C/CS/Phys C191 Circuits, Randomized computation, Deferred measurements 10/02/07
Fall 2007 Lecture 11

1 Review of quantum circuit model

Recall that in the quantum circuit model we have n qubits that we can manipulate in the following ways:

1. Initialization: The qubits can be initialized to the state $|0^n\rangle$. Preparing a different input state $|x\rangle$, $x \in \{0,1\}^n$ can be done by flipping the required bits.
2. Universal set of gates: Certain sets of one- and two-qubit gates can approximate any constant dimensional unitary transformation sufficiently closely. For example, the CNOT gate together with all one qubit transformations (rotations on the Bloch sphere) forms a universal gate set.
3. Measurement of some (or all) of the qubits output by the quantum circuit. For example if $|\psi\rangle = \sum_x \alpha_x |x\rangle$ and we do a full measurement in the standard/computational basis, then we measure x with probability $|\alpha_x|^2$. If we only measure the first k bits of x, then the probability of measuring $z \in \{0,1\}^k$ is $\sum_{x:z \text{ is a prefix of} x} |\alpha_x|^2$. The resulting partially collapsed quantum state is, up to normalization, $\sum_{x:z \text{ is a prefix of} x} \alpha_x |x\rangle$.
4. Classical postprocessing of the measured value to get the solution to the problem being solved. Quantum computers are expensive and rare (!), so we would probably prefer to use classical processing as much as possible.

The size of a quantum circuit is the number of gates in the circuit. We are interested in finding *efficient* circuits for problems, i.e., circuits for which the total size of the circuit is polynomially bounded in the number of input bits. For example, a family of circuits of size $c \cdot n^5$ is good. But exponentially large – 2^n – circuits are bad.

2 Randomized computation

Many important classical algorithms are randomized. For example, the most common primality testing algorithm needs as input a random string which is then used to construct a test of whether the number is prime (see, e.g., ”primality test” in http://Mathworld.wolfram.com). (Note that a deterministic polynomial time algorithm was discovered in 2002 by Agrawal et al.)

Rabin-Miller Strong Pseudoprime test:

For odd integer n, let $n = 2^r s + 1$ with s odd, choose a random integer α, $1 \leq \alpha \leq n-1$. If $\alpha^s = 1 (\mathrm{mod}\, n)$ or $\alpha^{2^j s} = -1 (\mathrm{mod}\, n)$ for some $0 \leq j \leq r-1$, then n passes the test, i.e. it is prime. A true prime number will pass the test for all α. Thus this protocol can give us erroneous result for some random α (i.e. tell us that n is prime, when it isn’t), but with a small probability.

For each x, for most choices of α, the circuit computes the correct answer.

To simulate quantumly:

1. First create the corresponding reversible circuit with inputs x, α and ancilla 0’s.

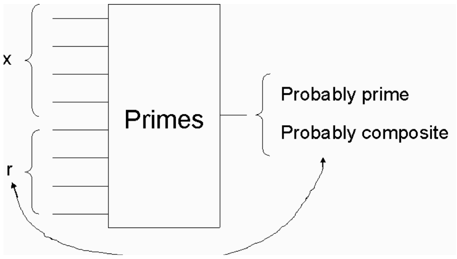

Figure 1: A circuit for primality testing which takes as additional input a random string α.

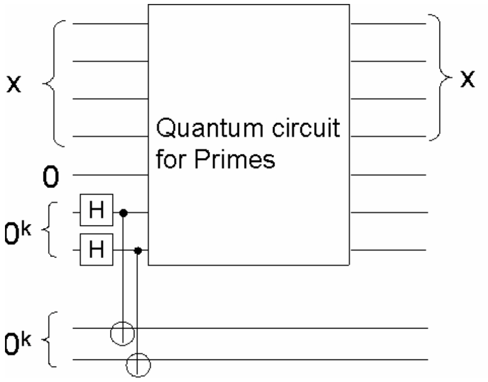

Figure 2: The corresponding quantum circuit; copying with a CNOT the qubits $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is equivalent to measuring them, giving a random string α.

