CSE 291 / Math 277A - Quantum Complexity Theory September 27, 2022

Lecture 2

Lecturer: Daniel Grier *Scribe: Tom Wu*

1 Warm-Up Question

Does a $(2n)$-qubit unitary U exist, such that

$$U(|\psi\rangle \otimes |0...0\rangle) = |\psi\rangle \otimes |\psi\rangle \,,\ \forall\, |\psi\rangle$$

for all possible pure states ψ?

Answer This cannot exist and we can construct a short proof just for the case $U(|\psi\rangle \otimes |0\rangle),\ |\psi\rangle \in \mathbb{C}^2$. This result is also called the "no-cloning theorem".

Proof. Let $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ be an unknown pure state that we want to clone and $|0\rangle$ the state to clone onto. In formula this means, we want a cloning unitary U that fulfills

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \,.$$

Writing out the left hand side, we arrive at

$$U(|\psi\rangle \otimes |0\rangle) = U(a\,|00\rangle + b\,|10\rangle) = aU(|00\rangle) + bU(|10\rangle). = a\,|00\rangle + b\,|11\rangle \,,$$

where the last equality follows from the assumption that U clones any state in the first register to the second register. Writing out the right hand side, we arrive at

$$|\psi\rangle \otimes |\psi\rangle = a^2\,|00\rangle + ab\,|01\rangle + ab\,|10\rangle + b^2\,|11\rangle \,.$$

Comparing both sides, we see that this equality can only hold, if $ab = 0$ (and in particular either $a = 1,\ b = 0$ or $a = 0,\ b = 1$). This idea can be extended to any state $|s\rangle$ that we want to copy onto. A short sketch of this is: Let $|\psi\rangle\,, |\phi\rangle$ be two pure unknown states that we want to copy. We have

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

and

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$$

Multiply the conjugate transpose of the first to the second (the inner product of the first equation and the second equation) gives

$$(\langle\psi| \otimes \langle s|)U^\dagger U(|\phi\rangle \otimes |s\rangle) = \langle\psi|\phi\rangle^2 \,.$$

Using the unitary property ($U^\dagger U = I$), we have $\langle\psi|\phi\rangle \langle s|s\rangle = \langle\psi|\phi\rangle$. Furthermore, $\langle s|s\rangle$ must be 1 for $|s\rangle$ to be a valid quantum state. Hence, we arrive at $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$. This holds only when ψ and ϕ are parallel or orthogonal to each other and hence not for two arbitrary states ϕ, ψ. $\square$

2 Pure State Picture

Recall that a 1-qubit state $|\psi\rangle \in \mathbb{C}^2$ can be written as a linear combination of the basis vectors $|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,,\ \ a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. The column form vector $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ is called a *ket* and its conjugate transpose $\langle\psi| = \begin{bmatrix} a^* & b^* \end{bmatrix}$ is called a *bra*. Together, the inner product of two states can be written as $\langle\psi|\phi\rangle := \langle\psi|\,|\phi\rangle$, hence the names bra and ket ("braket"). For example, we can state the conditions for the amplitudes (the complex coefficients a, b) simply as $\langle\psi|\psi\rangle = 1$.

This 1-qubit state definition can then be extended to the n-qubit state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$. We can expand this further in a linear combination of the orthogonal basis vectors

$$|\psi\rangle = \sum_{i \in \{0,1\}^n} a_i\,|i\rangle \,.$$

Operations

The permitted quantum operations are precisely described by the unitary matrices:

$$UU^\dagger = U^\dagger U = I.$$

Unitary operations preserve inner products—that is, for all states $|\psi\rangle$ and $|\phi\rangle$, the states transformed under the unitary ($U|\psi\rangle$ and $U|\phi\rangle$) have the same inner product:

$$\langle\psi|\phi\rangle = (U|\psi\rangle)^\dagger(U|\phi\rangle) = \langle\psi| U^\dagger U |\phi\rangle = \langle\psi|\phi\rangle .$$

This was used to prove the no-cloning theorem.

