Lecture 10. Quantum information basics

Xiao Yuan

November 11, 2021

The original framework of quantum theory consists of pure states, unitary evolution, and projective measurements. Here we extend the framework to density matrices, quantum channels, and positive observable valued measure (POVM).

1 Density matrix

1.1 From pure states to density matrices

There are at least two clear motivations that we need to generalize pure states to density matrices.

First, imagine we have a source that randomly prepares a pure state $|\psi_j\rangle$ with probability $p_j \geq 0$ satisfying $\sum_j p_j = 1$, how can we describe the system? We generally call it an ensemble and denote it as $\{p_j, |\psi_j\rangle\}$. Suppose we want to evolve the state, it then becomes $\{p_j, U|\psi_j\rangle\}$. Suppose we want to measure the state, we have outcomes $\{p_j, \langle\psi_j| O |\psi_j\rangle\}$ for observable O. This seems ok, but also quite cumbersome. **If we only want to focus on the average behaviours, or equivalently when we do not know which state is prepared each time**, we have the following equivalent description.

$$\begin{aligned}\{p_j, |\psi_j\rangle\} &\leftrightarrow \rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|, \\ \{p_j, U|\psi_j\rangle\} &\leftrightarrow U\rho U^\dagger, \\ \{p_j, \langle\psi_j| O |\psi_j\rangle\} &\leftrightarrow \mathrm{Tr}[\rho O].\end{aligned} \tag{1}$$

We can thus use the density matrix ρ to equivalently describe a quantum ensemble.

We can also understand why we need density matrix description when we consider a subsystem of a larger system. For example, consider a joint state $|\psi\rangle_{AB}$ of system A and B, what is the expectation value if we measure O_A of system A. From what we have learnt from pure state theory, the expectation value is

$$\langle O\rangle = \langle\psi| O_A \otimes \mathrm{id}_B |\psi\rangle_{AB} = \mathrm{Tr}_{AB}[(O_A \otimes \mathrm{id}_B) \cdot |\psi\rangle\langle\psi|_{AB}]. \tag{2}$$

We can apply (partial) trace B first and then we have

$$\langle O\rangle = \mathrm{Tr}_A[\rho_A O_A] \tag{3}$$

with $\rho_A = \mathrm{Tr}_B[|\psi\rangle\langle\psi|_{AB}]$. Therefore, any expectation value on system A could be easily calculated with ρ_A. This indeed aligns with the principle of causality. That is, any local operation on system B would not affect system A (Prove it!).

Definition 1. *Quantum states are described by density matrices, which are positive and normalized matrices satisfying $\rho \geq 0$ and $Tr[\rho] = 1$.*

1.2 Two equivalent ensembles

Theorem 1. *We have two equivalent state ensembles*

$$\rho = \sum_j p_j |\psi_j\rangle \langle\psi_j| = \sum_k q_k |\phi_k\rangle \langle\phi_k| , \tag{4}$$

iff there exists a unitary U such that

$$\sqrt{p_j} |\psi_j\rangle = \sum_k U_{jk} \sqrt{q_k} |\phi_k\rangle . \tag{5}$$

If the number of $|\psi_j\rangle$ is different from the number of $|\phi_k\rangle$, we add zeros.

Proof. The if part is straightforward. For the only if part, we consider the spectral decomposition of ρ as

$$\rho = \sum_e p_e |e\rangle \langle e| . \tag{6}$$

Since $\{|e\rangle\}$ is a basis, we can represent $|\psi_j\rangle$ and $|\phi_k\rangle$ as

$$|\psi_j\rangle = \sum_e \psi_{je} |e\rangle , |\phi_k\rangle = \sum_e \phi_{ke} |e\rangle . \tag{7}$$

Then we have

$$\rho = \sum_e p_e |e\rangle \langle e| = \sum_{jee'} p_j \psi_{je} \psi^*_{je'} |e\rangle \langle e'| = \sum_{kee'} q_k \phi_{ke} \phi^*_{ke'} |e\rangle \langle e'| , \tag{8}$$

and hence

$$\sum_j p_j \psi_{je} \psi^*_{je'} = \sum_k q_k \phi_{ke} \phi^*_{ke'} = p_e \delta_{ee'}. \tag{9}$$

