Introduction to Quantum Information

Siddhant Midha and Aaryan Gupta

Last updated on June 17, 2022

Table of Contents

Linear Algebra-Pauli Matrices

We will be using these matrices quite frequently.

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Linear Algebra-Operator Functions

- A function f from the set of complex numbers to the set of complex numbers can be generalised to normal operators.
- After a spectral decomposition, we just apply the function to its diagonal values.
- Note that this could not be done for any general matrix because the functions wouldnt be functions.
- Let A be a matrix which has the spectral decomposition

$$A = \sum_i \lambda_i \left| i \right\rangle \left\langle i \right|$$

Then $f(A)$ will be defined as

$$f(A) = \sum_i f(\lambda_i) \left| i \right\rangle \left\langle i \right|$$

The Spectral Decomposition

Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V. Conversely, any diagionalizable operator is normal.

Polar Decomposition

Let A be a linear operator on a vector space V. Then there exists unitary U and positive operators J, K such that

$$A = UJ = KU$$

where, $J = \sqrt{A^\dagger A}, K = \sqrt{AA^\dagger}$.Further, if A is invertible then U is unique.

Linear ALgebra- Decompositions

Polar Decomposition

Let A be a linear operator on a vector space V. there exists unitary U and positive operators J, K such that

$$A = UJ = KU$$

where, $J = \sqrt{A^\dagger A}, K = \sqrt{AA^\dagger}$. Further, if A is invertible then U is unique.

Singular Value Decomposition

Let A be a square matrix.Then there exist unitaries U, V and a diagonal matrix D with non-negative entries such that

$$A = UDV$$

Linear ALgebra- Commutator and Anti-Commutator

- The commutator between two operators is defined as $[A, B] = AB - BA$
- The anticommutator between two operators is defined as $A, B = AB + BA$

Simultaneous Diagonalization

Let A, B be hermitian operators on a vector space V. , $[A, B] = 0 \Leftrightarrow$ there exists an orthonormal basis for V which can diagonalize both A and B

Table of Contents

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

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

Linear Algebra-Tensor Products

- The tensor product is a way of combining two vector spaces to form larger vector spaces
- Suppose V, W are vector spaces of dimension m, n respectively. Then $V \otimes W$ is a vector space of dimension mn.
- Tensor products are distributive and linear over the input.
- Suppose A is a m by n matrix and B is a p by q matrix, then the tensor product can be represented in Kronecker product form as-

$$A \otimes B \equiv \left.\overbrace{\begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}}^{nq}\right\} mp \,.$$

Table of Contents

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 → 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

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

- $\langle\phi|\,\langle 0|\,U^* U\,|\psi\rangle\,|0\rangle = \sum_{m,m'} \langle\phi|\,M_m^* M_m\,|\psi\rangle \left\langle m \middle| m' \right\rangle = \sum_m \langle\phi|\,M_m^* M_m\,|\psi\rangle$ (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 → 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 $E_m \equiv M_m^* M_m$

Some Points

- A physical intuition: Projective measurements are repeatable, many real world measurements may not be.
- General measurement formalism provides more control over the measurement scheme which is useful in QCQI (example?)
- POVMs are a mathematical convenience, a restriction to the general measurement formalism in which we don't care about the post measurement state, only the measurement statistics.

Distinguishing Quantum States

- Let us consider a game between two players Alice and Bob where Alice chooses a state $|\psi_i\rangle$ for $i = 1 \ldots n$ and Bobs has to guess which state Alice gave him.
- If the states are orthonormal, Bob can do quantum measurement to win the game in the following way-
  1. Define measurement operators $M_i = |\psi_i\rangle \langle\psi_i|$ for each i and define M_0 as the positive square root of the positive operator $I - \sum_{i \neq 0} |\psi_i\rangle \langle\psi_i|$
  2. The measurement operators satisfy the completeness relation and if state i occurs then $p_i = \langle\psi_i| M_i |\psi_i\rangle = 1$ and Bob wins the game.
- If the states are not orthonormal, no quantum measurement is capable of distinguishing them.
- This is intuitively explained as follows: A state $|\psi_2\rangle$ can be decomposed to a component parallel to another state $|\psi_1\rangle$ and a component perpendicular to it. Suppose Bob guesses state $|\psi_1\rangle$ when he observes outcome j. But since $|\psi_2\rangle$ has a non-zero component parallel to $|\psi_1\rangle$, there is a probability that j is observes when $|\psi_2\rangle$ is prepared. Hence, Bob might guess wrong.

