COL7160 : Quantum Computing

Lecture 25: Mixed States, Density Matrix, General Measurements, and Complexity Classes

Instructor: Rajendra Kumar **Scribe:** Naman Goyal

1 Mixed States

In many quantum algorithms and physical scenarios, we do not have complete knowledge of the exact state a quantum system is in. Instead of being in a single definite pure state, the system might be in one of several pure states $|\varphi_i\rangle$ with corresponding classical probabilities p_i. Such a system is said to be in a *mixed state* [NC10].

Definition 1 (Mixed State)**.** A mixed state is represented by an ensemble $\{(p_1, |\varphi_1\rangle), (p_2, |\varphi_2\rangle), \ldots, (p_k, |\varphi_k\rangle)\}$, meaning the system is in the state $|\varphi_i\rangle$ with probability p_i, where $\sum_{i=1}^{k} p_i = 1$. Importantly, the states $|\varphi_i\rangle$ are not required to be mutually orthogonal [dW23].

Note that a quantum superposition involves a linear combination of state vectors with complex amplitudes (e.g., $\sum_i \sqrt{p_i}\,|\varphi_i\rangle$), whereas a mixed state represents classical uncertainty regarding which pure state the system is actually in.

Example 1 (Distinguishing a Superposition from a Mixed State)**.** Consider two different systems:

1. A pure state in an equal superposition: $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$.
2. A mixed state where the system is $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$.

If we measure both systems in the standard computational basis $\{|0\rangle, |1\rangle\}$, both will yield the outcome 0 with probability $1/2$ and the outcome 1 with probability $1/2$.
However, there is a procedure to distinguish them. We can apply the Hadamard gate (H) before measuring in the standard basis:

- **For the pure state:** $H|+\rangle = |0\rangle$. A subsequent measurement in the standard basis will yield the outcome 0 with probability 1.
- **For the mixed state:** Since we don't know anything about the state it is very difficult to comment as to what will be the result of applying H gate and then measuring the states.

Since the measurement statistics differ in general, the two systems are not the same state.

2 Constructing the Density Matrix

Suppose we want to measure the mixed state in an arbitrary orthonormal basis $\{|b_1\rangle, |b_2\rangle, \ldots, |b_n\rangle\}$. We want to calculate the total probability of measuring a specific basis state $|b_j\rangle$.

$$\begin{aligned} P(b_j) &= \sum_{i=1}^{k} p_i \left|\langle b_j|\varphi_i\rangle\right|^2 \\ &= \sum_{i=1}^{k} p_i \langle b_j|\varphi_i\rangle \langle\varphi_i|b_j\rangle \\ &= \langle b_j| \left(\sum_{i=1}^{k} p_i |\varphi_i\rangle \langle\varphi_i|\right) |b_j\rangle \end{aligned}$$

Definition 2 (Density Matrix)**.** The density matrix ρ of the ensemble $\{(p_i, |\varphi_i\rangle)\}$ is defined as:

$$\rho = \sum_{i=1}^{k} p_i \, |\varphi_i\rangle \, \langle\varphi_i|$$

Hence, the probability of the system collapsing to the basis state $|b_j\rangle$ upon measurement is just:

$$P(b_j) = \langle b_j| \, \rho \, |b_j\rangle$$

Theorem 1. *If two states yield the exact same density matrix ρ, then they represent the same mixed state. Hence, they are indistinguishable by any quantum measurement [NC10].*

Example 2. Calculate the density matrix ρ_1 for a system prepared in the state $|+\rangle$ with probability $1/2$ and the state $|0\rangle$ with probability $1/2$.
Solution: By definition:

$$\rho_1 = \frac{1}{2} \, |+\rangle \, \langle +| + \frac{1}{2} \, |0\rangle \, \langle 0|$$

Converting the outer products to their matrix representations in the standard computational basis:

$$\rho_1 = \frac{1}{2} \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix} + \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix}$$

