6.896 Quantum Complexity Theory Oct. 28, 2008

Lecture 16

Lecturer: Scott Aaronson

1 Recap

Last time we introduced the complexity class QMA (quantum Merlin-Arthur), which is a quantum version for NP. In particular, we have seen Watrous's Group Non-Membership (GNM) protocol which enables a quantum Merlin to prove to a quantum Arthur that some element x of a group G is not a member of H, a subgroup of G. Notice that this is a problem that people do not know how to solve in classical world. To understand the limit of QMA, we have proved that $QMA \subseteq PP$ (and also $QMA \subseteq PSPACE$).

We have also talked about QMA-complete problems, which are the quantum version of NP-complete problem. In particular we have introduced the Local Hamiltonians problem, which is the quantum version of the SAT problem. We also have a quantum version of the Cook-Levin theorem, due to Kitaev, saying that the Local Hamiltonians problem is QMA complete.

We will prove Kitaev's theorem in this lecture.

2 Local Hamiltonians is QMA-complete

Definition 1 (Local Hamiltonians Problem) *Given m measurements $E_1, \ldots, E_m$ each of which acts on at most k (out of n) qubits where k is a constant, the Local Hamiltonians problem is to decide which of the following two statements is true, promised that one is true:*

1. *$\exists$ an n-qubit state $|\varphi\rangle$ such that $\sum_{i=1}^{m} \Pr[E_i \text{ accepts } |\varphi\rangle] \geq b$; or*
2. *$\forall$ n-qubit state $|\varphi\rangle$, $\sum_{i=1}^{m} \Pr[E_i \text{ accepts } |\varphi\rangle] \leq a$.*

(Here $b - a > \frac{1}{p(n)}$ for some polynomial $p(\cdot)$.)

Theorem 1 (Kitaev) *The Local Hamiltonians problem is QMA-complete (as a promised problem).*

To prove this theorem, first of all, it is easy to see that the Local Hamiltonians problem is indeed in QMA, because to prove that there exists a state making all measurements accept, Merlin can simply send $|\psi\rangle = \max_{|\varphi\rangle} \sum_{i=1}^{m} \Pr[E_i \text{ accepts } |\varphi\rangle]$ as a witness.

Now we want to prove that every QMA problem can be reduced to the Local Hamiltonians problem.

The first trial would be to start from the proof that 3SAT is NP-complete —the famous Cook-Levion Theorem we talked about last time— and just put the word "quantum" in front of everything. So what happens if we do this? Let's say Arthur has asked Merlin to send him a computation tableau $|\psi_1\rangle, \ldots, |\psi_T\rangle$, and want to check it's valid by making a bunch of *local* measurements — that is, measurements on $O(1)$ qubits each. The trouble is, while Arthur can indeed check that

$|\psi_{t+1}\rangle = U_t|\psi_t\rangle$ —that is, $|\psi_{t+1}\rangle$ is the state that results from applying the t-th local gate to $|\psi_t\rangle$—, the measurement that checks this point itself is not local. Arthur has to do a *swap test* between $|\psi_{t+1}\rangle$ and $U_t|\psi_t\rangle$ (like on the pset), but that involves all the qubits of $|\psi_t\rangle$ and all the qubits of ψ_{t+1}, and is not local any more.

Therefore instead, Arthur will ask Merlin to send him the witness state

$$\frac{1}{\sqrt{T}}\sum_{t=1}^{T}|t\rangle|\psi_t\rangle.$$

(To allow Arthur to do repeated test, the state sent is actually $(\frac{1}{\sqrt{T}}\sum_{t=1}^{T}|t\rangle|\psi_t\rangle)^{\otimes \mathrm{poly}(n)}$, but this is not the critical point.) Further more, in this state, the time t is encoded in unary, that is, $|1\rangle = |100000\rangle$, $|2\rangle = |110000\rangle$, $|3\rangle = |111000\rangle$, etc. Now we can check such a state is correct using a set of measurements on at most 5 qubits each —3 adjacent qubits from the clock register, and at most 2 qubits from the computation register. Each measurement does the following: pick a random t, and measure the $(t-1)$-th and $(t+1)$-th qubits of the clock register. See if we get $|1\rangle$ and $|0\rangle$ respectively. If we do, that means we are now at the t-th time step, and the state left in the t-th qubit of the clock register and in the computation register is $\frac{|0\rangle|\psi_t\rangle+|1\rangle|\psi_{t+1}\rangle}{\sqrt{2}}$. (Notice that if the clock register is "bad", we can detect it with $1/\mathrm{poly}(n)$ probability. The error probability can be reduced by repeating polynomial times.) Now apply U_t^{-1} to the two relevant qubits in the computation register (U_t is local and applies only on 2 qubits), conditioned on the t-th qubit is $|1\rangle$. The state becomes $|0\rangle|\psi_t\rangle + |1\rangle U_t^{-1}|\psi_{t+1}\rangle = |0\rangle|\psi_t\rangle + |1\rangle|\psi_t\rangle$ (unnormalized). Finally, apply a Hadamard to the t-th qubit in the clock register, measure it, and accept if we get $|0\rangle$, reject otherwise. Notice that the final Hadamard translates the state into $|0\rangle|\psi_t\rangle + |1\rangle|\psi_t\rangle + |0\rangle|\psi_t\rangle - |1\rangle|\psi_t\rangle = |0\rangle|\psi_t\rangle$, therefore the final measurement will always get $|0\rangle$ if the computation history is correct and we will accept with probability 1. The key fact that Kitaev proved is that if the history is *far* from correct, we'll detect that with probability at least $1/\mathrm{poly}(n)$.