Suppose we add zeros so that the three sets $\{|e\rangle\}$, $|\psi_j\rangle$, and $|\phi_k\rangle$ have the same length, then we have

$$\sqrt{p_j} |\psi_j\rangle = \sum_e U_{je} \sqrt{p_e} |e\rangle , \sqrt{q_k} |\phi_k\rangle = \sum_e V_{ke} \sqrt{p_e} |e\rangle , \tag{10}$$

with unitary $U_{je} = \psi_{je}$ and $V_{ke} = \phi_{ke}$. Then we have

$$\sqrt{p_j} |\psi_j\rangle = \sum_k (U \cdot V^\dagger)_{jk} \sqrt{q_k} |\phi_k\rangle . \tag{11}$$

□

1.3 Pauli basis

For any qubit state ρ, we have the Bloch sphere representation

$$\rho = \frac{1 + \vec{n} \cdot \vec{\sigma}}{2}, \tag{12}$$

where $\vec{n}$ is a vector with norm less than 1 and $\vec{n} = \mathrm{Tr}[\rho \cdot \vec{\sigma}]$. Tensor products of the Pauli basis $\{\mathrm{id}, \vec{\sigma}\}$ also forms a basis for multi-qubit states.

1.4 Purification

For any system A described by density matrix ρ_A, its purification is given by a joint pure state ψ_{AE} satisfying $\rho_A = \mathrm{Tr}_E[\psi_{AE}]$. There are several properties of purification.

- Purification is not unique.
- Given two purifications ψ^1_{AE} and ψ^2_{AE}, they are convertible via isometry V, i.e., $\psi^2_{AE} = V\psi^1_{AE}V^\dagger$ satisfying $V^\dagger V = 1$.
- Given any decomposition of $\rho_A = \sum_j p_j |\psi_j\rangle \langle\psi_j|_A$, an explicit purification is $|\psi\rangle_{AE} = \sum_j \sqrt{p_j}\, |\psi_j\rangle_A |j\rangle_E$.
- Denote the maximally entangled state as $|\Phi^+\rangle_{AE} = \sum_j |jj\rangle_{AE}$, an explicit purification is $\mathrm{id}_A \otimes \sqrt{\rho_E}\, |\Phi^+\rangle_{AE}$.

2 Quantum channels

2.1 From unitary to quantum channels

There are at least three ways to see why we need quantum channels.

From the mathematical point of view, quantum channels are just physical transformations of states. Since we now consider density matrix, its physical transformation now corresponds to quantum channels. What does physical means? It means linear, completely positive, and trace preserving. Specifically, an operation $\mathcal{E}(\rho)$ is linear iff $\mathcal{E}(\rho_1 + \rho_2) = \mathcal{E}(\rho_1) + \mathcal{E}(\rho_2)$. The concept of completely positive is slightly more involved. An operation is called positive, if $\mathcal{E}_A(\rho_A) \geq 0$ whenever $\rho_A \geq 0$. However, only positivity is not sufficient. Consider an entangled state ρ_{AB} and a positive operation $\mathcal{E}_A$, we cannot guarantee $\mathcal{E}_A(\rho_{AB}) \geq 0$ even if we do have $\mathcal{E}_A(\rho_A) \geq 0$. A notable example is the transpose operation (check it!). Completely positive is thus a stricter requirement, which says $\mathcal{E}_A(\rho_{AB}) \geq 0$ for all $\rho_{AB} \geq 0$. At last trace preserving just means $\mathrm{Tr}[\mathcal{E}(\rho)] = \mathrm{Tr}[\rho]$. To summarize, a quantum channel is defined as follows.

