PH 534: Quantum Information and Computing
TSC

Siddhant Midha
https://siddhantmidha.com/

March 27, 2025

The postulates

- Associated to any isolated physical system is a complex vector space equipped with an inner product, known as the *state space* of the system. The state of the system is completely described by its *state vector*, which is a normalized vector in the state space.
- The evolution of a **closed** quantum system is described by a unitary transformation.That is,

$$|\psi(t_1)\rangle = U(t_1, t_2)|\psi(t_2)\rangle$$

The evolution postulate can also be written as the Schrodinger equation $i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r}, t) = \hat{H}\Psi(\mathbf{r}, t)$. This can be transformed back using $U(t_1, t_2) = exp(\frac{-iH(t_1 - t_2)}{\hbar})$. The above expression assumes a time independent hamiltonian

The postulates – Quantum Measurements

- Quantum measurements are described by a set of measurement operators M_m which act on the state space of the system under consideration. The index m refers to the measurement outcome. The probability of measuring the outcome m given the current state is $|\psi\rangle$ is

  $$p(m) = \langle\psi|M_m^* M_m|\psi\rangle$$

  and after measuring m the state collapses to

  $$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^* M_m|\psi\rangle}}$$

  The measurement operators satisfy the completeness relation

  $$\sum_m M_m^* M_m = I$$

The postulates – Composite Systems

- The state space of the composite system is mathematically described by the tensor product operation. If we have systems 1, 2, 3 ... with hilbert spaces $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$ ... and states $|\psi_1\rangle, |\psi_2\rangle, \ldots |\psi_n\rangle$, then

$$\mathcal{H}_{1,2,\ldots n} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \mathcal{H}_n$$

  With the state of the composite system

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots |\psi_n\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \mathcal{H}_n$$

Notations

- States: $|\psi\rangle$
- $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$
- Density operators: $\rho, \sigma ...$
- Hilbert Space: $\mathcal{H}$
- Set of linear operators from $\mathcal{H}_1$ to $\mathcal{H}_2$: $L(\mathcal{H}_1, \mathcal{H}_2)$
- Set of density matrices on $\mathcal{H}$: $D(\mathcal{H}) \subset L(\mathcal{H})$
- Set of linear operators from $L(\mathcal{H}_1)$ to $L(\mathcal{H}_2)$: $T(\mathcal{H}_1, \mathcal{H}_2)$
- Set of quantum channels from $L(\mathcal{H}_1)$ to $L(\mathcal{H}_2)$: $C(\mathcal{H}_1, \mathcal{H}_2) \subset T(\mathcal{H}_1, \mathcal{H}_2)$

Density Operators

- If a system exists in the states $|\psi_i\rangle$ with probabilities p_i, then its density operator ρ is defined as

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$$

- The density operator is positive and has unit trace. The converse holds.
- Unitary evolution

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \rightarrow \sum_i p_i U |\psi_i\rangle \langle\psi_i| U^* = U\rho U^*$$

- Measurements

$$p(m) = Tr(M_m^* M_m \rho)$$

$$\rho_m = \frac{M_m \rho M_m^*}{Tr(M_m^* M_m \rho)}$$

Analyzing subsystems

If we have systems A and B, described by the density operator $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$, we define the density operator for the subsystem A as

$$\rho_A \equiv Tr_B(\rho_{AB}) \in D(\mathcal{H}_A)$$

with the partial trace operation Tr_B being defined as

$$Tr_B(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|) \equiv |a_1\rangle \langle a_2| \, tr(|b_1\rangle \langle b_2|))$$

and for general states ρ_{AB} the definition extends by superposition. Or,

$$Tr_B(\rho_{AB}) := \sum_j (I_A \otimes \langle j|_B)\rho_{AB}(I_A \otimes |j\rangle_B)$$

Schmidt Decomposition

Theorem 2.7 of QCQI

Let $|\psi\rangle \in \mathcal{H}_{AB}$. Then there exist orthonormal states $|i_A\rangle \in \mathcal{H}_A$ and orthonormal states $|i_B\rangle \in \mathcal{H}_B$ such that

$$|\psi\rangle = \sum_i \lambda_i \, |i_A\rangle \otimes |i_B\rangle$$

where $\lambda_i \geq 0$ and $\sum_i \lambda_i^2 = 1$.

