Lecture Notes

November 8, 2002

CS 294-4, Quantum Computation

Lecturer: Umesh Vazirani

Scribes: Kevin Lacker and Brian Carnes

1. Review

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

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

Properties of the density matrix:

- $Tr(\rho) = 1$
- ρ is Hermitian
- ρ's eigenvalues are nonnegative
- Mixed states with density matrices ρ and σ can be distinguished with probability $||\rho - \sigma||_{Tr}$
- 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 classical entropy of this classical mixture.

2. Bipartite States

Consider a space $\mathcal{H}_A \otimes \mathcal{H}_B$, where the first K bits are controlled by player A, and the last L bits are controlled by player B. Without loss of generality we say $K \leq L$. In general you can look at a bipartite state as a joint state $|\Phi_{AB}\rangle$ which is entangled. Typically one writes this as

$$|\Phi_{AB}\rangle = \sum_{i=1}^{K} \sum_{j=1}^{L} m_{ij} |a_i\rangle |b_j\rangle \tag{2}$$

where the $|a_i\rangle$ are a basis of $\mathcal{H}_A$ and the $|b_j\rangle$ are a basis of $\mathcal{H}_B$.

The Schmidt decomposition is much nicer. There are special orthonormal bases $|e_i\rangle \in \mathcal{H}_A$ and $|f_i\rangle \in \mathcal{H}_B$ such that:

$$|\Phi_{AB}\rangle = \sum_{i=0}^{K} \lambda_i |e_i\rangle |f_i\rangle \tag{3}$$

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.

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*

$$(U_A \otimes I_B)|\Phi_{AB}\rangle = |\Psi_{AB}\rangle \tag{4}$$

Proof: Write the Schmidt decompositions of both bipartite states.

$$|\Phi_{AB}\rangle = \sum_i \lambda_i |e_i\rangle |f_i\rangle \tag{5}$$

$$|\Psi_{AB}\rangle = \sum_i \lambda'_i |e'_i\rangle |f'_i\rangle \tag{6}$$

But since $\rho_B = \sigma_B$, $f_i = f'_i$ and $|\lambda_i| = |\lambda'_i|$. The existence of an appropriate U_A follows immediately.

■

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, called "sealing" and "binding", are that:

- B gets no information during the commitment
- A cannot change her mind about her chosen bit

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 $|\Phi^1_{AB}\rangle$, such that:

- B cannot distinguish $|\Phi^0_{AB}\rangle$ from $|\Phi^1_{AB}\rangle$
- A cannot switch $|\Phi^0_{AB}\rangle$ to $|\Phi^1_{AB}\rangle$

But our theorem 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 change 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.

3. Quantum Communication

Suppose we have a quantum channel over which we can send n entangled qubits. How much information can be sent over this quantum channel?

In the problem of quantum communication, we have an m-bit random variable $X = x_1 x_2 \cdots x_m$ which we want to send across the channel. Our general procedure will be to encode x into the n-dimensional quantum state $|\Phi_x\rangle$ and send this across the channel. The person on the other side adds an ancilla to get $|\Phi_x\rangle|0^{m-n}\rangle$, and then measures in some basis to get an m-bit random variable Y. We would like for Y to be close to X in some way.

One measure of how close X and Y are is the mutual information, denoted by $I(X:Y)$, defined as

$$I(X:Y) = H(X) + H(Y) - H((X,Y)) \tag{7}$$

Example: $X = Y$

$$\begin{aligned} I(X:Y) &= H(X) + H(X) - H((X,X)) && (8)\\ I(X:Y) &= H(X) + H(X) - H(X) && (9)\\ I(X:Y) &= H(X) && (10) \end{aligned}$$

Example: X and Y are independent

$$\begin{aligned} I(X:Y) &= H(X) + H(Y) - H((X,Y)) && (11)\\ I(X:Y) &= H(X) + H(Y) - (H(X) + H(Y)) && (12)\\ I(X:Y) &= 0 && (13) \end{aligned}$$

Theorem 2 (Holevo) *If ρ is the density matrix of the mixed state sent across the channel, then*

$$I(X:Y) \leq S(\rho) \tag{14}$$

Corollary:

$$I(X:Y) \leq n \tag{15}$$

To understand ρ, let ρ_x denote $|\Phi_x\rangle\langle\Phi_x|$, and p_x denote $Pr[X = x]$. Then

$$\rho = \sum_x p_x \rho_x \tag{16}$$

So if X is uniform and $Y = X$, then $m \leq n$. Of course, this is no better than we can achieve classically. A similar theorem is true if we allow entanglement.

