CS59200-PRS: Pseudorandomness Nov 3, 2025

Lecture 19: Basic of Quantum Computing (Part II)

Lecturer: Wei Zhan *Scribe: Wenbo Xie*

1 Mixed States and Density Operators

Last week we introduced quantum states which are unit complex vectors. In many scenarios we need to work with distributions of quantum states, which are captured by the notion of mixed states.

Definition 1 (Mixed State)**.** *A mixed state is a quantum state that represents a statistical ensemble of different pure states. In other words, the quantum system in pure state $|\psi_i\rangle$ with probability p_i.*

The mixed state can be represented as an operator defined below:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{1}$$

The operator is called the density operator.

Definition 2 (Density Operator)**.** *The matrix $\rho \in \mathbb{C}^{N\times N}$ is a density operator and can represent a mixed state if:*

- $\rho = \rho^\dagger$ *(Hermitian)*
- $\rho \succeq 0$ *(semi-positive-definite),*
- $\mathrm{Tr}(\rho) = 1$.

Remark 1. If $\mathrm{rank}(\rho) = 1$, i.e., $\rho = |\psi\rangle\langle\psi|$, then ρ is a pure state.

Example. After measuring $|+\rangle$ in the computational basis, the state collapses to $|0\rangle$ or $|1\rangle$ with probability $\frac{1}{2}$ each. Thus, the mixed post-measurement state is given by

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}I.$$

Such a state is called *maximally mixed state* on a single qubit. In general, for n qubits, the maximally mixed state is:

$$\left(\frac{1}{2}I\right)^{\otimes n} = \frac{1}{2^n}I_{2^n}.$$

The maximally mixed state can be viewed as the uniform distribution over the basis $\{|x\rangle \mid x \in \{0,1\}^n\}$. In fact, every classical distribution can also be represented by a density operator which is a diagonal matrix.

Remark 2. Mixed states can be non-uniquely decomposed into mixtures of pure states. For example, for the single-qubit maximally mixed state, we also have

$$\frac{1}{2}I = \frac{1}{2}|+\rangle\langle+| + \frac{1}{2}|-\rangle\langle-|,$$

or in general,

$$\frac{1}{2}I = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b|,$$

for every pair of orthogonal states $\langle a|b\rangle = 0$.

1.1 Operations on Mixed States

As mixed states are distributions over pure states, the operations we can apply on mixed states are the same as the ones on pure states. These include unitaries and measurements.

Unitary Operators on Mixed States: Recall that for any pure state $|\psi\rangle$, the unitary U acts on $|\psi\rangle$ as:

$$U : |\psi\rangle \mapsto U|\psi\rangle$$

As a result, the unitary operator U acts on ρ as:

$$U : \rho \mapsto \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = U\rho U^\dagger.$$

Measurement on Mixed States: When we apply the projective measurement $\{\Pi_j\}$ on the pure state $|\psi\rangle$, the probability that the measurement outcome is j is given by $\langle\psi|\Pi_j|\psi\rangle$, and the state collapses to

$$\frac{\Pi_j|\psi\rangle}{\sqrt{\langle\psi|\Pi_j|\psi\rangle}}.$$

As a result, if we apply the measurement on the mixed state ρ, the probability that the measurement outcome is j is given by

$$\sum_i p_i\langle\psi_i|\Pi_j|\psi_i\rangle = \sum_i p_i \mathrm{Tr}[\Pi_j|\psi_i\rangle\langle\psi_i|] = \mathrm{Tr}[\Pi_j\rho],$$

and the state collapses to

$$\frac{\Pi_i\rho\Pi_i^\dagger}{\mathrm{Tr}[\Pi_i\rho]}.$$

Remark 3. If we discard the measurement outcome, the resulting state will again be a mixture over the collapsed states with different measurement outcomes, and therefore represented by the mixed state

$$\sum_i \mathrm{tr}[\Pi_i \rho] \cdot \frac{\Pi_i \rho \Pi_i^\dagger}{\mathrm{Tr}[\Pi_i \rho]} = \sum_i \Pi_i \rho \Pi_i^\dagger.$$

Notice that this is not necessarily the same state as ρ, which means that even if you just perform the measurement without reading the outcome, the quantum state will still be changed.

2 Partial Trace

In classical probability theory, given a joint distribution, the marginal distribution is obtained by summing over parts of the joint distribution corresponding to the variables being ignored. In quantum computing, the partial trace plays an analogous role: it produces the reduced state of a subsystem by tracing out the degrees of freedom of the other. Consider a composite quantum system consisting of two subsystems—A with n qubits and B with m qubits—so that the total system contains $n+m$ qubits. How can we describe the reduced state on the first n qubits?