Question Consider the state, $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$. Find its Schmidt Decomposition. How do you do this? SVD?

Purification

- Suppose
$$\rho_A = \sum_i p_i |i_A\rangle \langle i_A|$$
- Introduce R with $\mathcal{H}_R = \mathcal{H}_A$ (can we do better?) and a orthonormal basis $|i_R\rangle$.
- Define
$$|\psi_{AR}\rangle \equiv \sum_i \sqrt{p_i} |i_A\rangle |i_R\rangle$$
- See that
$$\rho_A = Tr_R(|\psi_{AR}\rangle \langle \psi_{AR}|)$$

Question Compute the purification for the state

$$\rho = \frac{1}{2}(|0\rangle \langle 0| + |+\rangle \langle +|)$$

Projective Measurements

Given a hermitian observable M, let its spectral decomposition be

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace with eigenvalue m. Upon measuring this observible with the state $|\psi\rangle$, the state collapses into a projection onto one of the eigenspaces, with probability

$$p(m) = \langle\psi|P_m|\psi\rangle$$

with the collapsed state being

$$|\psi|m\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}$$

It is easy to see that

$$\mathbb{E}[M] = \langle\psi|M|\psi\rangle$$

The notion of 'measuring in a basis' $|i\rangle$ can be viewed as a projective measurement with $P_i = |i\rangle \langle i|$.

Differences between General Measurements and Projective Measurements

- Both general measurements and projective measurements satisfy the completeness relation i.e. $\sum_m M_m^* M_m = I$.
- In addition to general measurements, projective measurements also satisfy the additional constraints-
  1. P_m are hermitian.
  2. $P_m P_{m'} = \delta(m, m')\ M_m$

  These two conditions just mean that P_m are orthogonal projectors.

Projective Measurement $\rightarrow$ General Measurements!

- The projective measurements rule together with the postulate on unitary time evolution is sufficient to derive the postulate on general measurements using the composite systems postulate.
- Suppose we have a quantum system with state space Q with measurement operators M_m. Now we introduce an *ancilla system* with the state space M with an orthonormal basis $|m\rangle$.
- Let $|0\rangle$ be a fixed state in M. Define operator U on the products $|\psi\rangle|0\rangle$ with $|\psi\rangle$ from state space Q and $|0\rangle$ as the fixed state in M as

$$U|\psi\rangle|0\rangle = \sum_m M_m|\psi\rangle|m\rangle$$

- $\langle\phi|\langle 0|U^*U|\psi\rangle|0\rangle = \sum_{m,m'}\langle\phi|M_m^*M_{m'}|\psi\rangle\langle m|m'\rangle = \sum_m \langle\phi|M_m^*M_m|\psi\rangle$ (Using orthonormality of m) $= \langle\phi|\psi\rangle$ (Using completeness of M_m)

Projective Measurement $\rightarrow$ General Measurements!

- We saw above that the operator U preserves inner products between states of the form $|\psi\rangle|0\rangle$. As $|0\rangle$ was an arbitrary state in M, we can extend the definition of U to a unitary operator on space $Q \otimes M$ generalised from $Q \otimes |0\rangle$.
- We now perform projective measurements on the two systems describes by projectors $P_m = I_Q \otimes |m\rangle\langle m|$.
- This set of projective measurements give us the probability and the final state of the system in accordance to the measurement postulate.

Projective Measurement $\rightarrow$ General Measurements!

