**Quantum Information Theory.**

![Diagram](image)

**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 $\mathcal{H}$.

$u, v \in \mathcal{H}$ <inner product>

$\langle u, v \rangle$ <inner product>

$L \in \mathcal{L}(\mathcal{H})$ <inner product>

$\langle u, Lv \rangle = \langle L^*u, v \rangle$ <inner product>

$\langle L^*u, v \rangle = \overline{\langle u, Lv \rangle}$ <inner product>

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

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

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

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

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

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

Bra-ket notation:

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

defined by $\langle u \rangle : \mathbb{C} \to \mathcal{H}$ <inner product>

$\lambda \mapsto \lambda u$. <inner product>

The adjoint $\langle u \rangle^* \in \mathcal{L}(\mathcal{H}, \mathbb{C})$ is denoted $\langle u \rangle^*$ <inner product>
\[ \langle u \rangle : H \rightarrow C \]
\[ \sigma \mapsto \langle u, \sigma \rangle \]

We have \( \langle u \rangle : \sigma \rightarrow \langle u, \sigma \rangle \), \( \langle u \rangle \in \mathcal{L}(C, C) \) identified with \( C \).

\[ \langle u, v \rangle \rightarrow \] will denote inner product by \( \langle u, v \rangle \).

. \( \langle v \rangle u \in \mathcal{L}(H) \)
Ex: \( e_i \) is a basis of \( H \) then

\[ \mathbb{E} \quad \text{orthonormal} \]

then \( I = \sum_i \langle e_i, e_i \rangle \).

\[ \text{Rk: We will often use shorthand } \langle i \rangle \quad \text{for } \langle 1, e_i \rangle \quad \text{for } \langle 1 e_i \rangle \]

**Spectral decomposition**

. For any Hermitian \( S \in \mathcal{L}(H) \), then

exists an orthonormal basis of \( H \) \( \{ e_i \} \) s.t.

\[ S = \sum_i \delta_i \langle e_i, e_i \rangle \]

with \( \delta_i \in \mathbb{R} \).

. In other words \( S \) written in ONB \( \{ e_i \} \)

is diagonal \( S = \begin{pmatrix} \delta_1 & 0 \\ 0 & \ddots \end{pmatrix}_{\dim(H)} \)
• $S$ is positive iff $d_i \geq 0 \ \forall i$.

• For $f : \mathbb{R} \rightarrow \mathbb{C}$,
  \[ f(S) = \sum_i f(d_i) |x_i||x_i| \]

---

**Tensor products:**

- Multiple systems $A, B, C, \ldots$, $X, Y, \ldots$
- Hilbert space $H_A, H_B, H_C$
- Hilbert space for joint system: $H_A \otimes H_B$
  - Vector space spanned by $u \otimes v$
    - for $u \in H_A, v \in H_B$
  - Inner product: $\langle u \otimes v, u' \otimes v' \rangle = \langle u, u' \rangle \langle v, v' \rangle$
    - and linear extension

- For $SEL(H_A, H_A')$, $TEL(H_B, H_B)$ define $S \otimes T$:
  \[ (S \otimes T)(u \otimes v) = (Su) \otimes (Tv), \] and linear extension.
We identify: $L(H_A, H_A^\prime) \otimes L(H_B, H_B^\prime)$ and $L(H_A \otimes H_B, H_A^\prime \otimes H_B^\prime)$

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

---

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

- The set of density operators is denoted $S(H)$.
- $\rho$ is said to be pure if $\text{rank}(\rho) = 1$
- $\rho = 14 \times 14$ is said.
- $\rho = \frac{1}{\dim H} I$ is maximally mixed.

---

**Density operator formalism:**

- If a system is represented by a vector $|\psi\rangle$ (e.g., $|\alpha\rangle \otimes |\beta\rangle$)
  Then the density operator $\rho$ representing this system is given by $\rho = 14 \times 14$.
- e.g.: $\rho = \begin{pmatrix} |\alpha|^2 & |\beta|^2 \\ \overline{|\beta|^2} & |\alpha|^2 \end{pmatrix}$ in the basis $\{|\alpha\rangle, |\beta\rangle\}$.