The proof of the above is extremely difficult. A related statement is much simpler to prove:

Theorem 3 (Nayek) *If X is a m bit binary string, we send it using n qubits, and decode it via some mechanism back to an m bit string Y, then our probability of correct decoding is given by*

$$Pr[X = Y] \leq \frac{2^n}{2^m} \tag{17}$$

This is "really bad".

Proof: Say x gets mapped to $|\phi_x\rangle$. Consider the message space as being a $C_2^{\otimes n}$ subspace of the full decoding space. So each $|\phi_{x_0}\rangle$ is mapped to some $|e_{x_0}\rangle$. Then, since the decoder is measuring in an orthonormal state

$$Pr[X = Y] = \frac{1}{2^m} \sum_x ||P_x|\phi_x\rangle||^2 \tag{18}$$

$$Pr[X = Y] = \frac{1}{2^m} \sum_{x,j} ||\langle\phi_x|e_{x,j}\rangle||^2 \tag{19}$$

$$Pr[X = Y] \leq \frac{1}{2^m} \sum_{x_j} ||Q|e_{x,j}\rangle||^2 \tag{20}$$

where Q is some projection back into the message space, $e \rightarrow \phi$. The reverse projection will be at least as long.

Now pick your basis $|f_1\rangle ... |f_{2^n}\rangle$ orthonormal to the message space.

So the projection equals

$$= \frac{1}{2^m} \sum_{x,j} \sum_i^{2^n} ||\langle e_{x,j}||f_i\rangle||^2 \tag{21}$$

$$= \frac{1}{2^m} \sum_i^{2^n} \sum_{x,j} ||\langle e_{x,j}||f_i\rangle||^2 \tag{22}$$

But $\sum_{x,j} ||\langle e_{x,j}||f_i\rangle||^2 = 1$ because the f_i were unit vectors. Leaving us with

$$= \frac{1}{2^m} \sum_i^{2^n} 1 \tag{23}$$

$$= \frac{2^n}{2^m} \tag{24}$$

■

4. Quantum Lower Bounds

Recall our task of finding a lower bound on searching for the solution to $f(x) = 1$, where $f : 1...N \rightarrow 0, 1$ and $f(j) = 1$ for some unique j.

The $\Omega(\sqrt{N})$ algorithm querying in superposition was found by initially considering a classical adversary, finding its weak point, then going quantum after that.

Now what about finding a lower bound when we have a Quantum adversary?

Consider input $Z_i = 000...1...000$ with a 1 in the ith position.

Suppose we have some fast Quantum algorithm that will work on a superposition of Z_i.

So the algorithm will take the superposition and an initially empty work and output register:

$$\sum_i |Z_i\rangle|0...0\rangle$$

and upon completion will produce:

$$\sum_i |Z_i\rangle|i, \text{junk}\rangle$$

where we'll see i or Z_i in either register with probability $\frac{1}{N}$. Consider measuring the work register; it does nothing before we start, but measuring at the end of the algorithm will collapse the input register into the appropriate Z_i. So the algorithm must change the input register. The registers start off unentangled, and end up perfectly entangled.

Consider the density matrices: Initially the nxn matrix is:

$$\begin{bmatrix} \frac{1}{N} & \cdots & \frac{1}{N} \\ \vdots & \ddots & \vdots \\ \frac{1}{N} & \cdots & \frac{1}{N} \end{bmatrix}$$

and ends up as

$$\begin{bmatrix} \frac{1}{N} & 0 & \cdots & 0 \\ 0 & \frac{1}{N} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \frac{1}{N} \end{bmatrix}$$

So, how entangled are the registers? The measure we use here is the sum of the off-diagonal entries. $S = \sum_{i \neq j} |\sigma_{i,j}|$. Initially, $S = N - 1$, and finally, $S = 0$.

Claim: S can only change by $O(\sqrt{N})$ at each step. So to accumulate the N entanglements takes $\sqrt{N}$ steps.

Justification of Claim: As the algorithm proceeds, consider the state ϕ_t in the following:

$$|\phi_t\rangle = \sum_{j,y} |j, y\rangle|\psi_{j,y}\rangle \tag{25}$$

$$\text{andsoforeach} \tag{26}$$

$$\sigma = \sum_{j,y} |\alpha_{j,y}|^2 |\psi_{j,y}\rangle\langle\psi_{j,y}| \tag{27}$$

So all this can do is change the jth row,column. By Cauchy-Schwartz, the sum is at most $\sqrt{N}$.