Lecture: Quantum Information

Transcribed by: Crystal Noel and Da An (Chi Chi)

November 10, 2016

1 Final Project Information

Find an issue related to class you are interested in and either: read some papers and synthesize your understanding in the context of the question or develop an independent interest related to something from class and translate into the language of quantum information.

Final product should be a paper and short presentation (either slides or chalk talk). A sign up will be made available to avoid overlapping topics.

2 Mixed Quantum States

Density matrix $\rho = \sum_i p_i \left|\Psi_i\right\rangle \left\langle\Psi_i\right|$ with probability p_i that the system is in state $\left|\Psi_i\right\rangle$. ρ can describe either a pure state or a mixture of pure states. Consider a system coupled to the environment; when the environment is traced out, the system is likely left in a mixed state. For example, consider the following two mixed states:

$$\rho = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| + \frac{1}{2}\left|1\right\rangle\left\langle 1\right|$$

$$\sigma = \frac{1}{2}\left|+\right\rangle\left\langle +\right| + \frac{1}{2}\left|-\right\rangle\left\langle -\right|$$

There is no measurement that can distinguish between these two states. In matrix notation of the $\left|0\right\rangle, \left|1\right\rangle$ basis:

$$\rho = \frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = \tfrac{1}{2}\mathbb{1}$$

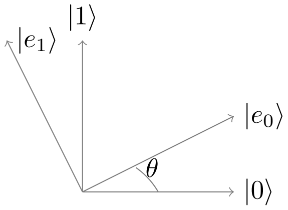
$$\sigma = \frac{1}{2}\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\frac{1}{\sqrt{2}}\\-\frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = \tfrac{1}{2}\mathbb{1}$$

The density matrices are identical, so the result of measurement can be written in terms of the density matrix. If the measurement basis is $\{\left|e_j\right\rangle\}$ then the probability of measurement result j can be re-written in terms of the density matrix:

$$p[j] = \sum_i |\left\langle e_j|\Psi_i\right\rangle|^2 = \sum_i p_i \left\langle e_j|\Psi_i\right\rangle\left\langle\Psi_i|e_j\right\rangle = \left\langle e_j\right|\rho\left|e_j\right\rangle$$

therefore the density matrix contains the measurement information.

Consider a measurement in the $\{e_0, e_1\}$ basis as shown here:



The probability of measuring 0 is:

$$p[0] = \frac{1}{2}\cos^2\theta + \frac{1}{2}\sin^2\theta = \frac{1}{2}$$

The measurement does not depend on which orthogonal basis you use. The density matrix is a notation that shows what information is available to extract.

3 Properties of the Density Matrix

- Hermitian
- $Tr(\rho) = 1$
- $\rho_{jj} = P$[outcome j when measuring in the standard basis]
- $\rho \geq 0$ (all eigenvalues are positive)
- for eigenvectors $\{e_j\}$ and eigenvalues λ_j:
  $\langle e_j| \rho |e_j\rangle = \lambda_j = P$[outcome j when measuring in $\{e_j\}$ basis]

4 Distinguishing density matrices

Suppose we have two density matrices $\rho \neq \sigma$. How can we distinguish them? Diagonalize $\rho - \sigma$, then measure in the new basis $\{e_j\}$.

$$\rho - \sigma = E\Lambda E^*$$

We measure ρ and its associated probability distribution, D_ρ, and also measure σ and D_σ. Then we can measure the difference between the distributions, which we call the total variation distance:

$$\frac{1}{2}\sum_j |D_\rho(j) - D_\sigma(j)|$$

$$|D_\rho - D_\sigma| = \frac{1}{2}\sum_j |\lambda_j| = ||\rho - \sigma||_{tr}$$

where $||M||_{tr}$ is the trace norm of the matrix M, which is the absolute value of the sum of the eigenvalues. Next, show that this is the best possible measurement to distinguish the two states. Suppose we chose a different basis $\{f_j\}$. Then the distance achieved is:

$$||\rho - \sigma||_{tr} = \frac{1}{2}\sum_j | \langle f_j| \rho |f_j\rangle - \langle f_j| \sigma |f_j\rangle |$$

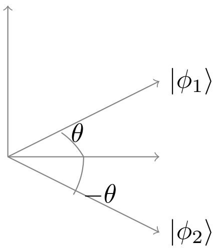
$$= \frac{1}{2}\sum_j | \langle f_j| A |f_j\rangle | = \frac{1}{2}\sum_j | \langle f_j| \sum_i \lambda_i |e_i\rangle \langle e_i|f_j\rangle$$

$$\leq \frac{1}{2}\sum_j \sum_i |\lambda_i|| \langle f_j|e_i\rangle |^2 \leq \frac{1}{2}\sum_i |\lambda_i|$$

where $A = \rho - \sigma$

5 Understanding Von Neumann Entropy

Start with a classical probability distribution: X. The classical entropy $H(X)$ measures degree of uncertainty in p_i. If the classical entropy is small, it means the distribution is narrowly peaked and predictable. For a quantum distribution p_i over states $|\Psi_i\rangle$. If the quantum entropy is small, then either p_i is focused around a couple of states or the states $|\Psi_i\rangle$ are nearly indistinguishable quantum states. For example:



$$|\phi_1\rangle = \tfrac{1}{2}(\cos\theta\,|0\rangle + \sin\theta\,|1\rangle)$$
$$|\phi_2\rangle = \tfrac{1}{2}(\cos\theta\,|0\rangle - \sin\theta\,|1\rangle)$$

