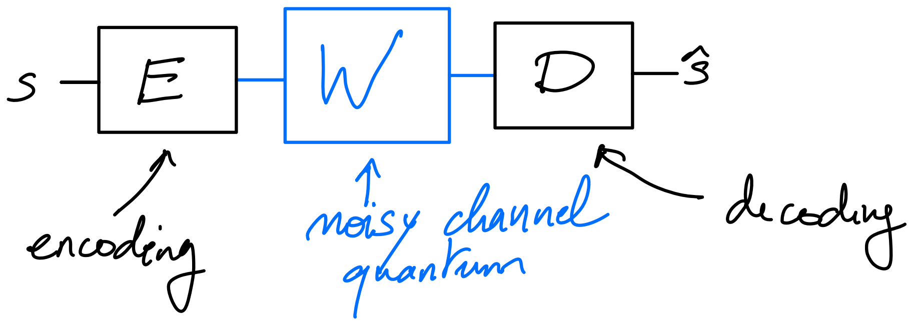
QUANTUM INFORMATION THEORY.



WANT : * $s \simeq \hat{s}$ with high probability

* maximize bits or qubits in s.

Objective : Understand fundamental limits

Plan :
1. States, channels.
2. State discrimination, Stein's lemma.
3. Data processing for the quantum relative entropy
   Also called strong subadditivity of von Neumann entropy
4. Classical communication over quantum channels.
   Shannon channel coding will be a special case.
5. Quantum communication over quantum channels.

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 $\cdot\ \underset{\langle u, v\rangle .}{\underset{\|}{\langle u|\cdot|v\rangle}} \in L(\mathbb{C}, \mathbb{C})$ 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 $\underset{\text{orthonormal}}{\text{basis}}$ of $\mathcal{H}$ then

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 $\lambda_i \geq 0 \ \forall i$.
- For $f: \mathbb{R} \to \mathbb{C}$,

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

Tensor products:

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

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 $S \otimes T$:

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

We identify: $\underbrace{L(\mathcal{H}_A, \mathcal{H}_A') \otimes L(\mathcal{H}_B, \mathcal{H}_B')}^{= \text{span}\{S \otimes T\}}$ 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.

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

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

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

Prepare ρ_A on system A and independently ρ_B on B: $\rho_A \otimes \rho_B$.

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 $p(x)$.

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

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

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 $S(B)$

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

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

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

- Trace-preserving:

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

<u>Remark</u>: Why complete positivity and not just positivity?

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

It turns out that positivity of a map is not stable under tensor product i.e.

$\exists$ $\mathcal{E}$, $\mathcal{F}$ positive maps $\mathcal{E}: L(A) \to L(B)$, $\mathcal{F}: L(\bar{A}) \to L(\bar{B})$ such that $\mathcal{E} \otimes \mathcal{F}$ defined by:

$$(\mathcal{E} \otimes \mathcal{F})(S \otimes T) = \mathcal{E}(S) \otimes \mathcal{F}(T)$$

is not positive

Clearly if $\rho \in \mathrm{Pos}(A)$, $\sigma \in \mathrm{Pos}(\bar{A})$ then

$$(\mathcal{E} \otimes \mathcal{F})(\rho \otimes \sigma) \in \mathrm{Pos}(B \otimes \bar{B})$$

So $(\mathcal{E} \otimes \mathcal{F})(\mathrm{Sep}(A : \bar{A})) \subseteq S(B \otimes \bar{B})$

where $\mathrm{Sep}(A : \bar{A}) = \mathrm{conv}\left\{ \rho \otimes \sigma : \begin{array}{l} \rho \in S(A) \\ \sigma \in S(B) \end{array} \right\}$

separable states.

$(\mathcal{E} \otimes \mathcal{F})(\rho)$ can fail to be positive for $\rho \in S(A \otimes \bar{A}) \setminus \mathrm{Sep}(A : \bar{A})$

Typical example showing positivity is not stable:

$\mathcal{E}$: Transpose map

$\mathcal{F}$: identity map.

Complete positivity is stable under tensor product.

<u>Ex:</u> • $\mathcal{E} : L(A) \to L(A)$ 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.

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

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

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

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

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

$\{|a\rangle\}_a$ ONB of A
$\{|b\rangle\}_b$ ONB of B

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

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

Sum of CP is CP.

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

- Measurements.