Example 3. Calculate the density matrix ρ_2 for a system prepared in the state $|0\rangle$ with probability $1/2$ and the state $|1\rangle$ with probability $1/2$.
Solution: Using the definition of the density matrix:

$$\rho_2 = \frac{1}{2} \, |0\rangle \, \langle 0| + \frac{1}{2} \, |1\rangle \, \langle 1|$$

Representing these outer products as matrices:

$$\rho_2 = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} = \frac{I}{2}$$

Example 4. Calculate the density matrix ρ_3 for a system prepared definitively in the state $|+\rangle$ with probability 1.
Solution: Using the similar procedure as shown in the previous examples:

$$\rho_3 = 1 \cdot |+\rangle \, \langle +|$$

$$\rho_3 = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

Remark 1. For any valid density matrix ρ, the trace must always equal unity: $\mathrm{Tr}(\rho) = 1$, as the trace of ρ directly corresponds to the sum of the classical probabilities ($\sum p_i = 1$) of the constituent pure states in the mixture.

Theorem 2. *If two quantum systems are described by distinct density matrices ($\rho_1 \neq \rho_2$), then they represent different physical states. Consequently, we can always find a measurement which can distinguish between the two states.*

Remark 2. To distinguish whether a given density matrix represents a pure state or a mixed state, we evaluate the trace of the squared density matrix, $\mathrm{Tr}(\rho^2)$, if it is 1 then it implies a pure state or a mixed state otherwise.

Remark 3. When we apply a unitary operator U, the individual state vectors transform as $|\varphi_i\rangle \to U \, |\varphi_i\rangle$. The density matrix ρ updates via conjugation with U.
If the initial density matrix is defined as $\rho = \sum_{i=1}^{k} p_i \, |\varphi_i\rangle \, \langle\varphi_i|$, then the post-unitary density matrix ρ' is given by:

$$\rho' = U \rho U^\dagger = \sum_{i=1}^{k} p_i (U \, |\varphi_i\rangle)(\langle\varphi_i| \, U^\dagger)$$

Remark 4. Whenever a density matrix is diagonal in a given basis, it indicates that the system is entirely a mixture of those specific basis states.

3 Projective Measurement

In quantum mechanics, a projective measurement is described by a set of projector matrices.

Definition 3 (Projectors)**.** Let $\{P_1, \ldots, P_M\}$ be a set of projector matrices representing the possible measurement outcomes. These operators must satisfy [NC10]:

1. **Completeness:** $\sum_{i=1}^{M} P_i = I$.
2. **Idempotence:** $P_i^2 = P_i$.

For every diagonalizable matrix, you can write it as a sum of weighted projectors: $M = \sum_i \lambda_i P_i$, where λ_i are the eigenvalues.

Definition 4 (Measurement Rule)**.** If a quantum system is currently in a pure state $|\psi\rangle$, performing a projective measurement will yield the i-th outcome with a probability:

$$p(i) = \| P_i |\psi\rangle \|^2$$

Note: Since P_i is a projector, this is mathematically equivalent to $\langle\psi| P_i |\psi\rangle$.
Upon obtaining this i-th outcome, the system collapses. The post-measurement state is updated and renormalized as follows:

$$|\psi\rangle \to \frac{P_i |\psi\rangle}{\| P_i |\psi\rangle \|}$$

4 Positive Operator-Valued Measurement (POVM)

This formulation is particularly useful when we are only interested in the classical measurement outcomes (probabilities) rather than the exact post-measurement quantum state.

Definition 5 (Positive Operator-Valued Measure)**.** A POVM is defined by a set of M positive semi-definite matrices $\{E_1, \ldots, E_M\}$ that satisfy the completeness relation [NC10]:

$$\sum_{i=1}^{M} E_i = I$$

A matrix E_i is positive semi-definite if $\langle\psi| E_i |\psi\rangle \geq 0$ for all states $|\psi\rangle$. This property guarantees that E_i can be decomposed (e.g., into the form $A^\dagger A$), which ensures all resulting measurement probabilities are strictly non-negative.