- The probabilities are calculated as follows

$$p(m) = \langle \phi | \langle 0 | U^* P_m U | \phi \rangle | 0 \rangle = \langle \phi | M_m^* M_m | \phi \rangle$$

- The joint state of the system QM, given that result m occurs is

$$\frac{P_m U | \psi \rangle | 0 \rangle}{\sqrt{\langle \psi | U^* P_m U | \psi \rangle}} = \frac{M_m | \psi \rangle | m \rangle}{\sqrt{\langle \psi | M_m^* M_m | \psi \rangle}}$$

- As the state of the system M after measurement is given by $|m\rangle$, it follows that the final state of the system Q after measurement is given by $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^* M_m|\psi\rangle}}$

Conclusion – Thus unitary dynamics and projective measurements alongwith the ability to introduce ancilla systems enables us to implement general measurements, as described in postulate three.

POVMs

- Convenient formalism of measurement.
- Useful when we care about only the measurement statistics and not the output states.
- Formally, any set of operators E_m form a POVM if
  1. Each E_m is positive.
  2. $\sum_m E_m = I$
- We have the probabilities

$$p(m) = \langle \psi | E_m | \psi \rangle$$

- Can go from a measurement set M_m to a POVM E_m by defining $E_m \equiv M_m^* M_m$

A use of POVMs

- Consider the states $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Distinguishing between these states is impossible. However, it is possible to distinguish the states by measurement for some of the time such that if an identification is made, it is always correct.
- Let the POVM $= \{E_1, E_2, E_3\}$ contain three operators

$$E_1 = \frac{\sqrt{2}}{\sqrt{2}+1} |1\rangle \langle 1|$$

$$E_2 = \frac{\sqrt{2}}{\sqrt{2}+1} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}$$

$$E_3 = I - E_1 - E_2$$

- Notice that $\langle\psi_1| E_1 |\psi_1\rangle = 0$ and $\langle\psi_2| E_2 |\psi_2\rangle = 0$. So after the POVM measurement, if we get E_1 as a result, then we can conclude that $|\psi_1\rangle$ is not the state, and $|\psi_2\rangle$ must have been the state. The same logic can be applied to the pair E_2 and $|\psi_2\rangle$. However, if we observe E_3 we cannot comment anything on the state.

Quantum Operations: Beyond Unitaries

- Natural Extension of unitary operations (Church of Larger Hilbert Space):

$$\mathcal{E}(\rho) = Tr_{env}(U(\rho \otimes \rho_{env})U^*)$$

- Discard the environment: need some axioms.
  1. $Tr[\mathcal{E}(\rho)] \in [0,1] \forall \rho$ ($Tr[\mathcal{E}(\rho)]$ is the probability that ρ undergoes the transformation $\mathcal{E}$).
  2. Convex linearity

     $$\mathcal{E}(\sum_i p_i \rho_i) = \sum_i p_i \mathcal{E}(\rho_i)$$

     for all density matrices ρ_i and probabilities p_i s.t. $\sum_i p_i = 1$
  3. $\mathcal{E}$ is completely positive. Not only does $\mathcal{E}$ preserve positivity, $(I \otimes \mathcal{E})$ also preserves positivity for I being the identity on an aribtrarily dimensional system's hilbert space.

Formally,

$$\mathcal{E} : L(\mathcal{H}_1) \rightarrow L(\mathcal{H}_2) \in C(\mathcal{H}_1, \mathcal{H}_2)$$

The operator sum representation

Theorem 8.1 of QCQI

The map $\mathcal{E}$ satisfies the axioms for a valid quantum operation iff there exists a set of operators $\{E_i\}$ such that

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^*$$

for all valid density matrices ρ and $0 \preccurlyeq \sum_i E_i^* E_i \preccurlyeq I$

Note: $A \preccurlyeq B$ if $B - A$ is PSD. So if we are just dealing with CPTP maps, then these E_i satisfy $\sum_i E_i^* E_i = I$, and are called the *kraus operators.*

Quantum computers in a classical world

- The challenge in designing substrates for QIC lies around the fact that quantum systems *decohere*.
- This decoherence cannot be reversed easily. Not unitary!
- A more general transformation.
- For example, *dephasing*:

$$\rho \mapsto (1-p)\rho + pZ\rho Z \tag{1}$$

- Question: What are the Kraus operators for this channel?

