Lecture Notes

November 8, 2002

CS 294-4, Quantum Computation

Lecturer: Umesh Vazirani

Scribes: Kevin Lacker and Brian Carnes

Edited by Ashwin Nayak, May 2003

1. Review

In general, a quantum system exists in a mixture of pure states. Say that in this mixture, the state $|\Phi_i\rangle$ has a probability p_i of occurring. All accessible information about this mixed state is encoded in its density matrix ρ:

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

Properties of the density matrix:

- $\mathrm{tr}(\rho) = 1$
- ρ is Hermitian
- ρ's eigenvalues are nonnegative
- Mixed states with density matrices ρ and σ can be distinguished with probability $\| \rho - \sigma \|_{\mathrm{tr}}$
- When measuring in the standard basis, ρ_{jj} is the probability of outcome j.

Diagonalizing ρ gives a classical mixture whose density matrix is ρ. We define the Von Neumann entropy $S(\rho)$ to be the Shannon entropy of this classical mixture.

2. Bipartite States

Consider a space $\mathcal{H}_A \otimes \mathcal{H}_B$, where the qubits in the first space are controlled by player A, and the remaining qubits (those corresponding to $\mathcal{H}_B$ are controlled by player B. Let $K = \dim \mathcal{H}_A$, and $L = \dim \mathcal{H}_B$, with $K \leq L$. In general you can look at a bipartite state as a joint state $|\Phi_{AB}\rangle$ which is entangled. Typically one writes this as

$$|\Phi_{AB}\rangle = \sum_{i=1}^{K} \sum_{j=1}^{L} m_{ij} |a_i\rangle |b_j\rangle$$

where the $|a_i\rangle$ form an orthonormal basis of $\mathcal{H}_A$ and the $|b_j\rangle$ form an orthonormal basis of $\mathcal{H}_B$.

There is a much nicer representation for this state, called its Schmidt decomposition. There are special orthonormal bases $\{|e_i\rangle\}$ for $\mathcal{H}_A$ and $\{|f_i\rangle\}$ for $\mathcal{H}_B$ such that:

$$|\Phi_{AB}\rangle = \sum_{i=0}^{K} \lambda_i |e_i\rangle|f_i\rangle$$

If A measures her qubits, B is left with some mixed state ρ_B. The only information about $|\Phi_{AB}\rangle$ that is available to B is the information contained in ρ_B. If A measures her qubits in the Schmidt basis $|e_i\rangle$, then B has the mixed state in which each $|f_i\rangle$ occurs with probability $|\lambda_i|^2$. Thus, ρ_B is diagonal in the $|f_i\rangle$ basis. The converse is also true: if $\rho_B = \sum_k p_k |g_k\rangle\langle g_k|$, in diagonal form, then we may choose $\{|g_k\rangle\}$ as our Schmidt basis for $\mathcal{H}_B$. This in fact gives us a proof of the existence of the Schmidt decomposition, as below.

Note that

$$\rho_B = \sum_{i,j_1,j_2} m_{ij_1} m^*_{ij_2} |b_{j_1}\rangle\langle b_{j_2}| = \sum_k p_k |g_k\rangle\langle g_k|.$$

In particular, $\langle g_k|\rho_B|g_\ell\rangle = \delta_{k\ell} p_k$. ($\delta_{k\ell} = 1$ if $k = \ell$, and 0 otherwise.) To prove the Schmidt decomposition theorem, it suffices to show the following: When the $\mathcal{H}_B$ part of the state $|\Phi_{AB}\rangle$ is expressed in the $\{|g_k\rangle\}$ basis as $\sum_k \alpha_k |h_k\rangle|g_k\rangle$, then the states $|h_k\rangle$ are orthonormal, and $|\alpha_k|^2 = p_k$. (Note that for an arbitrary basis for $\mathcal{H}_B$, the states $|h_k\rangle$ need not be orthonormal.) In other words, if we measure the second part of the state in the $|g_k\rangle$ basis, the residual states $|h_k\rangle$ are orthonormal, and occur with probability p_k. Since measuring ρ_B in this basis gives outcome $|g_k\rangle$ with probability p_k, we have $|\alpha_k|^2 = p_k$. Now, the residual states are given by:

$$|h_k\rangle = (1/\sqrt{p_k}) \sum_{ij} m_{ij} |a_i\rangle\langle g_k|b_j\rangle.$$

We may now verify that these are orthonormal:

$$\begin{aligned}
\langle h_\ell|h_k\rangle &= (1/\sqrt{p_k p_\ell}) \sum_{i,j_1,j_2} m_{ij_1} m^*_{ij_2} \langle b_{j_2}|g_\ell\rangle\langle g_k|b_{j_1}\rangle \\
&= (1/\sqrt{p_k p_\ell}) \langle g_k|\rho_B|g_\ell\rangle \\
&= \delta_{k\ell}.
\end{aligned}$$

We will now see a neat application of the Schmidt decomposition theorem.

Theorem 1 *Consider two bipartite states, $|\Phi_{AB}\rangle$ and $|\Psi_{AB}\rangle$. For each of these states there is a corresponding density matrix that results when A measures her bits. Denote these matrices as ρ_B and σ_B respectively. Suppose that $\rho_B = \sigma_B$. Then there exists a unitary transformation $U_A : \mathcal{H}_A \to \mathcal{H}_A$ such that*

$$(U_A \otimes I_B)|\Phi_{AB}\rangle = |\Psi_{AB}\rangle \quad (1)$$

Proof: Let $\rho_B = \sigma_B = \sum_i p_i |f_i\rangle\langle f_i|$. From the preceding discussion, we may write the Schmidt decomposition of the bipartite states as:

$$|\Phi_{AB}\rangle = \sum_i \sqrt{p_i}\, |e_i\rangle|f_i\rangle \quad (2)$$

$$|\Psi_{AB}\rangle = \sum_i \sqrt{p_i}\, |e'_i\rangle|f_i\rangle. \quad (3)$$

Since $\{|e_i\rangle\}$ and $\{|e'_i\rangle\}$ are two orthonormal bases, there is a unitary transformation that maps one to the other, and the theorem follows. ∎

This theorem shows that quantum bit commitment is impossible. Bit commitment is a protocol wherein A commits to a bit that B cannot see, but A can provide a key later to prove what bit it was. The two requirements of bit commitment, are that it be "sealing" and "binding":

- (**sealing**) B gets no information about the bit during the commitment, and
- (**binding**) A cannot change her mind about her chosen bit after the commitment.

Classically, bit commitment is possible up to a degree of difficulty, given the existence of one-way functions. The idea of quantum bit commitment is to use the laws of quantum computation to enforce the two requirements. Specifically, there must be two bipartite states, $|\Phi^0_{AB}\rangle$ and $|\Phi^1_{AB}\rangle$ (which are the joint states at the end of the commitment phase, corresponding to the value of the bit committed), such that:

- B cannot distinguish between his part of the two states $|\Phi^0_{AB}\rangle$ and $|\Phi^1_{AB}\rangle$, and
- A cannot switch from $|\Phi^0_{AB}\rangle$ to $|\Phi^1_{AB}\rangle$ (or vice-versa) by a local operation on her part of the state.

But the theorem above states that this is impossible.

This theorem can be generalized to say that if B gets only ϵ information, then A can switch with only some small chance of getting caught. So this method of bit commitment is not useful. What one can do is have A deposit a quantum state with B, and ask B not to look. B can get information from this state, but A will be able to tell if B looked or not. This is called quantum bit escrow, which is completely impossible classically.