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

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

Input: A 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:

$$\mathrm{Tr}\left(\sum_x |x\rangle\langle x| \otimes M_x T M_x^*\right) \overset{\downarrow\, \mathrm{Tr}(|x\rangle\langle x|) = 1.}{\underset{\uparrow\, \mathrm{Tr}(S\otimes T) = \mathrm{Tr}(S)\cdot\mathrm{Tr}(T).}{=}} \sum_x \mathrm{Tr}(M_x^* M_x T) \overset{\downarrow\, \sum_x M_x^* M_x = I.}{=} \mathrm{Tr}(T)$$

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.

Representation of a quantum channel

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

<u>The Choi operator:</u> 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

<u>Rk</u>: We often just write A instead of $\bar{A}$.

<u>Ex</u>: • $\mathcal{E} = I$ identity channel $(B\cong A)$

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

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

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

• $\mathcal{E}(S) = \mathrm{Tr}(S)\sigma$ (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 : $L(L(A), L(B)) \longrightarrow L(A\otimes B)$

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

and its inverse is

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

$$J \longmapsto \Big[\underbrace{S_A \longmapsto \mathrm{Tr}_A\big((S_A^T \otimes I_B)\, J\big)}_{\mathcal{F}.}\Big]$$

Check:

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

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

$$= \sum' |a\rangle\langle a'| \otimes \langle a|\, J\, |a'\rangle$$

$$= J.$$

$J^{\mathcal{E}}$ 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

$$\Updownarrow$$

$$J^{\mathcal{E}}_{AB} \geq 0$$

• $\mathcal{E}$ is trace-preserving $\Longleftrightarrow$ $J^{\mathcal{E}}_A = I_A$.

$\mathrm{Tr}_B(J^{\mathcal{E}}_{AB})$

Conseq: • Complete positivity can be checked efficiently.

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

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.

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

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

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

$$\mathcal{E}(S_A) = \sum_{\substack{x,a,a' \\ b,b'}}' \lambda_x \langle a|S_A^T|a'\rangle |b'\rangle\langle b|.\langle a',b'|\varphi_x\rangle\langle\varphi_x|a,b\rangle$$
$$= \sum_{\substack{x \\ a\,b\,a'\,b'}}' \sqrt{\lambda_x}\langle a'b'|\varphi_x\rangle|b'\rangle\langle a'|S_A|a\rangle\langle b|\ \langle\varphi_x|a,b\rangle\cdot\sqrt{\lambda_x}$$
$$= \sum_x' K_x S_A K_x^* \text{ where } K_x = \sum_{a'b'} \langle a'b'|\varphi_x\rangle |b'\rangle\langle a'| \sqrt{\lambda_x}$$

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

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

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: 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 $\underbrace{M^* M = I_A}_{\text{M is an isometry}}$

i.e. preserves norms

$\| M|\psi\rangle \| = \| |\psi\rangle \|$

Proof:

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

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

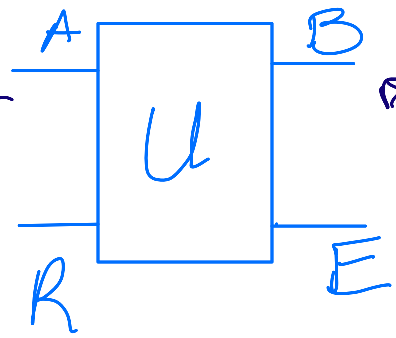
and $M = \sum_x K_x \otimes |x\rangle$

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)

A concept we will use: operator $\begin{matrix}\text{monotone}\\ \text{convex}\end{matrix}$ functions

$f: \underset{\text{interval } \subseteq \mathbb{R}}{I} \to \mathbb{R}$ **operator monotone** if for any $d \geq 1$

for any Hermitian operators $A, B \in \mathrm{Herm}(\mathbb{C}^d)$

with $\mathrm{spec}(A), \mathrm{spec}(B) \subseteq I$.

$$\underbrace{A \geq B}_{\text{means } A - B \in \mathrm{Pos}(\mathbb{C}^d)} \Rightarrow f(A) \geq f(B)$$

Rk: There exist functions that are monotone but not operator monotone e.g. $x \mapsto x^2$ (Ex: find example)

But $x \mapsto \log x$ & $x \mapsto \sqrt{x}$ are operator monotone.

$f: I \to \mathbb{R}$ **operator convex** if for any $d \geq 1$

for any Hermitian operators $A, B \in \mathrm{Herm}(\mathbb{C}^d)$

with $\mathrm{spec}(A), \mathrm{spec}(B) \subseteq I$.

$$f(\lambda A + (1-\lambda) B) \leq \lambda f(A) + (1-\lambda) f(B).$$

Rk: . Example of non-operator convex: $x \mapsto x^3$.

. Example operator convex: $-\log x$, $\frac{1}{x}$