Definition 2. *A quantum channel is a completely positive, trace preserving (CPTP) linear map.*

A much more physical way to understand quantum channels is to consider the subsystem dynamics of a joint evolution. Consider state ρ_A and an ancillary state $|0\rangle\langle 0|_E$ under a joint evolution U_{AE}, the evolved state becomes $U_{AE}(\rho_A \otimes |0\rangle\langle 0|_E)U^\dagger_{AE}$. If we only focus on system A, can we follow a similarly spirit to get the effective evolution on system A? Specifically, we want to partial trace E as

$$\begin{aligned}
\mathrm{Tr}_E[U_{AE}(\rho_A \otimes |0\rangle\langle 0|_E)U^\dagger_{AE}] &= \sum_j \langle j|_E U_{AE}(\rho_A \otimes |0\rangle_E \langle 0|_E)U^\dagger_{AE}|j\rangle_E\,, \\
&= \sum_j \langle j|_E U_{AE}\,|0\rangle_E\, \rho_A\, \langle 0|_E\, U^\dagger_{AE}|j\rangle_E\,, \\
&= \sum_j K_j \rho_A K_j^\dagger,
\end{aligned} \tag{13}$$

where $K_j = \langle j|\, U_{AE}\, |0\rangle_E$. Therefore the effective quantum evolution on system A is

$$\mathcal{E}_A(\rho_A) = \sum_j K_j \rho_A K_j^\dagger. \tag{14}$$

We can verify that $\sum_j K_j^\dagger K_j = \mathrm{id}_A$.

At last, we introduce the *Kraus representation* of quantum channels just as Eq. (14), which bridges the previous two formulations. We can show that

Theorem 2. *(1) Any Kraus operation of Eq.* (14) *is a quantum channel, i.e., a CPTP linear map, and vice versa. (2) Any Kraus operation of Eq.* (14) *can be physically implemented by a joint unitary on the state with another ancillary state.*

To prove (1), we need to introduce another equivalent representation of channels, the *Choi matrix*, defined as

$$\Phi_{\mathcal{E}_A} = \mathcal{E}_A \otimes \mathrm{id}_E(\Phi^+_{AE}), \tag{15}$$

where $\Phi^+_{AE} = \sum_{i,j} |ii\rangle \langle jj|$ is the unnormalized maximally entangled state. It is easy to see that $\Phi_{\mathcal{E}_A} = \mathcal{E}_A(|i\rangle \langle j|_A) \otimes |i\rangle \langle j|_E$, therefore

$$\mathcal{E}_A(|i\rangle \langle j|_A) = \mathrm{Tr}_E[\Phi_{\mathcal{E}_A} \cdot |i\rangle \langle j|^T_E] \tag{16}$$

or we have the inverse transform

$$\mathcal{E}_A(\rho_A) = \mathrm{Tr}_E[\Phi_{\mathcal{E}_A} \cdot \rho^T_E]. \tag{17}$$

Note that ρ_E is defined as the density matrix of ρ_A.

Now we prove (1) that any CPTP map has a Kraus representation (the other direction is quite straightforward).

Proof. For any CP map $\mathcal{E}_A$, its Choi matrix $\Phi_{\mathcal{E}_A}$ is positive. Consider a decomposition of $\Phi_{\mathcal{E}_A}$ as

$$\Phi_{\mathcal{E}_A} = \sum_j |\psi_j\rangle_{AE} \langle\psi_j|_{AE}, \tag{18}$$

where $|\psi_j\rangle_{AE}$ are unnormalized. Suppose $|\psi_j\rangle_{AE} = \sum_k |\psi_{jk}\rangle_A |k\rangle_E$ with unnormalized states $|\psi_{jk}\rangle_A$, we have

$$\begin{aligned}
\mathcal{E}_A(\rho_A) &= \mathrm{Tr}_E\left[\sum_j |\psi_j\rangle_{AE} \langle\psi_j|_{AE} \cdot \rho^T_E\right], \\
&= \mathrm{Tr}_E\left[\sum_{j,k,k'} |\psi_{jk}\rangle_A |k\rangle_E \langle\psi_{jk'}|_A \langle k'|_E \cdot \rho^T_E\right], \\
&= \sum_{j,k,k'} |\psi_{jk}\rangle_A \langle\psi_{jk'}|_A \cdot \langle k'|_E \rho^T_E |k\rangle_E, \\
&= \sum_{j,k,k'} |\psi_{jk}\rangle_A \langle\psi_{jk'}|_A \cdot \langle k|_A \rho_A |k'\rangle_A, \\
&= \sum_j \left[\sum_k |\psi_{jk}\rangle_A \langle k|_A\right] \rho_A \left[\sum_{k'} |k'\rangle_A \langle\psi_{jk'}|_A\right],
\end{aligned} \tag{19}$$