**Composition:** State of a composite system is given by density operators on $H_A \otimes H_B$ if individual state spaces are $H_A$ and $H_B$. 

$= \text{span} \{ S \otimes T \}$
Prepare \( \rho_A \) on system \( A \) and independently \( \rho_B \) on \( B \): \( \rho_A \otimes \rho_B \).

**Notation:** \( H_A \rightarrow A \).

(For short we call the Hilbert space \( A \)).

**Evolution:** Isolated evolution of a subsystem \( A \) corresponds to a unitary on \( A \). For a state \( \rho_{AB} \) 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 \( \{ M_\alpha \}_{\alpha \in \mathcal{X}} \), for some set \( \mathcal{X} \), \( M_\alpha \in L(A) \) satisfying

\[
\sum_{\alpha \in \mathcal{X}} M_\alpha^* M_\alpha = I.
\]

Prob of outcome \( \alpha \): \( p(\alpha) = \text{Tr}(M_\alpha \otimes I_B \rho_{AB} M_\alpha^* \otimes I_B) \).

Check: \( \sum_\alpha p(\alpha) = \sum_\alpha \text{Tr}(M_\alpha^* M_\alpha \otimes I_B \rho_{AB}) = \text{Tr}(\rho_{AB}) = 1. \)

\( \text{Tr}(ST) = \text{Tr}(TS) \).

Post-measurement state conditioned on \( \alpha \):

\[
\rho_{AB,\alpha} = \frac{(M_\alpha \otimes I_B)\rho_{AB}(M_\alpha^* \otimes I_B)}{p(\alpha)}.
\]
• Special case: projective measurement

You might be used to special case

\[ M_\alpha = P_\alpha \quad \text{with} \quad P_\alpha \ \text{projector} \quad (i.e. \ P_\alpha^* = P_\alpha = P_\alpha^2) \]

coming from the spectral decomposition of observable \( O \)

\[ O = \sum_\alpha \lambda_\alpha P_\alpha \]

A general measurement can model, e.g., a unitary followed by a projective measurement: \( U \) followed by \( P \) \( x \in \mathbb{E} \)

\[ p(\alpha) = \text{Tr}_B \left( (P_\alpha U_A \otimes I_B) C_{AB} (U_A^* P_\alpha \otimes I_B) \right) \]

\[ = \text{Tr}_B \left( M_\alpha^* M_\alpha \otimes I_B C_{AB} \right) \]

\[ = \text{Tr}_B \left( M_\alpha^* M_\alpha \otimes I_B C_{AB} \right) \]

• Special case: POVM measurement.

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

\[ p(\alpha) = \text{Tr}_B \left( (P_\alpha \otimes I_B) C_{AB} (M_\alpha^* \otimes I_B) \right) \]

\[ = \text{Tr}_B \left( M_\alpha^* M_\alpha \otimes I_B C_{AB} \right) \]

We let \( E_\alpha = M_\alpha^* M_\alpha \). 

\( \uparrow \) only need to know \( E_\alpha \) to determine \( p(\alpha) \) and not \( M_\alpha \).
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 $x = \text{Tr}(E_x e)$.

Quantum channels

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

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

* Completely positive:

  For any Hilbert space $R$
  $E \in \text{Pos}(A \otimes R)$
  $(E \otimes I_R)(e) \in \text{Pos}(B \otimes R)$

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

* Trace-preserving:
  For $T \in L(A)$
  $\text{Tr}(E(T)) = \text{Tr}(T)$
Remark: Why complete positivity and not just positivity?

A positive map $E$: For any $p \in \text{Pos}(A)$, $E(p) \in \text{Pos}(B)$. It turns out that positivity of a map is not stable under tensor product i.e.