Measurements

Born Rule: The quantum mechanical principle that measurement of the state $|\psi\rangle = a_1|1\rangle + ... + a_{2^n}|2^n\rangle$ results in outcome i with probability equal to the square of the magnitude of the amplitude a_i: $|a_i|^2 = |\langle i|\psi\rangle|^2$, where $|i\rangle$ is the unit vector with entry 1 at index i. This leaves the system in the post-measurement state $|i\rangle$. The set of basis vectors $|x_1x_2...x_n\rangle$ with $x_i \in \{0,1\}$ is called the computational basis. If the measurement from the above Born rule is carried out in this basis, it will be called "computational basis measurement".

3 Mixed State Picture

Sometimes, we don't want to think of a quantum system being in a single pure state, but rather an ensemble of pure states. This makes sense, if we for example only know that our system can be in different (pure) states, but not in which state it currently is prepared in. Such states are called mixed states and are represented by a *density matrix*.

It turns out this alternate formulation is (almost) equivalent to the vector view (pure state) and will be shown at the end of this lecture. The formulation is as follows: Suppose our quantum system can be in multiple pure states $|\psi_i\rangle$, with probabilities p_i. We shall call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states. The density operator for the system is defined by the equation

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

From this formulation, we can define a few properties of any density matrix:

- Unit trace ($\mathrm{tr}(\rho) = 1$):

$$\mathrm{tr}(\rho) = \sum_i p_i \,\mathrm{tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i \langle\psi_i|\psi_i\rangle = \sum_i p_i = 1.$$

- Positive semidefinite (ρ is Hermitian and $\forall |\phi\rangle, \langle\phi|\rho|\phi\rangle \geq 0$):

$$\langle\phi|\rho|\phi\rangle = \sum_i p_i \langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle = \sum p_i |\langle\phi|\psi_i\rangle|^2 \geq 0$$

In fact, every density matrix with just those two properties defines a proper mixed state. To see this, notice that because ρ is positive semidefinite (PSD) and therefore Hermitian, we can apply the spectral theorem. We get a decomposition of the density matrix into a linear combination of eigenvalues (λ_i) and orthonormal eigenvectors (v_i):

$$\rho = \sum_i \lambda_i v_i v_i^\dagger$$

Since ρ is PSD with unit trace the λ_i will be positive and sum to 1, so we can associate them with a probability distribution. Since the v_i are orthonormal, we can associate them with pure states.

Operations

If one applies a unitary transformation U to the mixed state ρ, the density matrix then becomes $U\rho U^\dagger$. More generally, the transformation applied can also be randomized. The most general form of operation applicable in the mixed state picture is called a completely positive trace preserving map (CPTP) or quantum channel.

Measurement

For a mixed state with density matrix ρ, measuring with respect to the computational basis gives outcome i with probability $\rho_{ii} = \langle i| \rho |i\rangle$.

The most general notion of measurement is captured by a *positive operator-valued measure* (POVM). A POVM consists of a set of PSD matrices $\{E_i\}_{i=1}^k$ s.t. $\sum E_i = I$. The measurement outcome i is associated with the POVM element E_i and is obtained with probability $\mathrm{tr}(\rho E_i)$.

4 Reconciling Pure and Mixed State Pictures

We can see that a pure state can easily be represented as a mixed state, by just taking the pure state as the ensemble, i.e. $\rho = |\phi\rangle\langle\phi|$. In particular, for a state with density matrix ρ, it is pure if and only if $1 = \mathrm{tr}(\rho^2) = \mathrm{tr}(\rho)$.

We then try to represent a mixed state by a pure state. One should not hope to find a representation of a mixed in a pure state with the same number of parameters, because for the same n, a pure state has only 2^n parameters (vector of dimension 2^n), while a mixed will require 4^n parameters (since the density matrix is a $2^n \times 2^n$ matrix). The idea is to represent a mixed state using a pure state on $2n$ qubits, such that the number of parameters match.

