rangle_{AB}, |\varphi\rangle_{AB} \\ \text{purifications of} \\ \rho_A, \sigma_B}} |\langle\psi|\varphi\rangle| .$$

<u>Proof</u>: Let $\{|i\rangle_A\}_i$ be an orthonormal basis of A and $\{|i\rangle_B\}_i$ an orthonormal basis of B (assume $\dim A = \dim B$)

Define $|\Phi\rangle_{AB} = \sum_i' |i\rangle_A \otimes |i\rangle_B$. $\in A\otimes B$.

unnormalized entangled state.

• Claim: For any purification $|\psi\rangle_{AB}$ of ρ_A, there exist unitaries U_A, U_B such that

$$|\psi\rangle_{AB} = \left(\sqrt{\rho_A}\, U_A \otimes U_B\right) |\Phi\rangle_{AB} .$$

In fact, write Schmidt decomposition

$$|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i}\, |u_i\rangle_A \otimes |v_i\rangle_B .$$ where λ_i are eigenvalues of ρ_A and $|u_i\rangle$ eigenvectors

Let U_A be the unitary $|i\rangle_A \to |u_i\rangle_A$

U_B be the unitary $|i\rangle_B \to |v_i\rangle_B$

So $\sqrt{\rho_A}\, U_A \otimes U_B\, |i\rangle_A \otimes |i\rangle_B = \sqrt{\lambda_i}\, |u_i\rangle |v_i\rangle$

which proves the claim.

Similarly $|\varphi\rangle_{AB} = \sqrt{\sigma_A}\, V_A \otimes V_B\, |\Phi\rangle_{AB}$.

• Another useful fact about $|\Phi\rangle_{AB}$:

$$\left(I_A \otimes S_B\right) |\Phi\rangle_{AB} = \left(S'_A \otimes I_B\right) |\Phi_{AB}\rangle$$

where $S'_A = S_B^T$ ← Transpose in fixed basis $|i\rangle_B$.

(To be accurate, $S'_A = W^{-1} S_B^T W$ with $W: |i\rangle_A \mapsto |i\rangle_B$)

"Transpose trick".

So

$$|\langle\psi|\varphi\rangle| = |\langle\Phi| U_A^\dagger \sqrt{\rho_A}\sqrt{\sigma_A} V_A \otimes U_B^\dagger V_B |\Phi\rangle|$$

$$= |\langle\Phi| U_A^\dagger \sqrt{\rho_A}\sqrt{\sigma_A} V_A \underbrace{(U_B^\dagger V_B)^T}_{\text{acts on } A} \otimes I_B |\Phi\rangle|$$

$$= \left| \mathrm{Tr}\left(U_A^* \sqrt{\rho_A}\sqrt{\sigma_A} V_A (U_B^* V_B)^T \right) \right|$$

$$= \left| \mathrm{Tr}\left(\sqrt{\rho_A}\sqrt{\sigma_A}\, U \right) \right| \quad \text{where } \underbrace{U = V_A (U_B^* V_B)^T U_A^*}_{\text{unitary}} .$$

<u>Lemma:</u> Operator S, $\max_{U \text{ unitary}} |\mathrm{Tr}(SU)| = \mathrm{Tr}\sqrt{S^* S}$

Proof: Polar decomposition + Cauchy-Schwarz.

This concludes the proof of Uhlmann ■

Rk: Some consequences

* $0 \leq F(\rho,\sigma) \leq 1$.
* $F(\rho_{AB}, \sigma_{AB}) \leq F(\rho_A, \sigma_A)$

$$\max_{\substack{\rho_{ABC}\ \sigma_{ABC} \\ \text{purifications}}} F(\rho_{ABC}, \sigma_{ABC}) \leq \max_{\substack{\rho_{AD}\ \sigma_{AD} \\ \text{purification}}} F(\rho_{AD}, \sigma_{AD})$$

Specific purifications of ρ_A and σ_A

* Satisfies "data processing" inequality. $\mathcal{E}$ quantum channel

$$F(\rho,\sigma) \leq F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) .$$ (see TD)

<u>Lemma:</u> $\rho, \sigma \in S(A)$.

$$1 - F(\rho,\sigma) \leq \Delta(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}$$

More on the representation of quantum channels

Recall we defined a quantum channel $\mathcal{E} : L(A) \to L(B)$ completely positive & trace preserving.