Proof

- Here we try to formally prove the fact that if the states are not orthonormal, no quantum measurement is capable of distinguishing them.
- If Bob observes outcome j, he guesses the state i the system is in using the rule $i = f(j)$.
- We proceed by a proof by contradiction. Suppose such a measurement is possible. Then if the state $|\psi_1\rangle$ is prepared, the probability of measuring outcome j such that $f(j) = 1$ is 1.
- Define $E_i = \sum_{j:f(j)=i} M_j^* M_j$. Then we have $\langle\psi_1| E_1 |\psi_1\rangle = 1$ and similarly $\langle\psi_2| E_2 |\psi_2\rangle = 1$ as the observations. Since $\sum_i E_i = I$, it follows that $\sum_i \langle\psi_1| E_i |\psi_1\rangle = 1$. These imply that $\sqrt{E_2}\,|\psi_1\rangle = 0$.
- Decompose $|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,|\psi\rangle$ where $|\psi\rangle$ is orthogonal to $|\psi_1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, and $|\beta| < 1$. Then $\sqrt{E_2}\,|\psi_2\rangle = \beta\sqrt{E_2}\,|\psi\rangle$ which implies $\langle\psi_2| E_2 |\psi_2\rangle = |\beta|^2 \langle\psi| E_2 |\psi\rangle \leq |\beta|^2 < 1$. This implies contradiction.

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.

Table of Contents

Density Operators

- What if the system in consideration interacts with the environment?
- Can describe their combined behaviour by a $|\psi\rangle$.
- May not be able to describe the behaviour of the system with a pure state.
- Density operators.
- Encoding some classical uncertainity within the already present quantum uncertainity.

Density Operators

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

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

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

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \to \sum_i p_i U \left|\psi_i\right\rangle \left\langle\psi_i\right| U^* = U\rho U^*$$

- Measurements

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

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

Some more points

- We can even have a mixture of density operators $\{\rho_i, p_i\}$, such that $\rho = \sum_i p_i \rho_i$ describes the state of the system. Can be viewed as $\sum_{ij} q_{ij} \left|\psi_{ij}\right\rangle \left\langle\psi_{ij}\right|$. A simple example is the action of $\mathcal{M} = \{M_m\}$ on ρ without knowing the outcome.
- The postulates can be reformed in the density operator language.
- A ρ is pure iff $tr(\rho^2) = 1$.
- Set of density ops is convex, and the pure states occupy the boundary of this set. Intuitive example: two qubits.

Formation of density operators

Freedom in generation of the density operator.

Theorem 2.6 of QCQI

The vectors $\left|\tilde{\phi}_i\right\rangle$ and $\left|\tilde{\psi}_j\right\rangle$ generate the same density matrix (i.e., $\sum_i \left|\tilde{\phi}_i\right\rangle\left\langle\tilde{\phi}_i\right| = \sum_j \left|\tilde{\psi}_j\right\rangle\left\langle\tilde{\psi}_j\right|$) iff

$$\left|\tilde{\phi}_i\right\rangle = \sum_j u_{ij}\left|\tilde{\psi}_j\right\rangle$$

where $U = [u_{ij}]$ is a unitary matrices.

Note In the above theorem, we absorbed the probabilities into the vectors as $\left|\tilde{\psi}\right\rangle \equiv \sqrt{p}\,|\psi\rangle$.

Analyzing subsystems

If we have systems A and B, described by the density operator ρ_{AB}, we define the density operator for the subsystem A as

$$\rho_A \equiv Tr_B(\rho_{AB})$$

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,

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

Digression - Von Neumann Entropy

- Shannon entropy, for the distribution $p \equiv \{p_i\}$ is given as

$$H(p) := -\sum_i p_i \log p_i$$

- Quantifies the disorder in the distribution. Maximum for a uniform distribution. Zero if the p is perfectly predictable.
- Can we quantify the disorder in a state ρ?
- Von-Neumann entropy

$$S(\rho) := -Tr(\rho \log \rho)$$

- If $\rho = \sum_i \lambda_i |i\rangle \langle i|$ (spectral decomp) then

$$S(\rho) \equiv H(\{\lambda_i\})$$

- $S(\rho)$ is zero for pure states. Maximum for states of the form $I_D/dim(D)$ (called the maximally mixed states).

A nice example

Consider

$$|\psi\rangle_{AB} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Thus, $\rho_{AB} = |\psi\rangle_{AB} \langle\psi|_{AB}$. Now, we can compute $\rho_A = Tr_B(\rho_{AB})$.
(compute)

(comment on $S(\cdot)$)

Why the partial trace?

- The unique operation that preserves observable statistics.
- Let $M = \sum_m mP_m$ be an observable on the system A
- Let M' be the corresponding observable on the system AB. Thus, any state $|m\rangle_A |\psi\rangle_B$ of AB should have $p(m) = 1$.
- Thus, the corresponding projector for measuring m on AB is $P_m \otimes I_B$ and thus

$$M' = \sum_m mP_m \otimes I_B = M \otimes I_B$$

Why the partial trace?