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

$$(E \otimes F)(S \otimes T) = E(S) \otimes F(T)$$

is not positive

Clearly if $p \in \text{Pos}(A)$, $q \in \text{Pos}(A)$ then

$$(E \otimes F)(p \otimes q) \in \text{Pos}(B \otimes B)$$

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

where $\text{Sep}(A : A) = \{ \text{mv} \mid p \otimes q : p \in \text{ES}(A), q \in \text{ES}(B) \}$

$$(E \otimes F)(p)$$ can fail to be positive for $p \in \text{ES}(A \otimes A) \setminus \text{Sep}(A : A)$

Typical example showing positivity is not stable:

$E$: Transpose map

$F$: Identity map.

Complete positivity is stable under tensor product.
**Example:** \( E : L(A) \to L(A) \) unitary \( U \) \( E(T) = U T U^* \) for any \( T \in L(A) \).

*Completely positive:*

\[
(E \otimes I_B)(T) = (U \otimes I_B)(U^* \otimes I_B) T (U^* \otimes I_B) \geq 0
\]

\[
\langle v, (U \otimes I_B)(U^* \otimes I_B) T (U^* \otimes I_B) v \rangle
= \langle (U^* \otimes I_B) v, (U^* \otimes I_B) T (U^* \otimes I_B) v \rangle \geq 0
\]

More generally, a map \( E(T) = S T S^* \) for all \( T \) is completely positive.

*Trace preserving: \( \text{Tr}_A(U T U^*) = \text{Tr}_A(U^* U T) = \text{Tr}(T) \).*

*Partial trace map.*

\( \rho_{A B} \in S(A \otimes B) \) state of a composite system. What is the state of system \( A \) in its own? Should be a valid quantum channel, corresponds to "forgetting" \( B \).

\( \text{Tr}_B : L(A \otimes B) \to L(A) \)

\[
T \mapsto \sum_b \langle I_A \otimes b | T (I_A \otimes 1_b) | I_A \otimes 1_b \rangle
\]

where \( |1_b \rangle \) forms a basis of \( B \).
Note that

\[ \text{Tr}_B = \frac{I_A \otimes \text{Tr}_{\text{id}_{\mathcal{D}(B) \rightarrow \mathcal{C}}}}{\text{Tr}_{\text{id}_{\mathcal{D}(A) \rightarrow \mathcal{C}}}} \]

\[ \text{Tr}_B (A \otimes B) = \text{Tr}_B (A) \] if \( B \in \mathcal{S}(B) \).

\( \text{Tr}_B \) plays the role of taking the marginal distribution of a joint distribution.

\[ (A \otimes B) \text{Tr}_B (A) = \sum_{a,b} P(a,b) \text{Tr}_B (A) \text{Tr}_B (B) \]

Then \( (A \otimes B) \text{Tr}_B (A) = \sum_{a,b} P(a,b) \text{Tr}_B (A) \text{Tr}_B (B) \)

Check: Complete positivity: \( \text{Tr} (I_A \otimes B) T (I_A \otimes B) \) is CP.

- Sum of CP is CP.
- Trace preserving: \( \sum_{b} \text{Tr} (I_A \otimes b) T (I_A \otimes b) = \sum_{b} \text{Tr} (I_A \otimes b) \text{Tr} (T) = \text{Tr} (T) \).

Measurements.

\[ \sum_{x \in \mathcal{X}} M_x M_x = I_A \]

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

Input: \( A \) \hspace{1cm} Output: \( X \otimes A \) \hspace{1cm} postmeasurement state.

\( \text{Fix} \) holds outcome dim \( X = |X| \).
\[ M : L(A) \rightarrow L(X \otimes A) \]
\[ T \mapsto \sum_x |x x x| \otimes M_x T M_x^* \]

\[ \text{operator on } X \quad \text{operator on } A. \]

Check: \( CP \):
\[ 1_{x x x} \otimes M_x T M_x^* = (1_{x x x} \otimes M_x) \quad T \quad (1_{x x x} \otimes M_x^*) \]
\[ L(A, x \otimes A) \quad \in L(X \otimes A, A) \]

\( \Rightarrow \) same argument.