Some maffs

1. **The Vectorization Map**: vec : $L(\mathcal{H}_2, \mathcal{H}_1) \to \mathcal{H}_1 \otimes \mathcal{H}_2$, defined as

$$|vec(|a_1\rangle\langle b_2|)\rangle := |a_1\rangle \otimes |b_2\rangle$$

   Thus, the vec map takes operators in $L(\mathcal{H})$ to vectors in $\mathcal{H} \otimes \mathcal{H}$.

2. **The Choi Representation** $\mathcal{J} : T(\mathcal{H}_1, \mathcal{H}_2) \to L(\mathcal{H}_2 \otimes \mathcal{H}_1)$

$$J(\mathcal{E}) := (\mathcal{E} \otimes \mathbb{1}_{L(\mathcal{H}_1)})(|\mathrm{vec}(\mathbb{1}_{\mathcal{H}_1})\rangle\langle \mathrm{vec}(\mathbb{1}_{\mathcal{H}_1})|)$$

   Note that $|\mathrm{vec}(\mathbb{1}_{\mathcal{H}_1})\rangle$ is a vector in $\mathcal{H}_1 \otimes \mathcal{H}_1$, and thus $(|\mathrm{vec}(\mathbb{1}_{\mathcal{H}_1})\rangle\langle \mathrm{vec}(\mathbb{1}_{\mathcal{H}_1})|)$ is a operator on $\mathcal{H}_1 \otimes \mathcal{H}_1$. Now, we know that $\mathcal{E}$ takes operators from $L(\mathcal{H}_1)$ to $L(\mathcal{H}_2)$, and $\mathbb{1}_{L(\mathcal{H}_1)}$ takes operators from $L(\mathcal{H}_1)$ to $L(\mathcal{H}_1)$. Thus, $J(\mathcal{E})$ lies in $L(\mathcal{H}_2 \otimes \mathcal{H}_1)$.
   If $\mathcal{H}_1 = \mathcal{H}_2$,

$$J(\mathcal{E}) = \sum_{i,j} \mathcal{E}(|i\rangle\langle j|) \otimes |i\rangle\langle j|$$

Some maffs

The Choi Theorem

If $\mathcal{E} : \mathcal{H} \to \mathcal{H}$ is a quantum channel with kraus operators $\{A_i\}$, then,

$$\mathcal{J}(\mathcal{E}) = \sum_i |\text{vec}(A_i)\rangle \langle \text{vec}(A_i)|$$

Questions

1. Compute the Choi operator, $\mathcal{J}(\mathcal{E})$ for the channel with the following action:

$$\rho \mapsto (1-p)\rho + \frac{p}{3} Z\rho Z + + \frac{p}{3} Y\rho Y + + \frac{p}{3} X\rho X$$

2. Suppose,

$$\mathcal{J}(\mathcal{E}) = \frac{2}{3} |\phi^-\rangle \langle \phi^-| + \frac{4}{3} |\psi^+\rangle \langle \psi^+|$$

Calculate the Kraus operators for $\mathcal{E}$.

Distinguishing quantum states

- Setting: Alice chooses the ensemble $\{p_i, \rho_i\}$ of length n, samples a state from it and sends to Bob.
- Bob can conduct a $n-$port measurement, and wants to determine which state was sent.
- Strategy: Develop a measurement apparatus $\{M_i\}$ s.t. if outcome is at port i, decode ρ_i.
- Formally,

$$\max_{\{M_i\}} \sum_i p_i \mathrm{Tr}(M_i \rho_i) \text{ with } M_i \geq 0, \ \sum_i M_i = 1 \qquad (2)$$

- What is the quantity in red?