Definition 3 (Trace and Partial Trace)**.** *Let ρ_{AB} be a mixed state on the composite quantum system of $n+m$ qubits. The trace of ρ_{AB} is given by*

$$\mathrm{Tr}[\rho_{AB}] = \sum_{x \in \{0,1\}^{n+m}} \langle x | \rho_{AB} | x \rangle,$$

and the partial trace over the system B is given by

$$\mathrm{Tr}_B[\rho_{AB}] = \sum_{x \in \{0,1\}^m} (I_N \otimes \langle x |) \, \rho \, (I_N \otimes |x\rangle),$$

where I_N is the identity on A with $N = 2^n$.

Example. If ρ is a product state, i.e. $\rho = \rho_A \otimes \rho_B$, then

$$\mathrm{Tr}_B[\rho_{AB}] = \rho_A.$$

If $\rho = \sum_i \alpha_i \rho_{A,i} \otimes \rho_{B,i}$, then

$$\mathrm{Tr}_B[\rho_{AB}] = \sum_i \alpha_i \rho_{A,i} \mathrm{Tr}[\rho_{B,i}] = \sum_i \alpha_i \rho_{A,i}.$$

Using partial trace, we can show the following two important properties of quantum systems: That any local operation on a subsystem does not affect the others.

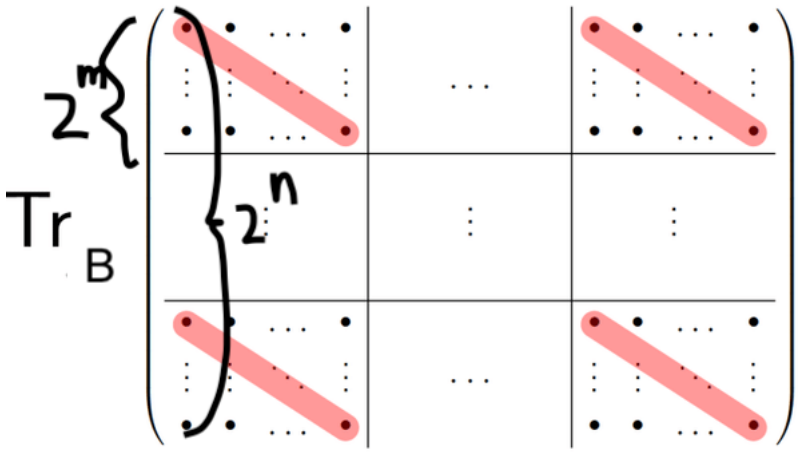

Figure 1: In the density operator representation, the state ρ_{AB} can be viewed as a block matrix of size $2^n \times 2^n$, where each block is itself a $2^m \times 2^m$ matrix corresponding to subsystem B. The partial trace over B can then be interpreted as taking the trace of each $2^m \times 2^m$ sub-block, as illustrated in the diagram.

Lemma 4. *Local unitaries on the subsystem one traces out do not affect the reduced state of the other subsystem. In other words, if one applies any unitary transformation U to the subsystem B, the reduced state on A remains unchanged.*

Proof. Let us consider the unitary U and apply it to the sub-system B only. Then, the reduced state on A is given by

$$\begin{aligned}
&\mathrm{Tr}_B\left[(I_N \otimes U)\rho_{AB}(I_N \otimes U^\dagger)\right] \\
&= \sum_x (I_N \otimes \langle x|U)\rho_{AB}(I_N \otimes U^\dagger|x\rangle) \\
&= \sum_x \left(\sum_{y,z} U_{xy}U^\dagger_{zx}(I_N \otimes \langle y|)\rho_{AB}(I_N \otimes |z\rangle)\right) \\
&= \sum_{y,z} (I_N \otimes \langle y|)\rho_{AB}(I_N \otimes |z\rangle)\left(\sum_x U_{xy}U^\dagger_{zx}\right) \\
&= \sum_{y,z} (I_N \otimes \langle y|)\rho_{AB}(I_N \otimes |z\rangle)\cdot\delta_{yz} \\
&= \sum_y (I_N \otimes \langle y|)\rho_{AB}(I_N \otimes |y\rangle) = \mathrm{Tr}_B[\rho_{AB}].
\end{aligned}$$

□

Lemma 5. *Local measurement on the subsystem one traces out do not affect the reduced state of the other subsystem. In other words, if one measures the subsystem B and measurement outcome is unknown, the reduced state on A remains unchanged.*

Proof. Let $\{\Pi_i\}$ be a set of measurement projectors on the subsystem B. After measuring B, which is equivalent to measuring the entire system with projectors $\{I_N \otimes \Pi_i\}$, the reduced state on A becomes

$$\begin{aligned}
&\mathrm{Tr}_B\left[\sum_i (I_N \otimes \Pi_i)\rho_A(I_N \otimes \Pi_i^\dagger)\right] \\
=&\sum_{i,x}\sum_{y,z} \Pi_{i,xy}\Pi_{i,zx}^\dagger (I_N \otimes \langle y|)\rho_A(I_N \otimes |z\rangle) \\
=&\sum_{y,z} (I_N \otimes \langle y|)\rho_A(I_N \otimes |z\rangle)\left(\sum_{i,x} \Pi_{i,xy}\Pi_{i,zx}^\dagger\right) \\
=&\sum_{y} (I_N \otimes \langle y|)\rho_{AB}(I_N \otimes |y\rangle) = \mathrm{Tr}_B[\rho_{AB}].
\end{aligned}$$

□

Lemma 5 could be used to explain that in the deferred measurement principle, we can ignore the measurement on the ancilla qubits as the operation of measurements does not affect the actual system that we care about.