\( \bullet \) Trac-preserving:
\[ \text{Tr}(1_{x x x}) = 1. \]
\[ \sum_x M_x^* M_x = I. \]
\[ \text{Tr}(\sum_x |x x x| \otimes M_x T M_x^*) = \sum_x \text{Tr}(M_x^* M_x T) = \text{Tr}(T) \]
\[ \text{Tr}(S \otimes T) = \text{Tr}(S) \cdot \text{Tr}(T). \]

Can check that this models the measurement.
\[ M(x_A) = \sum_x \text{Tr}(M_x^* A M_x^*) |x x x| \otimes \frac{M_x^* M_x}{\text{Tr}(M_x^* M_x)} \]

\( \text{prob of outcome } x \quad \text{post-measurement state conditioned on } x. \)

Rk: Such a state is called a classical-quantum state, i.e., of the form
\[ \rho_A = \sum_x P(x) |x x x| \otimes \rho_A^x \]
\[ \{ x A \} \text{ fixed basis, } \rho_A^x \text{ density operator.} \]
Representation of a quantum channel

3 ways of representing a quantum channel.

- Choi $\rightarrow$ one operator in $L(A \otimes B)$.
- Kraus $\rightarrow$ a list of operators in $L(A, B)$
- Stinespring $\rightarrow$ an operator in $L(A, B \otimes E)$
  \footnote{new space to be defined}

The Choi operator: Fix a basis of $A$, $\{a\}$, let $\bar{A} \equiv A$

$$J^E_{\bar{A}B} = \sum_{a,a'} |a x a\rangle_A \otimes E(|a x a\rangle) \in L(\bar{A} \otimes B)$$

$$= (I_A \otimes E)(\Phi)$$

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

Example: $E = I$ identity channel ($B \equiv A$)

$$J^E = \Phi = \sum_{a,a'} |a x a\rangle a'_{a'}$$

- $E = Tr$ ($B = C$)
  $$J^E = I_A$$

- $E(S) = Tr(S) \sigma$ (constant output)
  $$J^E = \sum_{a,a'} |a x a\rangle \otimes Tr(Tr(|a x a\rangle \sigma)) = I_A \otimes \sigma$$
Does \( J^E \) capture everything about \( E \)?

Choi-Jamiołkowski isomorphism: \( L(L(C_A), L(C_B)) \rightarrow L(A \otimes B) \)

\[ E \mapsto J^E \]

and its inverse is

\[ J \mapsto \left[ S_A \mapsto \text{Tr}_A \left( (S_A^T \otimes I_B) J \right) \right] \]

Check:

\[ \sum_{a, a'} |a a'| \otimes \mathcal{F}(|a a|) = \sum_{a, a'} |a a'| \otimes \text{Tr}_A \left( (|a a|)^T \otimes I \right) J \]

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

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

\[ = J. \]

\( J^E \) can be used to easily check if \( E \) is a valid quantum channel.

**Th:** \( E \in L(L(C_A), L(C_B)) \) is completely positive if

\[ \text{Tr}_B(J^E) \geq 0 \]

\[ \text{Tr}_B(J^E) \equiv 0 \]

\[ E \text{ is trace-preserving} \iff \text{Tr}_A(J^E) = I_A. \]

**Conseq:** Complete positivity can be checked efficiently for all \( (I_R \otimes \mathcal{E})(S) \geq 0 \) for \( \mathcal{E} \in \text{Pos}(R \otimes A) \).

