6.896 Quantum Complexity Theory Oct 21, 2008

Lecture 14

Lecturer: Scott Aaronson

1. Last Time

Last class, we finished the section on collision lower bounds and constructed an oracle relative to which SKZ is not contained in BQP.

Here's something extra from last class. It's tantalizingly easy to get a state $\frac{|x\rangle+|y\rangle}{\sqrt{2}}$, where x and y are a collision pair $(f(x) = f(y))$. If only we could measure twice, we might find out both elements of the collision pair! You can do this in Dynamical Quantum Polynomial Time (DQP), which extends BQP by letting you see the whole trajectory of a quantum state, in effect letting you measure multiple times. We know that DQP contains SZK, the class of statistical zero-knowledge proofs. There exists an oracle relative to which NP is not in DQP.

But can we use the power of DQP to speed up black-box search? Yes, but not by much. We can improve Grover's Algorithm by measuring after each application of the Grover Diffusion Operator. This process finds almost surely finds the marked item in $O\left(N^{1/3}\right)$ applications rather than the $O\left(N^{1/2}\right)$ of Grover. This has been proven optimal.

Now we return to quantum complexity land.

2. Placing BQP

So, where exactly does BQP lie within the classical complexity classes? There's a lot we don't know, such as whether BQP belongs inside NP. There's an even bigger question: How does BQP relate to the polynomial hierarchy (PH)? Whether there's an oracle relative to which BQP is not in PH remains an open problem. We've found oracle problems for which quantum algorithms have exponentially outpaced classical ones, such as Simon's problem and Shor's period-finding problem, but almost all of these lie in NP.

Here's a candidate for an oracle problem in BQP, but above the polynomial hierarchy.

> **Fourier Checking:** Given oracles for two Boolean functions $f : \{-1,1\}^n \rightarrow \{-1,1\}$ and $g : \{-1,1\}^n \rightarrow \{-1,1\}$, decide whether
>
> - Both f and g are uniformly random.
> - f is random, and $g = sgn\left(\hat{f}\right)$, where $\hat{f} = \sum_y (-1)^{x \cdot y} f(y)$ is the Fourier Transform of f.
>
> given that one of these is the case.

This problem is in BQP, since it can be solved with a quantum circuit:

In the first case where f and g are random, the final measurements give a random value.

If f and g satisfy the second promise, one can show that starting from a uniform distribution and applying f, then Hadamard gates to each qubit, then g, gives a nearly uniform distribution. So, the final set of Hadamard gates, will give a nearly all-zero state in this case.

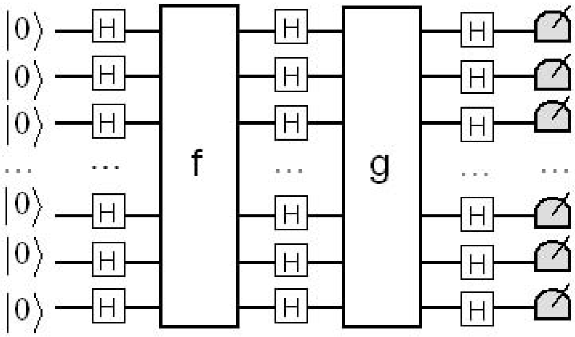

Figure 2.1. A quantum circuit for Fourier Checking

We conjecture that Fourier Checking is not in PH. It definitely does not seem to be in NP, since the relationship between f and g is a global property of the functions, so it would seem to be hard to demonstrate it in a certificate of polynomial size.

3. MA and AM

We don't know how BQP compares to NP, so let's make a quantum version of NP.

As a first step, we make a probabilistic version of NP, which we'll call MA, for Merlin-Arthur.

