CS 221: Computational Complexity **Prof. Salil Vadhan**

Lecture Notes 26

May 3, 2010 **Scribe: Christopher Simmons**

1 Agenda

- The quantum model.
- **BPP** vs. **BQP**.
- Quantum fourier transform.

2 What is quantum computing?

Quantum computing is a hypothetical computational model based on quantum mechanics that seems to violate the strong Church-Turing thesis. One of the ways in which quantum computers seem to violate the thesis is that they can factor integers in polynomial time. In fact, there are even problems solvable in polynomial time by quantum computers that are not known to lie in the polynomial hierarchy. On the other hand, it is not known how to solve **NP**-complete problems in polynomial time on a quantum computer (the best known is a quadratic speedup over exhaustive search, which is already quite nontrivial), and many researchers conjecture that this is impossible (though there is not much formal evidence to this effect).

There has been substantial effort in trying to build quantum computers (motivated partly by the fact that factoring would enable breaking most public-key cryptography currently in use), but so far there has not been success in building a scalable quantum computer. It is unknown whether there is a fundamental physical barrier to scalable quantum computation.

We will develop quantum computation by analogy with classical, probabilistic computation.

Table 1: (Classical) probabilistic vs. quantum computation

	Probabilistic n-bit system	Quantum n-qubit system
State of system	$\phi = \sum_{s\in\{0,1\}^n} \alpha\|s\rangle \in \mathbb{R}^{2^n}$ $\alpha_s \geq 0$ $\sum_s \alpha_s = 1$	$\phi = \sum_{s\in\{0,1\}^n} \alpha_s\|s\rangle \in \mathbb{C}^{2^n}$ $\sum_s \|\alpha_s\|^2 = 1$
Interpretation	observe s w.p. α_s	if *measure*, observe s w.p. $\|\alpha_s\|^2$
Evolution	$\phi_{t+1} = M_t\phi_t$ for stochastic matrix M_t	$\phi_{t+1} = M_t\phi_t$ for *unitary* matrix M_t

A *stochastic matrix* M is one in which column is a probability distribution. This ensures that if $\phi \in \mathbb{R}^{2^n}$ is a probability distribution, then so is $M\phi$. A *unitary matrix* M is one where $\|M\phi\| = \|\phi\|$ for every complex vector ϕ. This ensures that if ϕ is a unit vector, then so is $M\phi$. (An equivalent characterization of unitarity is that the conjugate transpose of M is the inverse of M.)

3 Effect of cancellations

Consider a 1-qubit system evolving by the Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Case 0: $\underbrace{|0\rangle}_{\text{observe 0}} \mapsto^H \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{\text{observe random bit}}$

Case 1: $\underbrace{|1\rangle}_{\text{observe 1}} \mapsto^H \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{\text{observe random bit}}$

Case 2: $\underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{\text{observe random bit}} \mapsto^H \underbrace{|0\rangle}_{\text{observe 0}}$

Note that even though Case 2 is an equal superposition of Cases 0 and 1 (which we observe if measuring the initial state), after applying H there is cancellation between these two cases, and we do not observe a value of 1 even though we would have seen it in both Cases 0 and 1. This is like the famous 2-slit experiment, where if light is shined two appropriately placed slits simultaneously, there are points where no light is observed even though light would be observed there if either of the slits were closed.

An important point is that the cancellation only occurs if the quantum state is *not* measured before applying H. If we do measure the initial state, the state will collapse to either case zero or case one with equal probabilities. (In the 2-slit experiment, if detectors are placed at the slits, then light is again observed at the point of cancellation.)

More generally, if we measure the first qubit of quantum state $\phi = \sum_{s \in \{0,1\}^n} \alpha_s |s\rangle$, then the probability that we observe a zero is $\sum_{t \in \{0,1\}^{n-1}} |\alpha_{0\,t}|^2$, and the probability that we observe a one is $\sum_{t \in \{0,1\}^{n-1}} |\alpha_{1\,t}|^2$. If we observe a zero, then the state collapses to:

$$\phi' = \frac{\sum_t \alpha_{0\,t} |0\,t\rangle}{\sum_t |\alpha_{0\,t}|^2}$$

4 Probabilistic and Quantum Circuits

Now, to model *computation,* we do not allow the system to evolve by arbitrary $2^n \times 2^n$ matrices. Even in the case of probabilistic circuits, this would allow computing every function $f : \{0,1\}^n \to$

$\{0,1\}^n$ in one time step! Instead, our notion of computation is that it is proceeds by *local* operations, that affect only a constant number of bits at a time. We begin by describing what this means in the case of probabilistic computation.

Probabilistic Circuits. Let $g : \{0,1\}^2 \to \{0,1\}$ be a probabilistic binary gate. One can view it as a 2×4, stochastic matrix

$$G = \begin{pmatrix} \Pr[g(00)=0] & \Pr[g(01)=0] & \dots & \Pr[g(11)=0] \\ \Pr[g(00)=1] & \dots & & \Pr[g(11)=1] \end{pmatrix}.$$

Or, equivalently, as a linear operator, e.g. $G(|0\,0\rangle) = \Pr[g(0\,0)=0]|0\rangle + \Pr[g(0\,0)=1]|1\rangle$. If applying the gate g to the 1st and 3rd bits of an n-bit register and put the result in the 2nd bit, the evolution of the n-bit system is given by a $2^n \times 2^n$ stochastic matrix M induced by G as follows:

$$M(|s_1 \dots s_n\rangle) = |s_1\rangle G(|s_1\, s_3\rangle)|s_3 \dots s_n\rangle,$$

which we extend linearly to all of R^{2^n}. This computation is local; it deals with a constant amount of information at each step.