2. To randomize α, feed each $|0\rangle$ qubit wire through a Hadamard gate, giving $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Immediately after applying the Hadamard gate, measure each qubit of α.

3. Instead of measuring the qubits of α, it is sufficient to copy (with CNOT gates) the outputs of the Hadamard gates into fresh qubits. For example, we change $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$ to $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Since they are entangled, measuring the bits into which we copied each computational basis state of α is equivalent to measuring the bits of α itself.

4. In fact, though, it doesn't matter whether we measure the fresh qubits before or after running the quantum circuit. In fact, we can delay their measurement arbitrarily long, or just avoid it altogether. This is known as the "principle of deferred measurement." Measurement is equivalent to entanglement of the system with its environment.

3 Deferred measurements

Another example of this principle of deferred measurement can be shown for teleportation. Figure 3 shows the usual teleportation circuit in which Alice (on left) performs the measurements of qubits 1 and 2, then sends the classical output of these measurements to Bob (on right). Figure 4 shows the equivalent circuit in which the measurements are done at the end, rather than in the middle. Instead of unitaries condition on the result of Alice's measurements, Bob makes controlled unitary operations on qubit 3. You can convince

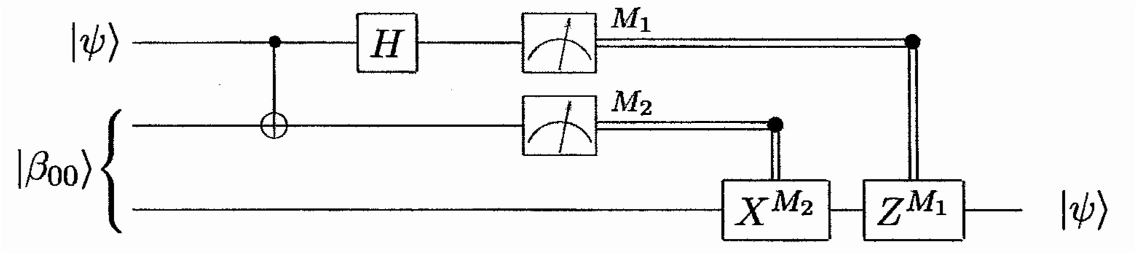

Figure 3: The usual teleportation circuit with measurement performed by Alice on qubits 1 and 2, who then sends the classical information from this to Bob who performs single qubit unitaries conditional on the results on qubit 3.

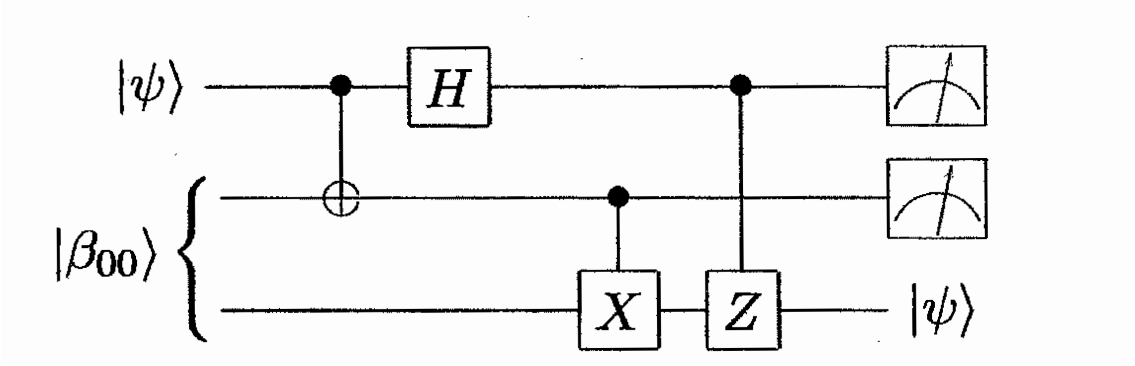

Figure 4: The deferrred measurement quantum teleportation circuit.

yourselves of the equivalence by writing out the states and actions of the measurements and controlled unitaries on then. The notation here is such that $|\beta_{00}\rangle = |\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$.