Theorem 6 (Purification)**.** *Every mixed state is a partial trace of a pure state.*

Proof. Given the mixed state ρ, let $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ be the eigen-decomposition. Consider the pure state $|\psi\rangle_{AB} = \sum_i \sqrt{p_i}|\psi_i\rangle_A|i\rangle_B$. Then,

$$\begin{aligned}
&\mathrm{Tr}_B[|\psi\rangle\langle\psi|] \\
=&\sum_{i,j} \sqrt{p_i p_j}\mathrm{Tr}_B[|\psi_i\rangle_A|i\rangle_B\langle\psi_j|_A\langle j|_B] \\
=&\sum_{i,j} \sqrt{p_i p_j}\left(\sum_x (I_N \otimes \langle x|)(|\psi_i\rangle_A|i\rangle_B\langle\psi_j|_A\langle j|_B)(I_N \otimes |x\rangle)\right) \\
=&\sum_i p_i|\psi_i\rangle\langle\psi_i| = \rho.
\end{aligned}$$

□

3 Haar Measure

Definition 4. *The Haar measure on n-qubit quantum states is the unique measure on*

$$\left\{|\psi\rangle \in \mathbb{C}^N : \||\psi\rangle\|_2 = 1\right\}$$

such that it is invariant under unitaries, i.e., $|\psi\rangle \sim \mathrm{Haar}(N)$ *and* $U|\psi\rangle$ *are equidistributed for every unitary* $U \in \mathbb{U}(N)$*.*

What is the density matrix ρ for a Haar random state? By definition, we know ρ must satisfy $\rho = U\rho U^\dagger$ for all $U \in \mathbb{U}(N)$. It follows that $\rho = \frac{1}{N}I_N$. Notice that this is the same

density matrix as a uniformly random base state (i.e., $\sum_{i\in[N]} \frac{1}{N}|i\rangle\langle i|$) can also be but a Haar random state is much more random. In fact, we can show that a Haar random state is almost always hard to prepare, while a random base state can be easily prepared using one layer of `NOT` gates from the initial state $|0^n\rangle$.

Theorem 7. *Given any finite universal gate set, the circuit complexity of preparing an n-qubit Haar random state (up to 0.1 error in ℓ_2-norm) is $2^{\Omega(n)}$ with high probability.*

Proof. First, we note that the number of circuits of size S is at most $2^{O(S\log n)}$, since there are $\mathrm{poly}(n)$ many choices for each gate. On the other hand, the probability that a Haar random state is ℓ_2-close to the state $C|0^{\otimes n}\rangle$ prepared by the circuit C is

$$\begin{aligned}
&\Pr_{|\psi\rangle\sim\mathrm{Haar}(N)}\left[\||\psi\rangle - C|0^{\otimes n}\rangle\|_2 \le 0.1\right] \\
=\ &\Pr_{|\psi\rangle\sim\mathrm{Haar}(N)}\left[\|C^\dagger|\psi\rangle - C^\dagger C|0^{\otimes n}\rangle\|_2 \le 0.1\right] && \text{(Property of the Norm)} \\
=\ &\Pr_{|\psi\rangle\sim\mathrm{Haar}(N)}\left[\||\psi\rangle - |0^{\otimes n}\rangle\|_2 \le 0.1\right] && \text{(Haar Measure is Invariant Under Unitary)} \\
\le\ &\Pr_{|\psi\rangle\sim\mathrm{Haar}(N)}\left[|\psi_0| \ge 0.9\right]
\end{aligned}$$

Here ψ_0 is the first coordinate of $|\psi\rangle \in \mathbb{C}^N$, and $|\psi_0|$ is concentrated around $1/\sqrt{N}$. A concentration bound can show that the above probability is at most $2^{-\Omega(N)}$, and thus by a union bound we have

$$\Pr_{|\psi\rangle\sim\mathrm{Haar}(N)}\left[\exists \text{ circuit of size } S : \||\psi\rangle - C|0^{\otimes n}\rangle\|_2 \le 0.1\right] \le 2^{O(S\log n)-\Omega(N)}$$

which is negligible for some $S = \Omega(N/\log n) \ge 2^{\Omega(n)}$. □