6.896 Quantum Complexity Theory October 23rd, 2008

Lecture 15

Lecturer: Scott Aaronson

Today we continue to work with the class QMA.

1 Last Time

We defined QMA, the class of languages $L \subseteq \{0,1\}^*$ for which $\exists$ a polytime Quantum Turing machine Q, polynomial p such that $\forall x \in \{0,1\}^n$:
$x \in L \rightarrow \exists\ p(n)$-qubit witness $|\phi\rangle$ such that $Q(x, |\phi\rangle)$ accepts with probability $\geq \frac{2}{3}$
$x \notin L \rightarrow \forall\ |\phi\rangle$, $Q(x, |\phi\rangle)$ accepts with probability $\leq \frac{1}{3}$
The current known complexity inclusion relations are:

$$P \subseteq NP \subseteq MA \subseteq QCMA \subseteq QMA \tag{1}$$

$$P \subseteq BPP \subseteq BQP \subseteq QCMA \tag{2}$$

$$BPP \subseteq SZK \subseteq AM \tag{3}$$

$$BPP \subseteq MA \subseteq AM \tag{4}$$

2 Watrous' QMA protocol for Group Non-Membership

We started on Watrous' QMA protocol for Group Non-Membership. Given a black-group G, a subgroup $H \subseteq G$ (specified by its generators), and an element $x \in G$, the Group Non-Membership problem asks, is $x \in H$?

Being given a quantum superposition is quite different from being given a classical probability distribution. The QCMA vs. QMA question gets at just how different they are.

When we last left him, Arthur was given a superposition $|H\rangle$ by Merlin

$$|H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle \tag{5}$$

where $|H\rangle$ is not necessarily something Arthur could prepare in polynomial time himself, even if Merlin gave him a classical description of $|H\rangle$. Babai and Szemeredi showed how to sample a random element from the subgroup H in polynomial time, but that's *not the same* as being able to prepare a superposition over the elements.

Given $|H\rangle$, what can Arthur do? First of all, he doesn't actually know whether Merlin gave him $|H\rangle$ or whether he cheated and gave him some other state. But let's assume for the time being that Merlin gave him $|H\rangle$. How could he use that state to test whether $x \in H$?

Arthur computes $|Hx\rangle$, where

$$|Hx\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |hx\rangle \tag{6}$$

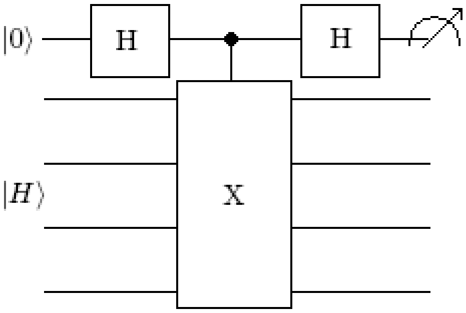

Figure 1: Circuit Diagram

After the above operation, the state becomes $|0\rangle|H\rangle + |1\rangle|Hx\rangle$. Arthur then Hadamards the first qubit and measures.

If $x \in H$, $|H\rangle = |Hx\rangle$ and $\langle H|Hx\rangle = 1$. So the state is $|0\rangle|H\rangle + |1\rangle|H\rangle = (|0\rangle + |1\rangle)|H\rangle$ and Hadamarding the first qubit always yields $|0\rangle$, because the $|0\rangle$ and $|1\rangle$ branches interfere with each other.

If $x \notin H$, Hx is disjoint from H, so $|H\rangle$ and $|Hx\rangle$ are orthogonal, and $\langle H|Hx\rangle = 0$. When Arthur prepares $|0\rangle|H\rangle + |1\rangle|Hx\rangle$, it's as if he's measured the first qubit. So when he Hadamards the first qubit and measures, he gets $|1\rangle$ with probability $\frac{1}{2}$.

However, one issue remains unaddressed: how can Arthur check that Merlin actually gave him $|H\rangle$ and not some other state? This is slightly tricky. Here's what Arthur can do. First, generate a (nearly) random element y of H (recall that Babai and Szemeredi showed that he can do this in polynomial time without help from Merlin). Then, letting $|H'\rangle$ be whatever state Merlin sent, Arthur prepares

$$|0\rangle|H'\rangle + |1\rangle|H'y\rangle \tag{7}$$

Arthur then Hadamards the first qubit and measures. Alternatively, Arthur could prepare a nearly random element y of G, then prepare

$$|0\rangle|H'\rangle + |1\rangle|H'y\rangle \tag{8}$$

then Hadamard the first qubit and measure. One can show that if theses tests give the expected results, then $|H'\rangle$ is either equal to $|H\rangle$ or else it's some other state that works just as well for Arthur's intended purpose. (To amplify the error probability, as usual, we can have Merlin send Arthur lots of copies of $|H\rangle$. Then Arthur can choose a different test to run on each copy.)

3 Upper bounds on QMA

It's easy to establish QMA $\subseteq$ NEXP as an upper bound: Arthur can simulate all the witness states Merlin could send to him.