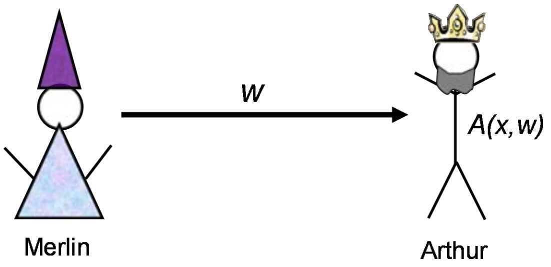

Figure 3.1. The Merlin-Arthur Protocol

The imaginative naming is from Babai. Merlin, an omniscient wizard with unbounded computation resources, wants to prove something to the king Merlin, who only has polynomial time to check. Merlin sends Arthur a certificate to try to convince Arthur to accept. Arthur can't be too gullible, since Merlin is devious and will try to get him to accept false statements as well as true ones. Formally,

Definition. MA is the set of languages $L \subset \{0,1\}^{\star}$ for which there exist a Turing Machine A in probabilistic polynomial time such that for all inputs x

- If $x \in L$, then there exists a polynomial-sized certificate w so that $A\left(x,w\right)$ accepts with probability at least $^2/_3$.
- If $x \notin L$, then for any polynomial-sized certificate w so that $A\left(x,w\right)$ accepts with probability at most $^1/_3$.

The probabilities are being taken over some random bits A has access to.

It makes not difference if we change the$^2/_3$ in the definition to a 1; this is a nontrivial theorem. However, we can't make it so that Arthur is never duped: If the $^1/_3$ in the definition is changed to a 0, we get NP.

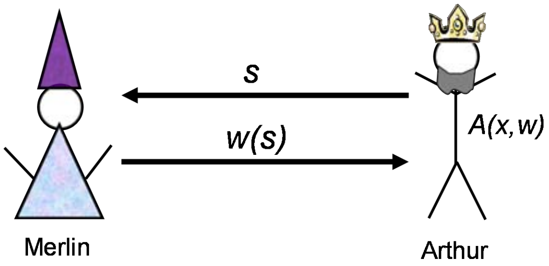

Figure 3.2. The Arthur-Merlin Protocol

Merlin-Arthur has a cousin, called Arthur-Merlin (AM), in which first Arthur sends a challenge string s to Merlin, then Merlin responds to the challenge. Since it gives an extra turn for Arthur to act, AM contains MA. It's also known that SKZ⊂AM.

Specifically, this means that the Graph Non-Isomorphism (GNI) problem is in AM. We can solve GNI with this AM protocol: Arthur sends Merlin challenge graphs, each a permutation of one of two graphs he's testing, and if Merlin can reliably say which graph was which, Arthur should be convinced that the graphs are not isomorphic. We don't know if GNI∈MA.

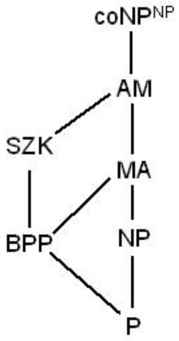

Figure 3.3. An inclusion diagram containing MA and AM

We conjecture that we can derandomize the random algorithms, which will collapse P=BPP and NP=MA=AM. Strong circuit bounds would suffice to do this.

4. QMA

To make a quantum analogue of MA, there are two parts we can "quantize": the verifier algorithm and the certificate. Making both quantum gives the class called Quantum Merlin-Arthur (QMA).

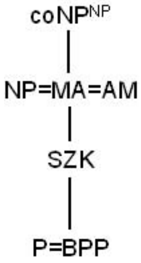

Figure 3.4. What the tree would look like if derandomization succeeds.

Definition. QMA is the set of languages $L \subset \{0,1\}^\star$ for which there exist a polynomial-time quantum circuit A such that for all inputs x

- If $x \in L$, then there exists a witness state $|\varphi\rangle$ so that $A(x, |\varphi\rangle)$ accepts with probability at least $2/3$.
- If $x \notin L$, then there for any witness state $|\varphi\rangle$, $A(x, |\varphi\rangle)$ accepts with probability at most $1/3$.

If Arthur has the power of a quantum circuit, but the witness must be classical, we get the oxymoronically named Quantum Classical Merlin Arthur (QCMA).

