18.435 Lecture 13
October 16th, 2003

Scribed by: Eric Fellheimer

This lectured started with details about the homework 3:

Typo in Nielsen and Chuang: If you pick random x such that gcd(x, N) = 1, x < N and N is the product of m distinct primes raised to positive integral powers, and r is the order of x mod N, then the probability that r is even and $x^{r/2} \neq -1 \bmod N \geq 1 - \frac{1}{2^{m-1}}$. The book erroneously has the power of 2 as m opposed to m -1.

In exercise 5.20 : The book states at the bottom of the problem that a certain sum has value $\sqrt{\frac{N}{R}}$ when l is a multiple of N/r. The answer should actually be N/r when l is a multiple of N/r.

Also, there will be a test on Thursday, October 23rd
-Open books
-Open notes
-in class
-covers through Grover's algorithm, teleportation, and superdense coding

From last lecture:
We know that quantum circuits can simulate Quantum Turing Machines (QTM) with polynomial overhead.

Now we will look in the reverse direction: implementing a Turing machine to simulate a quantum circuit.

We will need to show that we can approximate any gate with a finite set of gates.

<u>Thm</u>: CNOT gates and one-qubit gates are universal for quantum computation

Proof:

We already know gates of the form $\begin{bmatrix} a & b & & \\ g & d & & \\ & & 1 & \\ & & & 1 \end{bmatrix}\begin{bmatrix} a & & b & \\ & 1 & & \\ g & & d & \\ & & & 1 \end{bmatrix}\begin{bmatrix} a & & & b \\ & 1 & & \\ & & 1 & \\ g & & & d \end{bmatrix}$ are sufficient, where $\begin{bmatrix} a & b \\ g & d \end{bmatrix}$ is a unitary matrix.

We know use the fact that:

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix}\begin{bmatrix} a & & b & \\ & 1 & & \\ g & & d & \\ & & & 1 \end{bmatrix}\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix} = \begin{bmatrix} a & & & b \\ & 1 & & \\ & & 1 & \\ g & & & d \end{bmatrix}$$

This reduces the proof to only finding the first 2 of the 3 matrices above. The first 2, however, can be considered single-qubit operations. So if we can construct arbitrary single qubit operations, our proof is complete. We now look at forming controlled T^2 gates with

$$T = \begin{bmatrix} e^{i\Phi_1} & \\ & e^{-i\Phi_1} \end{bmatrix} \text{ or } T = \begin{bmatrix} \cos(q) & -\sin(q) \\ \sin(q) & \cos(q) \end{bmatrix}$$

We now know:

$$\begin{bmatrix} e^{i\Phi_1} & \\ & e^{-i\Phi_1} \end{bmatrix}\begin{bmatrix} \cos(q) & -\sin(q) \\ \sin(q) & \cos(q) \end{bmatrix}\begin{bmatrix} e^{i\Phi_2} & \\ & e^{-i\Phi 2} \end{bmatrix}$$

give arbitrary determinant 1, unitary 2X2 matrices. Thus, our proof is complete.

We know suppose Alice and Bob share stat (1/2) (|0000> + |0101> + |1011> + |1110>) where Alice owns the first 2 qubits.

They can use this state to teleport Alice's 2 qubits to Bob. To do this, Alice must send Bob 4 classical bits.

Quantum linear optics as a means for computation

- suppose you have a probabilistic method of applying CNOT gates and you know when it has worked
- you can measure in the Bell basis
- you can de single qubit operations

We argue that this strange set of requirements actually allows universal computation

We want

$$s_1^{'} \otimes s_2^{'} \quad CNOT \quad s_1^{-1} \otimes s_1^{-2} \left|a,b\right\rangle = CNOT\left|a,b\right\rangle$$

We now want to know that for each a,b {X, Y, Z, I} there exists a', b' such that

$$s_{a'} \otimes s_{b'} \quad CNOT \quad s_a \otimes s_b = CNOT$$

Knowing that the Pauli matrices are self inverses, we get:

$$s_{a'} \otimes s_{b'} \quad = CNOT \quad s_a \otimes s_b \quad CNOT$$

$$CNOT\ s_x(1)\ CNOT = s_x(1) \otimes s_x(2)$$

$$CNOT\ s_x(2)\ CNOT = s_x(2)$$

$$CNOT\ s_z(1)\ CNOT = s_z(1)$$

Thus, we have:

$$CNOT\ s_y(1)\ CNOT = -i\, CNOT\, s_z(1) s_x(1)\, CNOT$$

$$CNOT\ s_y(1)\ CNOT = -i\, CNOT\, s_z(1)\ CNOT\ \ CNOT\, s_x(1)\, CNOT$$

$$CNOT\ s_y(1)\ CNOT = -i\, s_z(1)\ s_x(1) s_x(2)$$

$$CNOT\ s_y(1)\ CNOT = \ s_y(1)\ s_x(2)$$

We have shown that we can teleport through controlled not gates to use quantum linear optics as a means of quantum computation.

Adiabatic Quantum Computation

Physical systems have Hamiltonians H such that $\left\langle \Psi \mid H \mid \Psi \right\rangle$ = E is the energy of the system.

H is a Hermitian operator.

The wave function satisfies the Schrödinger Equation:

$$i\hbar \frac{d\left|\ \Psi\right\rangle}{dt} = H\left|\ \Psi\right\rangle$$

<u>Thm</u>: If you change the Hamiltonian sufficiently slowly, and start in the ground state, you remain in the ground state.

Here, "sufficiently slow" means T is proportional to 1/|g|^2, where g is the gap between first and second energy eigenvalues.

If we start in state H_{init} and end in H_{final}, H_{init} / H_{final} are sums of Hamiltonians involving no more than a few qubits.

Finally, there is a theorem which states that using this setup can be equated to using quantum circuits.