Distinguishing states: the two state case

- $p_1 = p, p_2 = 1 - p$.
- Let $\rho := p\rho_1 + (1-p)\rho_2$, and $X := p\rho_1 - (1-p)\rho_2$
- Then, $p_{success} = \frac{1}{2}\left[1 + Tr((M_1 - M_2)X)\right] \underbrace{\leq \frac{1}{2}\left[1 + ||X||_1\right]}_{\text{Holevo-Helstrom Bound}}$
- Decompose

$$X = Q - R \text{ (Spectral, Hahn-Jordan) w}/Q, R \geq 0 \qquad (3)$$

  and let $M_1 = Q$.
- *Check*, that $Tr((M_1 - M_2)X) = ||X||_1$.
- Now have the optimal measurement set.

Shannon Entropies

- Distribution $p(x)$. R.V. $X \sim p(x)$. Define,

$$H(X) = H(p) := -\sum_{x \in \mathcal{X}} p(x) \log_2(p(x)) = -\mathbb{E}_{x \sim p(x)}(\log(p(x))) \tag{4}$$

- All sorts of cousins exist.
  1. Joint entropy for $X, Y \sim p(x, y)$

$$H(X, Y) = -\mathbb{E}_{x,y \sim p(x,y)}(\log(p(x, y))) \tag{5}$$

  2. Conditional entropy

$$H(X|Y) = \mathbb{E}_{y \sim p(y)}[H(X|Y = y)] \tag{6}$$

  3. **Chain rule**

$$H(X, Y) = H(X) + H(Y|X) \tag{7}$$
$$H(X, Y|Z) = H(X|Z) + H(Y|X, Z) \tag{8}$$

Shannon Entropies

- Relative entropy

$$D(p||q) := \sum_{x \in \mathcal{X}} p(x) \log_2 \frac{p(x)}{q(x)} \geq 0 \tag{9}$$

Not symmetric. But, $D(p||q) = 0 \Leftrightarrow p = q$.

- **Mutual information**

$$I(X:Y) := D(p_{XY}(x,y)||p_X(x)p_Y(y)) \geq 0 \tag{10}$$

Symmetric.

- Mutual information with entropies

$$I(X:Y) = H(X) - H(X:Y) \tag{11}$$

$$I(X:Y) = H(X) + H(Y) - H(X,Y) \tag{12}$$

- Exercise: Chain rule for relative entropy

$$D(p(x,y)||q(x,y)) = D(p(x)||q(x)) + D(p(y|x)||q(y|x)) \tag{13}$$

Shannon and the entropies: Quantumania

- Von-Neumann entropy

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho) \tag{14}$$

  Use? Entanglement? How?

- See that if $\rho = \sum_i p_i |i\rangle \langle i|$ (spectral), then

$$S(\rho) = H(\mathbf{p}) \tag{15}$$

- Conditional quantum entropy

$$S(A|B) = S(A,B) - S(B) \tag{16}$$

  Can be negative! Why? Can it be negative classically?

Shannon and the entropies: Quantumania

- Exercise: Additivity

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma) \tag{17}$$

- Exercise: Consider a classical quantum state

$$\rho_{XB} = \sum_{x \in \mathcal{X}} p_X(x) \left| x \right\rangle \left\langle x \right| \otimes \rho_B^x \tag{18}$$

  What is the entropy of this state? Answer,

$$S(XB) = S(\mathbf{p}(X)) + \sum_{x \in \mathcal{X}} p_X(x) S(\rho_B^x) \tag{19}$$

- **Fact**. For bipartite pure states $|\psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$, the VN entropy of a bipartition is a measure of entanglement in the state ψ.
  1. Does it matter which bipartition I choose?
  2. Compute the EE for
     - $\psi = (|00\rangle + |11\rangle)/\sqrt{2}$
     - $\psi = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2$

Quantum entropies: more

- Quantum relative entropy

$$S(\rho||\sigma) = Tr(\rho \log \rho - \rho \log \sigma) \geq 0 \tag{20}$$

- Subadditivity

$$S(A, B) \leq S(A) + S(B) \tag{21}$$

  with equality if?Proof?

- Strong subadditivity

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C) \tag{22}$$