Is QMA in EXP? It is, and we can show that.

We can think of what Arthur does as just performing a *measurement* on the witness state $|\phi\rangle$: a measurement that tells him whether to accept or reject. Arthur accepts iff the first qubit of

$$U(|\phi\rangle|0...0\rangle) \tag{9}$$

is measured to be $|1\rangle$, for some unitary U. But what does this mean, really?

$$|\phi\rangle = \alpha_1|1\rangle + ... + \alpha_N|N\rangle \tag{10}$$

$U|\phi\rangle =$

$$\begin{pmatrix} U_1 & 0...0 \\ U_2 & 0...0 \\ ... & ... \\ U_N & 0...0 \\ U_{N+1} & 0...0 \\ ... & ... \\ U_{2N} & 0...0 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ ... \\ \alpha_N \\ 0 \\ ... \\ 0 \end{pmatrix}$$

Arthur's acceptance probability thus equals

$$\sum_{i=1}^{M} |\langle U_i|\phi\rangle|^2 \tag{11}$$

$$= \sum_{i=1}^{M} \langle\phi|U_i\rangle\langle U_i|\phi\rangle \tag{12}$$

$$= \langle\phi| \left(\sum_{i=1}^{M} |U_i\rangle\langle U_i| \right) |\phi\rangle \tag{13}$$

where $i = 1, ..., M$ are the indices where ϕ_i are states that Arthur accepts.

Equivalently, there's a positive semidefinite matrix A such that this probability equals $\langle\phi|A|\phi\rangle$. This value is then just the largest eigenvalue of A. To maximize this value, we want ϕ to be the principle eigenvector, the eigenvector corresponding to this largest eigenvalue.

Thus, the problem reduces to this: given an exponentially-large matrix A for which we can compute each entry in exponential time, is $\lambda_{max}(A) \geq \frac{2}{3}$ or is $\lambda_{max}(A) \leq \frac{1}{3}$, promised that one of these is the case? We can solve this problem in EXP because it's just an exponential-size linear algebra problem.

Can we do better than that? We can. Let's solve it in PP.

Note that $Tr(A) = \sum_i \lambda_i$. Thus, if we're dealing with an n-qubit witness state,

$$(\lambda_{max})^d \leq Tr(A^d) = \sum_i \lambda_i^d \leq 2^n (\lambda_{max})^d \tag{14}$$

So $\lambda_{max} \leq \frac{1}{3}$ implies $Tr(A^d) \leq 2^n \left(\frac{1}{3}\right)^d$.

$\lambda_{max} \geq \frac{2}{3}$ implies $Tr(A^d) \geq (\frac{2}{3})^d$

Hence, by computing $Tr(A^d)$, we can estimate λ_{max}. But $Tr(A^d)$ is just a degree-d polynomial in the entries of A. It can be estimated in #P. Deciding whether it's above or below some threshold is a PP problem.

4 QMA-complete problems

Arguably, the single most famous discovery in theoretical computer science was NP-completeness: the fact that so many different optimization problems not only seem difficult, but capture the entire difficulty of the class NP. So it's natural to wonder: is there a theory of quantum NP-completness, analogous to the classical theory? It turns out there is, and it was created by Alexei Kitaev in 1999.

First, let's review classical NP-completeness. A problem is NP-complete if it's in NP and every other NP problem can be reduced to it. It's clear, almost by definition, that NP-complete problems exist. For example, "given a polytime Turing machine M, is there an input that causes M to accept?"

So the great discovery was not that NP-complete problems exist, but that many natural problems are NP-complete. The one that started the ball rolling was 3SAT, the problem of whether a boolean function of the AND of OR clauses of three variables each can be satisfied. We can prove 3SAT is NP-complete by taking Circuit-SAT (the problem of whether a boolean circuit has a satisfying assignment) and creating a 3CNF clause to check for each AND/OR/NOT gate to see whether it computed correctly.

What's a problem that's QMA-complete essentially by definition? It will have to be a promise problem:

Given a polytime Quantum Turing machine Q, is $max_{|\phi\rangle}\Pr[Q(|\phi\rangle)$ accepts$] \geq \frac{2}{3}$ or $\leq \frac{1}{3}$, promised that one is the case?

A more "natural" QMA-complete problem is the problem of k-local Hamiltonians:

Given 2-outcome measurements $E_1, ..., E_M$, each of which acts on at most k qubits (out of n), does there exist an n-qubit state $|\phi\rangle$ such that $\sum_{i=1}^{M}\Pr[E_i(|\phi\rangle)$ accepts$] \geq b$, promised that this sum is either $\geq b$ or $\leq a$ where b and a differ by $b - a = \Omega(\frac{1}{poly(n)})$?

The Cook-Levin Theorem proved that the boolean satisfiability problem SAT is NP-complete by simulating a Turing machine and checking to see if the simulation was run properly. Can we do this to prove QMA-completeness of the local Hamiltonians problem? It turns out we can't, and we'll see why next time.

6.845 Quantum Complexity Theory
Fall 2010