which agrees with the Kraus form if we let $K_j = \sum_k |\psi_{jk}\rangle_A \langle k|_A$. It is easy to show that TP guarantees $\sum_j K_j^\dagger K_j = \mathrm{id}_A$. □

To see (2), we need to construct a joint unitary such that it is equivalent to the Kraus form. Using ancillary state $|0\rangle$, the unitary can be constructed as

$$U_{EA} = \sum_j K_j \otimes |j\rangle_E \langle 0|_E + \cdots = \begin{bmatrix} K_1 & . & . & . & \\ K_2 & . & . & . & \\ K_3 & . & . & . & \\ \cdots & . & . & . & \end{bmatrix} \tag{20}$$

Here we swap the A and E indices for easier matrix representation. We can see that only the first column is determined so the unitary is not fixed.

2.2 Equivalent Kraus representations

Theorem 3. *Suppose two Kraus channels* $\{K_j\}$ *and* $\{\tilde{K}_k\}$ *are equivalent, then there exists a unitary* U *such that* $K_j = \sum_k U_{jk}\tilde{K}_k$.

Proof. The proof follows from an inverse construction of the previous proof and applying Theorem 1 to Eq. (18). □

2.3 Typical quantum channels

- State preparation $\mathcal{E}(\mathbb{C}) = \rho$.
- Unitary or isometry $\mathcal{E}(\rho) = U\rho U^\dagger$.
- Measurement $\mathcal{E}(\rho) = \sum_j \mathrm{Tr}[\rho O_j] \left|j\right\rangle\left\langle j\right|$. (We will study this soon)
- Typical qubit channels (consider their effect on a general qubit state)
  - Dephasing channel $\mathcal{E}(\rho) = (1-p)\rho + pZ\rho Z$.
  - Depolarizing channel $\mathcal{E}(\rho) = (1-p)\rho + p(X\rho X + Y\rho Y + Z\rho Z)$. (Note that $\frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z) = I/2$.)
  - Amplitude damping channel $K_0 = \sqrt{\gamma}\left|0\right\rangle\left\langle 1\right|$ and $K_1 = \left|0\right\rangle\left\langle 0\right| + \sqrt{1-\gamma}\left|0\right\rangle\left\langle 1\right|$.
  - Erasure channel $\mathcal{E}(\rho) = (1-p)\rho + p\left|2\right\rangle\left\langle 2\right|$.

3 POVM

A most general measurement is to correlate the system with some ancillary qubit, apply a joint unitary, and measure the ancillary state. It thus corresponds a measurement channel as

$$\mathcal{M}(\rho) = \sum_j \left\langle j\right|_E \mathrm{Tr}_A[U_{AE}(\rho_A \otimes \left|0\right\rangle\left\langle 0\right|_E)U_{AE}^\dagger]\left|j\right\rangle_E \left|j\right\rangle\left\langle j\right|_E . \tag{21}$$

Following the above derivation the measurement channel is

$$\mathcal{M}(\rho) = \sum_j \mathrm{Tr}[K_j^\dagger K_j \rho_A]\left|j\right\rangle\left\langle j\right|_E . \tag{22}$$

Denote $O_j = K_j^\dagger K_j$, then a POVM corresponds to positive O_j satisfying $\sum_j O_j = \mathrm{id}$. For example, $\{\left|0\right\rangle\left\langle 0\right|/3, \left|1\right\rangle\left\langle 1\right|/3, \left|\pm\right\rangle\left\langle \pm\right|/3, \left|\pm i\right\rangle\left\langle \pm i\right|/3\}$ is a valid POVM (construct it).