Definition 6 (POVM Measurement Rule)**.** If a system is prepared in a pure state $|\psi\rangle$, the probability of obtaining the i-th classical outcome is given by the trace rule:

$$p(i) = \mathrm{Tr}(E_i |\psi\rangle \langle\psi|)$$

As discussed in class, if we do not know which state the system is initially in, applying a POVM will collapse the possibilities and simply output a classical symbol representing the outcome index i, without necessarily leaving the system in a defined eigenstate.

Example 5 (Distinguishing Non-Orthogonal States)**.** Construct a POVM to distinguish between the non-orthogonal states $|0\rangle$ and $|+\rangle$. Our goal is to be always correct in our output.
Solution: Because the states are not completely orthogonal, a standard projective measurement cannot always distinguish them. Instead, we define a 3-element POVM to achieve unambiguous state identification. We set our measurement operators as:

$$E_1 = \frac{1}{2} |-\rangle \langle-|$$
$$E_2 = \frac{1}{2} |1\rangle \langle 1|$$
$$E_3 = I - E_1 - E_2$$

This measurement yields three possible classical outcomes:

- **Outcome 1 (State $\to |0\rangle$):** If we measure E_1, the initial state could not possibly have been $|+\rangle$ because the probability $\langle +| E_1 |+\rangle \propto |\langle -|+\rangle|^2 = 0$. Therefore, we conclude with certainty that the state was $|0\rangle$.
- **Outcome 2 (State $\to |+\rangle$):** If we measure E_2, the initial state could not have been $|0\rangle$ because $\langle 0| E_2 |0\rangle \propto |\langle 1|0\rangle|^2 = 0$. We conclude with certainty that the state was $|+\rangle$.
- **Outcome 3 (I don't know):** If we measure E_3, we output "I don't know".

5 Complexity Classes

Definition 7. We define the following standard classes of decision problems that can be solved in polynomial time with a bounded probability of error:

- BPP **(Bounded-error Probabilistic Polynomial time):** Solvable by a probabilistic classical Turing machine with an error probability of at most $1/3$ for all instances.
- RP **and** co-RP **(Randomized Polynomial time):** Classes featuring one-sided error. RP algorithms may yield false negatives but no false positives. Conversely, co-RP algorithms may yield false positives but never false negatives.
- BQP **(Bounded-error Quantum Polynomial time):** Solvable by a quantum computer in polynomial time, with an error probability bounded by $1/3$.

Example 6 (Polynomial Identity Testing)**.** This problem asks to identify whether a given multivariate polynomial is identically zero. While no deterministic polynomial-time algorithm is known, evaluating the polynomial at random points works efficiently. By the Schwartz-Zippel lemma, if it evaluates to zero, it is highly likely to be the zero polynomial. This places PIT in co-RP (and consequently within BPP).

Example 7 (Integer Factorization)**.** The problem of finding the prime factors of an integer is strongly believed to reside strictly outside BPP. However, Shor's Algorithm solves it efficiently on a quantum machine, definitively placing Integer Factorization within BQP [Sho94].

We next consider complexity classes based on the concept of *verification*.

Definition 8 (NP (Nondeterministic Polynomial time))**.** NP is the class of decision problems where, if the answer is a "yes" instance, there exists a classical proof (or *witness*) of polynomial size. The validity of this witness can be evaluated by a **deterministic verification** process in polynomial time [NC10].

Definition 9 (QMA (Quantum Merlin Arthur))**.** QMA is the quantum analog of NP (specifically, the quantum extension of the probabilistic class MA). In QMA, the verification process ensures that "everything is quantum":

- **The Prover / Witness:** An all-powerful prover supplies a polynomial-size quantum state ($|\psi\rangle$) as the witness.
- **The Verifier:** A polynomial-time quantum circuit evaluates the witness.

For a "yes" instance, there must exist some quantum witness that causes the verifier to accept with a probability $\geq 2/3$. For a "no" instance, the verifier must reject with probability $\geq 2/3$, regardless of what quantum state the prover attempts to supply [dW23].

References

[dW23] Ronald de Wolf. Quantum computing: Lecture notes, 2023.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, UK, 10th anniversary edition edition, 2010.

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.