$\mathcal{E} \otimes I_R$ positive $\qquad \mathrm{Tr} \circ \mathcal{E} = \mathrm{Tr}$.

3 ways of representing a quantum channel.

* Choi ← one operator in $L(A \otimes B)$.
* Kraus ← a list of operators in $L(A, B)$
* Stinespring ← an operator in $L(A, B \otimes E)$ ← new space to be defined

The Choi operator: Fix a basis of A $\{|a\rangle\}_a$, let $\bar{A} \cong A$

$$J^{\mathcal{E}}_{\bar{A}B} = \sum_{a,a'} |a\rangle\langle a'|_{\bar{A}} \otimes \mathcal{E}(|a\rangle\langle a'|_A) \in L(\bar{A} \otimes B)$$

$$= (I_{\bar{A}} \otimes \mathcal{E})(\Phi)$$

← unnormalized maximally entangled state

Rk: We often just write A instead of $\bar{A}$.

Ex:

- $\mathcal{E} = I$ identity channel $(B \cong A)$

$$J^{\mathcal{E}} = \Phi = \sum_{a a'} |aa\rangle\langle a'a'|$$

- $\mathcal{E} = \mathrm{Tr}$ $\qquad (B = \mathbb{C})$

$$J^{\mathcal{E}} = I_A$$

- $\mathcal{E}(S) = \mathrm{Tr}(S)\sigma$ (constant output)

$$J^{\mathcal{E}} = \sum_{aa'} |a\rangle\langle a'| \otimes \mathrm{Tr}(\mathrm{Tr}(|a\rangle\langle a'|)\sigma) = I_A \otimes \sigma$$

Does $J^{\mathcal{E}}$ capture everything about $\mathcal{E}$?

Choi-Jamiolkowski isomorphism : $L(L(A), L(B)) \longrightarrow L(A \otimes B)$

$$\mathcal{E} \mapsto J^{\mathcal{E}}$$

and its inverse is

Transpose with respect to basis $\{|a\rangle\}$

$$J \longmapsto \underbrace{\left[S_A \longmapsto \operatorname{Tr}_A\left(\left(S_A^T \otimes I_B\right) J \right) \right]}_{\mathcal{F}}.$$

Check:

$$\sum_{a,a'} |a\rangle\langle a'| \otimes \mathcal{F}(|a\rangle\langle a'|) = \sum_{a,a'} |a\rangle\langle a'| \otimes \operatorname{Tr}_A\left((\underbrace{|a\rangle\langle a'|^T}_{|a'\rangle\langle a|} \otimes I) J \right)$$

$$= \sum_{a,a'} |a\rangle\langle a'| \otimes \langle a'| \left(|a'\rangle\langle a| \otimes I\right) J |a'\rangle$$

$$= \sum_{a,a'} |a\rangle\langle a'| \otimes \langle a| J |a'\rangle$$

$$= J.$$

$J^{\mathcal{E}}$ can be used to easily check if $\mathcal{E}$ is a valid quantum channel

Th: • $\mathcal{E} \in L(L(A), L(B))$ is completely positive

$\Updownarrow$

$J_{AB}^{\mathcal{E}} \geq 0$

• $\mathcal{E}$ is trace-preserving $\iff J_A^{\mathcal{E}} = I_A$.

$\operatorname{Tr}_B(J_{AB}^{\mathcal{E}})$

Conseq: • Complete positivity can be checked efficiently.

for all R $(I_R \otimes \mathcal{E})(S) \geq 0$ for $S \in \operatorname{Pos}(R \otimes A)$.

Theorem says sufficient to take $R \cong A$ and $S = \sum_{a,a'} |aa\rangle\langle a'a'|$

Proof: • $\Downarrow$ is obvious

$\Uparrow$: $J_{AB}^{\mathcal{E}} = \sum_x' \lambda_x |\varphi_x\rangle\langle\varphi_x|$ eigendecomposition.