It is worth mention that people actually showed that a bunch of measurements acting on 2 qubits each is enough. Notice that 2SAT is in P. Do these results contradict with each other? No, because what we do in the local measurement above is actually sufficient to solve the max-k SAT problem, which is already NP-complete.

Another interesting issue is that there are many variants of the Cook-Levin Theorem in the classical world. One of them is the PCP Theorem, saying that, given a 3SAT formular $\psi(x_1, \ldots, x_n)$, deciding whether (1) ψ is satisfiable, or (2) at most 9/10 of ψ's clauses can be satisfied, is NP-complete. People still don't know whether we can have the quantum version of the PCP Theorem, says that the approximation of the Local Hamiltonians problem is already QMA-complete. Scott conjectures that this statement is true.

3 QMA vs QCMA

Last time we also talked about $QCMA$, where the proof sent by Merlin is classical, while Arthur can do a quantum check. As mentioned before, the problem $QMA \stackrel{?}{=} QCMA$ is still a major open problem in quantum computation. Actually, people still don't know whether there exists an oracle A which separates the two class, that is, $QMA^A \neq QCMA^A$.

In a recent paper, Aaronson and Kuperberg managed to give a "quantum oracle separation" between QMA and $QCMA$. Just like an oracle is some Boolean function $A : \{0,1\}^n \to \{0,1\}$ that

an algorithm can call as a black box, a quantum oracle is some unitary transformation U that an algorithm can apply as a black box. As it turns out, sometimes it's extremely useful to let the oracles themselves be quantum.

Just like the oracle that separates P from NP, we expect that the quantum oracle U separating QMA from $QCMA$ will encode a hard unitary search problem. The n-qubit unitary U is defined such that either

(i) $U = I$, that is, the identity matrix; or

(ii) there exists a secret "marked state" $|\varphi\rangle$ such that $U|\varphi\rangle = -|\varphi\rangle$, and $U|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle$ orthogonal to $|\varphi\rangle$.

As expected, the YES case that Merlin is going to prove is Case (ii).

Using a QMA protocol, Merlin simply send $|\varphi\rangle$ to Arthur. To verify, Arthur performs a controlled query to U and get the state $|0\rangle|\varphi\rangle + |1\rangle U|\varphi\rangle$. Arthur will get $|0\rangle|\varphi\rangle - |1\rangle|\varphi\rangle$ if the statement is true, while $|0\rangle|\varphi\rangle + |1\rangle|\varphi\rangle$ if false (i.e., $U = I$). Arthur then performs a Hadamard on the first register and measures it, accepts if getting $|1\rangle$, rejects otherwise. Therefore this problem is in QMA.

Is it in $QCMA$? In other words, are there poly(n) classical bits that Merlin can send to Arthur, that will enable Arthur to find $|\varphi\rangle$ with only poly(n) queries to U? Aaronson and Kuperberg prove the answer is no. The intuition is, Merlin's advice divides the set of all n-qubits quantum states into at most $2^{\mathrm{poly}(n)}$ "advice regions". But remember, the space of n-qubit states is *doubly* exponentially large (in the sense that there are 2^{2^n} states, every pair of which has large inner product). Hence at least one of those advice regions must be extremely large. And using a generalization of the BBBV hybrid argument, they prove that searching any large enough advice region for a random marked state requires exponentially many queries (in particular, $\Omega\left(\sqrt{\frac{2^n}{m+1}}\right)$, where m is the number of advice bits).

So how about a *classical* oracle separation between QMA and $QCMA$? Aaronson and Kuperberg showed that the Group Non-Membership problem cannot lead to such a separation. In particular, they gave a GNM protocol that uses a polynomial-size classical proof and poly(n) quantum queries to the group oracle (though also an exponential amount of postprocessing). The idea is: Merlin can just *tell* Arthur what the black-box group is. He can say, "it's the symmetric group," or "it's a semidirect product of the Monster group with a twisted Chevalley group of Ree type." It's a consequence of the Classification of Finite Simple Groups that Merlin can say what the group is using a polynomial number of bits. Then Merlin also gives Arthur a *mapping* from that explicit group into the black-box group. Then Arthur just has to check two things: that the mapping is homomorphism, and that it's 1-to-1. Checking that the mapping is a homomorphism can be done classically, and checking that it's 1-to-1 can be done by solving the Nonabelian Hidden Subgroup Problem. By the result of Ettinger, Hoyer, and Knill, that requires only a polynomial number of quantum queries. Once Arthur has an embedding from the explicit group into the black-box group, he can then solve the Group Non-Membership problem by looking only at the explicit group, without making any further queries to the black-box group.

4 QMA(k)

The last topic today is $QMA(k)$, quantum Merlin Arthur with multiple proofs. The scenario is that there are k Merlins, and each of them can send to Arthur a quantum proof. This is not interesting in the classical world, because we can just concatenate the k proofs into one, and thus $MA(k) = MA$. But in the quantum case, suppose Arthur knows that the k proofs are unentangled with each other. Can Arthur use that promise to his advantage? In a paper of Aaronson, Beigi, Drucker, Fefferman, and Shor, they give evidence that indeed Arthur can. For example, if a 3SAT formula of size n is satisfiable, then this satisfiability can be proved to Arthur using $O(\sqrt{n}\text{polylog}(n))$ unentangled quantum proofs with $\log(n)$ qubits each.

Next time we will talk about quantum interactive proofs.

6.845 Quantum Complexity Theory
Fall 2010