Intermezzo: Partial Trace

We introduce the partial trace of a density operator of a composite system $A \otimes B$ in order to talk about a subsystem B. The tool allows us to represent the statistics of a subsystem after "forgetting" the other qubits. Let $A \otimes B$ be a composite system. Let M_A be the set of density matrices for system A and M_B be the set of density matrices for system B. Then, mathematically, the partial trace operator tr_B is the unique linear mapping $M_A \times M_B \mapsto M_A$ satisfying

$$\mathrm{tr}_B(|a_i\rangle \langle a_j|) \otimes |b_i\rangle \langle b_j|) = |a_i\rangle \langle a_j| \, \mathrm{tr}(|b_i\rangle \langle b_j|) \,,$$

where a_i, a_j, b_i, b_j are basis elements for system A, B accordingly.

The physical interpretation is given below. Suppose we have physical systems A and B, whose joint state is described by a density operator ρ_{AB}. Then, the density matrix for the subsystem A after ignoring the subsystem B is given by

$$\rho_A = \mathrm{tr}_B\left(\rho_{AB}\right).$$

As an example, if we apply the partial trace operator to a product state we get, unsurprisingly,

$$\mathrm{tr}_B\left(\rho_A \otimes \rho_B\right) = \rho_A.$$

In this case, we would say that we are "tracing out" system B.

Purification

Now, we have the tool for showing how one could embed a mixed state as a subsystem of a pure state with more qubits. Let ρ be a n-qubit mixed state:

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

We will then "embed" the mixed state into a $(2n)$-qubit pure state $|\psi\rangle$. That is, we will define a state $|\psi\rangle$ such that tracing out the n of its qubits leaves the state ρ. To do this, we concatenate each pure state $|\psi_i\rangle$

with the computational basis $|i\rangle$ and make its amplitude exactly the square root of its probability in the original mixed state.

$$|\psi\rangle \coloneqq \sum_{i\in\{0,1\}^n} \sqrt{p_i}\, |\psi_i\rangle \otimes |i\rangle \,.$$

Let B be the system consisting of the last n qubits. Tracing out B, we get the density matrix:

$$\begin{aligned}
\operatorname{tr}_B\left(|\psi\rangle\langle\psi|\right) &= \operatorname{tr}_B\left(\left(\sum_i \sqrt{p_i}\,|\psi_i\rangle \otimes |i\rangle\right)\left(\sum_i \sqrt{p_i}\,|\psi_i\rangle \otimes |i\rangle\right)^\dagger\right) \\
&= \operatorname{tr}_B\left(\sum_{i,j} \sqrt{p_i p_j}\,(|\psi_i\rangle \otimes |i\rangle)\cdot(|\psi_j\rangle \otimes |j\rangle)^\dagger\right) \\
&= \operatorname{tr}_B\left(\sum_{i,j} \sqrt{p_i p_j}\,(|\psi_i\rangle\langle\psi_i| \otimes |i\rangle\langle j|)\right) \\
&= \sum_{i,j} \sqrt{p_i p_j}\,\operatorname{tr}_B\left(|\psi_i\rangle\langle\psi_j| \otimes |i\rangle\langle j|\right) && \text{(Linearity of partial trace)} \\
&= \sum_{i,j} \sqrt{p_i p_j}\,\left(|\psi_i\rangle\langle\psi_j|\right)\cdot \operatorname{tr}\left(|i\rangle\langle j|\right) && \text{(Definition of partial trace on the computation basis)} \\
&= \sum_i p_i\left(|\psi_i\rangle\langle\psi_i|\right) \,, && \text{(Trace of the outer product of orthogonal vectors is 0)}
\end{aligned}$$

which is precisely the mixed state that we wanted to embed in the first place. We say that $|\psi\rangle$ is a *purification* of ρ.