If θ is small, these states should have low entropy since they would be nearly indistinguishable.

$$\rho = \frac{1}{2}|\phi_1\rangle\langle\phi_1| + \frac{1}{2}|\phi_2\rangle\langle\phi_2|$$

$$= \frac{1}{2}\begin{pmatrix}\cos\theta \\ \sin\theta\end{pmatrix}\begin{pmatrix}\cos\theta & \sin\theta\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\cos\theta \\ -\sin\theta\end{pmatrix}\begin{pmatrix}\cos\theta & -\sin\theta\end{pmatrix}$$

$$= \begin{pmatrix}\cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta\end{pmatrix} + \begin{pmatrix}\cos^2\theta & -\cos\theta\sin\theta \\ -\cos\theta\sin\theta & \sin^2\theta\end{pmatrix}$$

$$= \begin{pmatrix} \cos^2\theta & 0 \\ 0 & \sin^2\theta \end{pmatrix}$$

Now that ρ is diagonalized, we can consider the classical entropy as the Von Neumann Entropy:

$$S(\rho) = H(\cos^2\theta)$$

which for small θ is close to zero. For any ρ, we can diagonalize and write in a mutually orthogonal basis $|e_j\rangle$ with probability λ_j. This eliminates the indistinguishability problem and classical entropy is used:

$$S(\rho) = H(\{\lambda_j\})$$

6 Quantum bit commitment

A scheme for secure quantum bit commitment was proposed by Bennett and Bassard in 1984. Two parties, Alice and Bob wish to use the protocol as part of an auction. In stage one, Alice must commit to a bid without Bob knowing what that bid is. She sends an encoded version of her bid (an encoded bit) to Bob. In the second stage, Alice sends the unique decoding information and Bob can reveal the bid by decoding the message he received in stage one.

Classically, the first bit from Alice would be encrypted by RSA, for example. In stage two, Alice sends Bob the unique decoding information.

In a quantum protocol, we consider two cases. Case one: Alice wishes to send a 0 as the first bit. She flips a coin and sends either the quantum state $|0\rangle$ or $|1\rangle$ with equal probability. Case two: Alice wishes to send a 1 as the first bit. She flips a coin and sends either the quantum state $|+\rangle$ or $|-\rangle$ with equal probability. In either case, Bob is left with the same density matrix, or the same information and he cannot decode the bit without more information from Alice. In stage two, Alice reveals which bit she intended and which quantum state she sent. If Bob measures his state in the correct basis, he will confirm her information.

The scheme suggests unconditionally secure information, but this is impossible information theoretically.

7 Purification

Purification is the concept that prevents this impossibility of quntuam bit commitment to be realized. It refers to the fact that every mixed state acting on finite-dimensional Hilbert spaces can be viewed as the reduced state of some pure state. Let ρ_A be a density matrix acting on a Hilbert space H_A of finite dimension n. Then there exist a Hilbert space H_B and a pure state $|\psi\rangle \in H_A \otimes H_B$ such that the partial trace of $|\psi\rangle\langle\psi|$ with respect to H_B, $\mathrm{tr}_B |\psi\rangle\langle\psi| = \rho_A$, and so $|\psi\rangle$ is the purification of ρ_A.

In more relevant terms to the quantum bit commitment, let us have $|\psi\rangle \in H_A \otimes H_B$ and $|\phi\rangle \in H_A \otimes H_B$, with density matrices ρ_B and σ_B associated with

$|\psi\rangle$ and $|\phi\rangle$, respectively. Then when you trace out A, we get that $\rho_B = \sigma_B$ through the Schmidt decomposition, which means that $|\psi\rangle$ can be mapped to the state $|\phi\rangle$ by a unitary transformation, $U_A \otimes I$. What this implies for the quantum bit commitment is that Alice does not actually need to commit to a bit, as she can simply perform a unitary transformation on her bit and change the state while keeping Bob's bit undisturbed.