It can be shown that every probabilistic gate of $O(1)$ arity can be approximated by AND, OR, and NOT gates and a coin flip gate, which is why we usually don't talk about arbitrary probabilistic gates.

Quantum circuits. In *quantum* circuits, local operations are given by O(1)-qubit, *unitary* operations. For example, a 3-qubit operation is given by a $2^3 \times 2^3$, unitary matrix. Unitary matrices are always square and invertible; therefore, the number of qubits in the system must remain the same and the computation is always reversible.

There is a universal basis of unitary operations consisting of 2-qubit operations, but it is more useful to think of general unitary matrices.

5 Quantum computation

To compute a function $f : \{0,1\}^n \to \{0,1\}^n$,

1. Start with input $|x\rangle$ in input registers, s scratch registers set to $|0\rangle$, and m other output registers.

2. at the end of the circuit should be the same number of outputs as there are inputs. The outputs corresponding to the input registers and the scratch registers should end as their counterparts began (namely in state $|x\rangle|0^s\rangle$). If we measure the outputs corresponding to the m last registers at the end, we should get $f(x)$ with probability $\geq \frac{2}{3}$.

Note that this model only allows measurement at the end. However, it is known that computations where measurement is done in the middle can be simulated by ones where measurement is done at the end with only a small loss in efficiency.

Definition 1 $\mathbf{L} \in \mathbf{BQTIME}(T(n))$ *if* $\exists$ *a sequence of logspace-uniform quantum circuits* C_n *of size* $T(n)$ $\ni \forall x \in \{0,1\}^n$ *if we run* $C_n(|x\rangle|0\rangle^{S(n)+1})$. *and measure the last quibit, get* $\chi_L(x)$ *w.p.* $\geq \frac{2}{3}$. $\mathbf{BQP} = \cup_c \mathbf{BQTIME}(n^c)$.

6 Simulating classical computation by quantum computation

Lemma 2 *If $C : \{0,1\}^n \to \{0,1\}^m$ is a boolean circuit with s gates, there is a quantum circuit C' on $n+s+m$ registers with $2s+m$ quantum gates s.t. $\forall x \in \{0,1\}^n C'(|x\rangle|0\rangle^{s+m}) = |x\rangle|0\rangle^s|f(x)\rangle$.*

Let g be a classical gate with inputs x_1, x_2. To make it reversible, make it take an additional input y and output x_1, x_2, z, where $z = g(x_1, x_2) \oplus y$. The new gate g' is its own inverse. g' can be described by a $2^3 \times 2^3$ permutation matrix, and all permutation matrices are unitary.

To simulate C, we use the reversible versions of each of the gates of C, with a new scratch register for each one (which after applying the gates will contain the output value of the original gate). Now copy the last m scratch registers (which have the outputs of C) into the m output registers. Now apply the reversible version C again, but in reverse order, to return the scratch registers back to $|0\rangle^s$.

Corollary 3 $\mathbf{P} \subseteq \mathbf{BQP}$

Corollary 4 $\mathbf{BPP} \subseteq \mathbf{BQP} \leftarrow$ *use Hadamards to toss coins.*

7 Quantum Fourier Transform

Definition 5 (DFT) *For a function $f : \mathbb{Z}_M \to C$, the* discrete fourier transform *of f is $\hat{f} : \mathbb{Z}_m \to C$ given by*

$$\hat{f}(x) = \frac{1}{\sqrt{M}} \sum_{y \in \mathbb{Z}_m} f(y)\omega^{xy},$$

where $\omega = e^{2\pi i/M}$ is a primitive M'th root of unity.

Theorem 6 (QFT) *For $M = 2^m$, there is a quantum algorithm QFT using $O(m^2) = O(\log^2 M)$ quantum operations s.t. $\forall f : \mathbb{Z}_M \to C$,*

$$\mathrm{QFT}\left(\sum_{x \in \{0,1\}^m} f(x)|x\rangle\right) = \sum_{x \in \{0,1\}^m} \hat{f}(x)|x\rangle.$$

Motivation: Fast Fourier Transform. The FFT is based on the following recursive description of the FFT:

$$\begin{aligned}
\hat{f}(x) &= \frac{1}{\sqrt{M}} \sum_{y \in \mathbb{Z}_m} f(y)\omega^{xy} \\
&= \frac{1}{\sqrt{M}} \sum_{y \in \mathbb{Z}_{M/2}} f(2y)(\omega^2)^{xy} + \frac{\omega^x}{\sqrt{M}} \sum_{y \in \mathbb{Z}_{M/2}} f(2y+1)(\omega^2)^{xy} \\
&= \frac{1}{\sqrt{2}} \cdot \left(\frac{1}{\sqrt{\frac{M}{2}}} \sum_{y \in \mathbb{Z}_{M/2}} f_{\mathrm{even}}(y)(\omega^2)^{xy} + \frac{\omega^x}{\sqrt{\frac{M}{2}}} \sum_{y \in \mathbb{Z}_{M/2}} f_{\mathrm{odd}}(y)(\omega^2)^{xy} \right) \\
&= \begin{cases} \frac{1}{\sqrt{2}} \cdot \left(\widehat{f_{\mathrm{even}}}(x) + \omega^x \cdot \widehat{f_{\mathrm{odd}}}(x) \right) & \text{if } x < M/2 \\ \frac{1}{\sqrt{2}} \cdot \left(\widehat{f_{\mathrm{even}}}(x - M/2) - \omega^{x-M/2} \cdot \widehat{f_{\mathrm{odd}}}(x - M/2) \right) & \text{if } x \geq M/2, \end{cases}
\end{aligned}$$

where the last case uses the fact that $\omega^{M/2} = -1$.