- Now, we want a map $f(\cdot)$ such that $f(\rho_{AB})$ gives us the density operator describing the state of A.
- We need

$$tr(Mf(\rho_{AB})) = tr((M \otimes I_B)\rho_{AB}) \text{ –}(\#)$$

- Let M_i be an orthonormal basis of the space of hermitian operators w.r.t. the inner product $(A, B) \equiv Tr(AB)$. Expand $f(\rho_{AB})$ as

$$f(\rho_{AB}) = \sum_i M_i tr(M_i f(\rho_{AB})) = \sum_i M_i tr((M \otimes I_B)\rho_{AB})$$

- Thus such an f is unique.
- Now see that $f = tr_B$ satisfies $(\#)$.

Schmidt Decomposition

This is a very useful theorem in quantum information.

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 $\sum_i \lambda_i^2 = 1$.

Purification

- Suppose we are given the state ρ_A for the system A.
- With the help of the previous theorem, we come up with an auxilliary system R, such that the combined state of these two systems is a pure state.
- Purification.
- Suppose

$$\rho_A = \sum_i p_i \left| i_A \right\rangle \left\langle i_A \right|$$

- Introduce R with $\mathcal{H}_R = \mathcal{H}_A$ and a orthonormal basis $\left| i_R \right\rangle$.
- Define

$$\left| \psi_{AR} \right\rangle \equiv \sum_i \sqrt{p_i} \left| i_A \right\rangle \left| i_R \right\rangle$$

- See that

$$\rho_A = Tr_R(\left| \psi_{AR} \right\rangle \left\langle \psi_{AR} \right|)$$

Table of Contents

Some classical intuition

- A register X with the alphabet Σ may be in a probabilistic state p.
- Some noise causes the state to change to q. We can use the law of total probability

$$q(a) = \sum_{b \in \Sigma} \mathbb{P}(X' = a | X = b)\mathbb{P}(X = b) \ \forall a \in \Sigma$$

- Thus we have

$$q = Ep$$

  for some matrix E *such that*

  1. Positivity is held: all entries of E are non negative.
  2. Completeness is fulfilled $\sum_{a \in \Sigma} \mathbb{P}(X' = a | X = b) = 1$ (columns sum to one).

Quantum Operations

- We know that systems may not be represented by a pure quantum states.
- Introduced density operator formalism.
- Now how does a system in the state ρ evolve?
- It might not be a closed system.
- Close the system by including the environment. Thus the net state is $\rho \otimes \rho_{env}$.
- The postulate now follows, so we have the new state $\mathcal{E}(\rho)$ of the system as

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

- Issue! Why must the combined state be a product one?
- Observation Input and output spaces needn't be the same.

Don't want the environment

- Goal: describe general quantum operations on open systems without accounting for the environment.
- Question arises: What kind of a map must $\mathcal{E}$ be so that it represents a valid quantum operation?
- 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.

Example

For a single qubit state ρ, a measurement in the computational basis can be described by the operations $\mathcal{E}_0(\rho) \equiv |0\rangle\langle 0|\rho|0\rangle\langle 0|$ and $\mathcal{E}_1(\rho) \equiv |1\rangle\langle 1|\rho|1\rangle\langle 1|$ with probabilities given as $tr[\mathcal{E}_0(\rho)]$ and $tr[\mathcal{E}_1(\rho)]$. The final state is

$$\frac{\mathcal{E}_i(\rho)}{Tr([\mathcal{E}_i(\rho)])} \text{for some } i \in \{0, 1\}$$

That is, if no measurement is happening, the map $\mathcal{E}$ would be a *completely positive trace preserving (CPTP)* map.

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.*

Concluding Points

- Kraus operators are not unique. Unitary equivalence exists as in the case of ensembles.
- Physical motivation for kraus ops: Unitary evolution on joint state, and then measurement[1] of the environment in some basis.
- Non trace preserving maps are those which have unitary evolution of the sys+env followed by projective measurement of the two. Thus trace of $\mathcal{E}_m(\rho)$ represents the probability that E_m took place out of all possible m.[2].
- Given an opsum representation, we can cook up an environment s.t. unitary evolution (plus possibly projective measurement) followed by tracing out environment describes the map.
- For a d dimensional system, a general CPTP map can be represented by atmost d^2 kraus operators.[3]

[1] *without knowing the outcome*

[2] that is, a single non trace preserving map $\mathcal{E}$ does NOT describe the dynamics fully, you need the set $\{\mathcal{E}_m\}$

[3] not in QCQI, elsewhere.