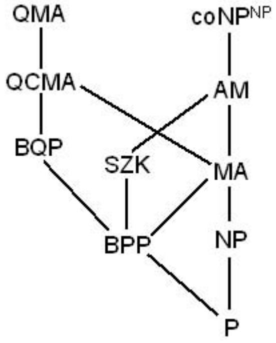

Figure 4.1. Placing BQP, QMA, and QCMA among classical complexity classes

5. Amplifying QMA

Unlike for MA, in QMA we don't know if we can make the accept rate $2/3$ into a 1. One thing we'd like to check is that our choice of constants $1/3$ and $2/3$ is not crucial for QMA; we don't want the definition to hang on arbitrary numbers. We'll check that Arthur can amplify to any probability he wants.

If Arthur could just copy the witness state $|\varphi\rangle$ a bunch of times, Arthur could amplify by running the verifier algorithm once on each witness, and take the majority result. But unknown states can't be cloned, so instead we'll have Merlin send the requisite copies of $|\varphi\rangle$. But can we trust Merlin not to do something tricky?

What if Merlin secretly cheats by sending a bunch of different states $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$? Then, each of them has its own probability p_i of Arthur accepting, and Merlin can do at least as well at making Arthur accept if he just send copies of the $|\varphi_i\rangle$ with the largest p_i.

What if Merlin keeps some qubits that are entangled with the witness states he sends? Then, from Arthur's view, Merlin has sent mixed states, so Arthur's probability of accepting is a weighted mean of the probability of accepting each component pure state. So, again, Merlin would be at least as well off sending the pure part with highest acceptance probability.

Now what if Merlin sends witness states that are entangled with each other? By convexity, some pure state $|\varphi\rangle$ maximizes the probability that Arthur accepts. Even after Arthur has performed an experiment on a register, Merlin can hope for nothing better than for the next register Arthur acts on to contain $|\varphi\rangle$. But then, why not just put the unentangled state $|\varphi\rangle$ there? So, entangling registers doesn't win Merlin anything.

6. Group Non-Membership

So, what can we actually do with QMA? One seemingly hard problem in QMA is Group Non-Membership.

We are given a black box group G. What this means is that each group element x has an arbitrary and distinct code string S_x, and we have oracles that implement the multiplication and inverse operations for G on these code strings. For notation, we'll just refer to the elements as themselves, rather than their code strings.

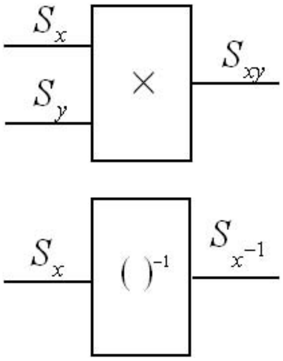

Figure 6.1. Black boxes for some group

Group Membership Problem: Given a subgroup H of G (as a list of generators), and an $x \in G$, decide if $x \in H$.

Note that G and H may have exponential size, but we can give always give a polynomial set of generators for G and H.

Is this problem in NP? Well, we can certainly show that $x \in H$ by giving a product of generators and their inverses to make x, which the verifier can check. But this might be exponential in length. For example, if H is the cyclic group of order 2^n, given by generator $\{1\}$, and $x = 2^{n-1}$, then reaching x takes 2^{n-1} operations. We can remedy this by using square-and-multiply. If we can save already-formed group elements and reuse them, any element can be formed in polynomial time.

What about Group Non-Membership, checking if $x \notin H$? This is trickier.

Here's an idea for to solve this in QMA. Have Merlin send Arthur the state

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

Here's a question: Could Arthur have just made the state himself? It's known that Arthur can pick a random element of H by himself: If Arthur randomly takes two elements from the set of generators, multiplies them with the oracle, and adds the result to the set, then with a polynomial number of repetitions, he'll get an element almost uniformly at random.

So then why can't Arthur make $|\varphi\rangle$ himself? Well, a probability distribution is not the same thing as quantum state. If Arthur runs the random algorithm on a quantum computer, he'll get

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle \, |garbage_h\rangle$$

where the garbage can from the process of computing $|h\rangle$. There's no obvious way to erase this workspace.

Next class, we'll prove that this verifier state $|\varphi\rangle$ can convince Arthur whether $x \notin H$.

6.845 Quantum Complexity Theory
Fall 2010