8 Fidelity of Quantum States

There are different notions of measuring difference between quantum states. As we have seen earlier, the trace norm, $||\rho - \sigma||_{tr}$, as a measurement using the density matrices of the states. In this section, we talk about an alternate scheme called fidelity, which can be used with pure states and mixed states. For two pure states with density matrices $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$, the fidelity is defined as $F(\rho, \sigma) = |\langle\phi|\psi\rangle|$ and it describes the overlap between the states. For two mixed states, Uhlmann's theorem generalizes the statement based on their purifications. Properties that come from Uhlmann's theorem are that the fidelity is symmetric in its arguments, $F(\rho, \sigma) \in [0, 1]$, and $F(\rho, \sigma) = 1$ iff $\rho = \sigma$. The fidelity is related to the trace norm as

$$1 - F(\rho, \sigma) \leq ||\rho - \sigma||_{tr} \leq \sqrt{1 - F(\rho, \sigma)^2}$$

where the upper bound inequality becomes an equality when ρ and σ are pure states.

9 Holevo's Theorem

Let us have some classical random variable $X = x_1, ..., x_n$, and through a wire, we want to communicate $Y = y_1, ..., y_n$. Then Holevo's Theorem states that

$$I(X : Y) \leq S(\rho) \leq m$$

where $I(X : Y)$ is the mutual information, $S(\rho)$ is the Von Neumann entropy, $\rho = \sum_x p_x \rho_x$ is the average density matrix being sent, and m denotes the number of qubits.

The mutual information is a measure of the goodness, i.e. how much information Alice is able to transfer to Bob. It is defined as

$$I(X : Y) = H(X) + H(Y) - H((X, Y))$$

where $H(X)$ is the classical entropy. For example, the ideal situation is if $X = Y$, then

$$I(X : Y) = H(X) + H(X) - H(X) = H(X)$$

The worst case scenario is if X and Y are independent, meaning

$$I(X:Y) = H(X) + H(Y) - [H(X) + H(Y)] = 0$$

There is another measure of information transfer other than mutual information: what is the probability that Bob has the correct information? This method generates a better bound, the Nayak bound, than Holevo's Theorem.

$$\mathop{\mathbb{E}}_{x} P[X = Y] = \sum_{x} p_x[Y[p_x] = X] \leq \frac{2^m}{2^n}$$

10 Quantum PCP Conjecture

Before diving in to the details of the conjecture, we first provide some useful background.

10.1 Monogamy of Entanglement

Imagine a collection of 3 qubits, $|\psi_A\rangle, |\psi_B\rangle, |\psi_C\rangle$. The monogamy property of entanglement states that if $|\psi_A\rangle$ and $|\psi_B\rangle$ are maximally entangled, i.e. they form a Bell state $|\Psi_A B\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, then they cannot be quantumly correlated at all with the their qubit, $|\psi_C\rangle$. This may be easily generalized to more particle systems. It may be helpful to think that the more correlated the two entangled states are, the more likely they are to form a tensor product with the rest of the system.

10.2 Classical PCP Theorem

This theorem states that the maximum fraction of satisfiable constraints of a constraint satisfaction problem is NP-hard to approximate within some constant factor. In mathematics terms, for some constraint satisfaction problem, $f(x_1, ..., x_n) = C_1 \wedge C_2 \wedge ... \wedge C_m$, the following is an NP-hard decision problem:

$$\exists x : \text{all constraints are satisfied}$$

$$\text{or } \forall x : \text{at least } \alpha\text{m constraints violated, where } \alpha < 1$$

Note that this is in contrast to the satisfiability problem, which is NP-complete, and stated for some constraint satisfaction problem, $f(x_1, ..., x_n) = C_1 \wedge C_2 \wedge ... \wedge C_m$, the following is an NP-easy:

$$\exists x : \text{all constraints are satisfied}$$

$$\text{or } \forall x : \text{at least 1 constraint is violated}$$

10.3 Quantum PCP Conjecture

Before moving to the quantum analog of the above classical PCP theorem, we first note the quantum satisfiability problem, which is QMA-complete. The statement of the problem is as follows: let us have some entanglement among n particles in the ground states of a local Hamiltonian, $H_L = H_1 + ... + H_m$. Given constants a and b, we ask if

$$\exists \left|\psi\right\rangle : \left\langle\psi\right| H_L \left|\psi\right\rangle \leq a$$

$$\text{or } \forall \left|\psi\right\rangle : \left\langle\psi\right| H_L \left|\psi\right\rangle \geq b$$

where $|b - a| = 1/poly(n)$. We now move to the quantum analog of the PCP theorem, which is the Quantum PCP Conjecture. Suppose we have a Hamiltonian that is D-regular (or D-local) for D sufficiently large; this can be thought of as a system of n particles with each particle entangled with D other particles. Then the claim is that

$$\exists \sigma, \text{a product state} : \mathop{\mathbb{E}}_{j,k \in E_0} ||\rho^{j,k} - \sigma^{j,k}|| \leq \mathcal{O}(\frac{d^2 \log d}{D})$$

where $\rho^{j,k}$ are the states restricted to the ground states to H_L. This claim has been shown for D large, but it remains to be shown true for D small.