Theorem says sufficient to take \( R = A \) and \( S \equiv \sum_{a, a'} |a a'| \).
Proof: \( \downarrow \) is obvious

\[ \sum_{\lambda} \left| \lambda \right| \text{eigen decomposition} \]

Write \( \mathcal{E}(S_A) = \sum_{\alpha} K_{\alpha} S_A K_{\alpha}^* \), directly CP.

\[
\mathcal{E}(S_A) = \sum_{\alpha, \beta} \langle a | S_A^T | b \rangle \langle b | S_A | a \rangle \langle a | \otimes \langle b | \text{eigen decomposition} \rangle
\]

Can write \( | \psi_\alpha \rangle = \sum_{\alpha, \beta} \langle \alpha | \psi_\beta \rangle | a \rangle \otimes | b \rangle \text{eigen decomposition} \]

So \( | \psi_\alpha \rangle = \sum_{\alpha, \beta} \langle \alpha' | \psi_\beta \rangle | a \rangle \otimes | b \rangle \text{eigen decomposition} \]

\[
\mathcal{E}(S_A) = \sum_{\alpha} \langle a | S_A^T | b \rangle \langle b | S_A | a \rangle \langle a | \otimes \langle b | \text{eigen decomposition} \rangle
\]

\[
= \sum_{\alpha} \sqrt{\langle a | S_A^T | b \rangle \langle b | S_A | a \rangle \langle a | \otimes \langle b | \text{eigen decomposition} \rangle}
\]

\[
= \sum_{\alpha} K_{\alpha} S_A K_{\alpha}^* \text{ where } K_{\alpha} = \sum_{\alpha'} \langle a | \psi_{\alpha'} \rangle | \beta \rangle \text{eigen decomposition} \]

\( \Rightarrow \) direct \( \Rightarrow \text{Tr}(\mathcal{E}(1_{x}1_{y})) = S_{ij} \)

\[
\text{Tr}(\mathcal{E}(1_{x}1_{y})) = \text{Tr}(\mathcal{E}(S_A^T \otimes I_B)) = \text{Tr}(S_A^T \otimes I_B) = \text{Tr}(S_A^T) \text{eigen decomposition} \]

\[
= \text{Tr}(S_A) \text{eigen decomposition} \]
Corollary: Any CP map $\map E : \mathcal{L}(A) \to \mathcal{L}(B)$ can be written as

$$
\map E(S_A) = \sum_{a=1}^r K_a S_A K_a^*
$$

where $K_a \in \mathcal{L}(A;B)$ are called Kraus operators

$\map E$ is trace-preserving iff $\sum_a K_a^* K_a = I_A$

Rk: Called operator-sum representation.

Proof: Let $\map E(S_A) = \sum_a K_a S_A K_a^*$

$\map E$ is trace-preserving iff $M^* M = I_A$

$M$ is an isometry, i.e., preserves norms $\|M \psi\| = \|\psi\|$, where $E = \text{span}\{ |a\> \}$.
\[ M = \sum_{i} K_{\alpha} \otimes |\omega_i\rangle \]

Then \[ MS_{A} M^{x} = \sum_{\alpha_{i} \alpha_i'} K_{\alpha} S_{A} K_{\alpha_{i}'} \otimes |\alpha \times \omega_i\rangle \]

**Interpretation:**

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

Input space of interest \( A \)

Output space of interest \( B \)

Fixed state \( |\beta\rangle \)

Environment \( \mathcal{R} \)

\[ U : |\psi\rangle_{A} \otimes |\beta\rangle_{R} \rightarrow |M\psi\rangle_{A} \] (check: such a unitary exists)
A concept we will use: operator monotone functions

\[ f: I \to R \text{ operator monotone if for any } d \geq 1 \]

for any Hermitian operators \( A, B \in \text{Herm}(C^d) \) with \( \text{spec}(A), \text{spec}(B) \leq I \).

\[ A \geq B \implies f(A) \geq f(B) \]

means \( A-B \in \text{Pos}(C^d) \)

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

But \( x \mapsto \log x \) & \( x \mapsto \frac{1}{x} \) are operator monotone.

\[ f: I \to R \text{ operator convex if for any } d \geq 1 \]

for any Hermitian operators \( A, B \in \text{Herm}(C^d) \) with \( \text{spec}(A), \text{spec}(B) \leq I \).

\[ f(dA + (1-d)B) \leq df(A) + (1-d)f(B). \]

**Rk:** Example of non-operator convex: \( x \mapsto x^3 \).

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