Write $\mathcal{E}(S_A) = \sum_x' K_x S_A K_x^*$, directly CP.

$$\mathcal{E}(S_A) = \sum_x' \lambda_x \mathrm{Tr}_A\big((S_A^T \otimes I_B)|\varphi_x\rangle\langle\varphi_x|\big)$$
$$= \sum_{x,a}' \lambda_x \langle a|(S_A^T \otimes I_B)\cdot|\varphi_x\rangle\langle\varphi_x|a\rangle$$

Can write $|\varphi_x\rangle = \sum_{a,b}' \langle a,b|\varphi_x\rangle |a\rangle_A \otimes |b\rangle_B$

So $|\varphi_x\rangle\langle\varphi_x| = \sum_{a,b,a',b'}' \langle a',b'|\varphi_x\rangle\langle\varphi_x|a,b\rangle |a'\rangle\langle a| \otimes |b'\rangle\langle b|$

$$= \sum_{\substack{a,a,a' \\ b,b'}}' \lambda_x \langle a|S_A^T|a'\rangle |b'\rangle\langle b| \cdot \langle a',b'|\varphi_x\rangle \langle\varphi_x|a,b\rangle$$

$$= \sum_{\substack{x \\ i\, b\, i' b'}}' \sqrt{\lambda_x}\langle a'b'|\varphi_x\rangle |b'\rangle \langle a'|S_A|a\rangle\langle b| \langle\varphi_x|a,b\rangle \cdot \sqrt{\lambda_x}$$

$$= \sum_x' K_x S_A K_x^* \text{ where } K_x = \sum_{a'b'} \langle a'b'|\varphi_x\rangle |b'\rangle\langle a'| \sqrt{\lambda_x}$$

• $\Rightarrow$ direct as $\mathrm{Tr}(\mathcal{E}(|i\rangle\langle j|)) = \delta_{ij}$

$\Leftarrow$ $\mathrm{Tr}\big(\mathrm{Tr}_A((S_A^T \otimes I_B) J_{AB}^{\mathcal{E}})\big) = \mathrm{Tr}\big((S_A^T \otimes I_B) J_{AB}^{\mathcal{E}}\big)$
$= \mathrm{Tr}\big(S_A^T \mathrm{Tr}_B(J_{AB}^{\mathcal{E}})\big)$
$= \mathrm{Tr}(S_A^T)$
$= \mathrm{Tr}(S_A)$ $\blacksquare$

Corollary: Any CP map $\mathcal{E}: L(A) \to L(B)$ can be written as

$$\mathcal{E}(S_A) = \sum_{x=1}^{r} K_x S_A K_x^*$$

where $K_x \in L(A,B)$ ← called Kraus operators

with $r \leq (\dim A)(\dim B)$ ← actually $r = \operatorname{rank}(J^{\mathcal{E}})$.

$\mathcal{E}$ is trace-preserving iff $\sum_x K_x^* K_x = I_A$

Rk: Also called operator-sum representation, Kraus

(Stinespring dilation)

Corollary: Any CP map $\mathcal{E}: L(A) \to L(B)$

can be written as

$$\mathcal{E}(S_A) = \operatorname{Tr}_E\left(M S_A M^*\right)$$

where $M \in L(A, B \otimes E)$

with $\dim E \leq (\dim A)(\dim B)$

$\mathcal{E}$ is trace-preserving iff $\underbrace{M^* M = I_A}_{M \text{ is an isometry}}$

i.e. preserves norms $\|M|\psi\rangle\| = \||\psi\rangle\|$

Proof:

Write $\mathcal{E}(S_A) = \sum_x K_x S_A K_x^*$

Let $E = \operatorname{span}\{|x\rangle\}$

and $M = \sum_x K_x \otimes |x\rangle$

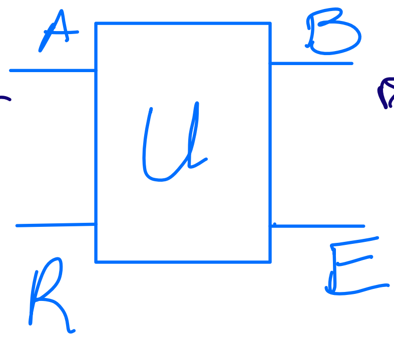
Then $M S_A M^* = \sum_{x,x'} K_x S_A K_{x'}^* \otimes |x\rangle\langle x'|_E$ ∎

Interpretation:

Can see any evolution modeled by quantum channel $\mathcal{E}: L(A) \to L(B)$ as a unitary evolution

Input space of interest

output space of interest



fixed state

environment we do not have access to

$U: |\psi\rangle_A \otimes |0\rangle_R \mapsto M|\psi\rangle$ (check: such a unitary exists)