Lecture 18

Lecturer: Scott Aaronson

1 Last Time: Quantum Interactive Proofs

1.1 IP = PSPACE $\subseteq$ QIP = QIP(3) $\subseteq$ EXP

The first result is interesting, because the fact the PSPACE Is contained in IP is slightly counter-intuitive. One consequence of this is that game theory questions (i.e. white has the win in chess) can be proved though a message exchange protocol. We also saw that QIP = QIP(3), or in other words, that any quantum protocol can be reduced to three rounds.

1.2 MIP = NEXP

If we allow for multiple provers, the situation becomes more interesting. Effectively, Alice and Bob are in separate rooms, and we try to interrogate them separately. This protocol gives us more power in the classical case, and possibly even more power in the quantum case.

1.3 ?? $\subseteq$ QMIP $\subseteq$??

Nothing is known about the relationship of QMIP to other complexity classes, because of the arbitrary amount of entanglement that is allowed. Answering this question requires a better understanding of entanglement than we currently have, which is a reason that this question is very studied currently. There is no way within the laws of physics to require that entanglement is not shared.

Classically, Alice and Bob can agree on their strategy in advance. So, does entangelement actually give us anything more? Ostensibly, the answer is yes. What we can be sure of, is that entanglement breaks some MIP protocols which work classically. CHTW [2] gives examples of such protocols.

1.4 Graph Two-Coloring

Given provers Alice and Bob who claim to know a two-coloring of a graph, your strategy is as follows: flip a coin, with 1/2 probability ask Alice and Bob how to color a specific vertex. Otherwise, ask them about adjacent vertices.

We can use a convexity argument to show why they can't cheat with perfect reliability in the classical world, on a graph containing an odd cycle. Given any probabilistic strategy for cheating, there will always be a deterministic strategy that does as well as the probabilistic one. Since there is no actual coloring that works, there is always a probability that they will be caught with non-zero probability. Since at least one vertex will trip them up, they will be caught with probability $\Omega(n^{-1})$.

On the other hand, in a quantum world, if Alice and Bob share the entangled state

$$\frac{|00\rangle + |11\rangle}{2}$$

then there is a strategy such that you catch them with probability $O(n^{-2})$ [2].

Here's what you do. We want each of the vertices on the cycle to correspond to quantum state (point on the unit circle) such that they are spaced $2\pi/n$ apart. We have Alice and Bob each measure their qubit in the basis that corresponds to the vertex that is queried. Accordingly, we want adjacent vertices to be nearly orthogonal, so we place adjacent vertices $\pi/2 + 2\pi/n$ radians apart. Given this ordering, Alice and Bob will either measure their qubit in the same basis, or in nearly orthogonal bases. When we say, "nearly orthogonal," this means something like $\cos^2 2\pi/n$ off, which corresponds to a likelihood is something like $1 - n^{-2}$, that Alice and Bob will measure different states.

This bound is tight for provers that are only allowed to share the state given above, but there exist strategies that allow the provers to cheat perfectly by sharing specific entangled states.

Remark 1 *QMIP with finite entanglement is upper bounded by the set of computable functions.*

Remark 2 *If P = NP, then EXP = NEXP. This follows from a simple padding argument.*

Quantum parallel games: write out best prover strategy as semi-definite program, using parallel repetition theorem.

2 Quantum computing with Postselection

Postselection refers to the process of conditioning the experiment on getting the outcome that you are looking for, and discarding the outcome otherwise. Today, we will investigate the computational power that this additional theoretic resource gives us. This has a very obvious tie-in with the many worlds interpretation of quantum mechanics.

Definition 1 *The many worlds interpretation concludes that the world splits at every quantum branching point, and we continue in a superposition of all of these states.*

For example, if you really want the answer to a problem, you can perform an experiment where you postselect on receiving a certain outcome, and otherwise shoot yourself. Accordingly, in universes where you are still alive, you get the answer that you were looking for.

Less morbidly, you could make a firm commitment, if you get the measurement you want, that you'll have lots of children, and many descendants. Otherwise, you will sterilize the human race. This maximizes the probability that someone will see the answer to your computational problem.

This gives rise to the class **PostBQP**.

Definition 2 *This is the class of $L \subseteq \{0,1\}^*$ such that $\exists$ a polytime quantum alogirhtm Q such that $\forall$ inputs x,*

- *$Q(x)$ gets selected with probability > 0*
- *If $x \in L$ conditioned on being selected, $Q(x)$ acepts with probability $\geq 2/3$*

- *If $x \notin L$, conditioned on being selected, $Q(x)$ accepts with probability $\leq 1/3$*

Overall, this algorithm consists of two measurements, one to decide whether to proceed or throw away the computation, and the second, to see if the computation ultimately accepts or rejects. Such experiments are very common in physics. For example, we could postselect on the condition that a photon didn't go where it was supposed to go.

A natural question to this is whether the presence of additional postelection measurements helps us. It turns out that it does not, by the Principle of Deferred Measurement. Without loss of generality, we can assume there is only one measurement, and simulate the rest with controlled-NOT gates.

Remark 3 *It should be immediately clear that BQP $\subseteq$ PostBQP.*

2.1 NP $\subseteq$ PostBQP?

We devise an algorithm for solving any problem in NP with a PostBQP algorithm. First, go into superposition over all inputs

$$\frac{1}{2^{n/2}} \sum |x\rangle |f(x)\rangle$$

and postselect on finding a valid certificate, then accept or reject accordingly. However, this has the flaw that it does not handle the case of there being no solutions. We fix this by adding a dummy state with extremely low amplitude (say, 2^{-20n}.) If we measure and postselect on getting a 1, and get the dummy solution, then there is almost certainly no real solution.

Can we find an upper bound on PostBQP? PSPACE immediately comes to mind, but it turns out that we can do better.

Theorem 1 (Adleman, DeMorrai, Huang) *PostBQP $\subseteq$ PP*

Proof: Do a Feynman path integral, and sum over all contributes to the final amplitude. Restrict to the states that you postselect, and make all of the others cancel. □

Theorem 2 *PP $\subseteq$ PostBQP*

Proof:

PP basically means that you can compute the majority function on an exponentially long string, hence we can model an arbitrary problem in PP in the following way.

- $f : \{0,1\}^n \to \{0,1\}$
- $s = |\{x : f(x) = 1\}|$
- Problem: Decide if $s \geq 2^{n-1}$, assume $s > 0$.

Prepare a 1-qubit state:

$$|\psi\rangle = \frac{(2^n - s)|0\rangle - s|1\rangle}{\sqrt{(2^n - s)^2 + s^2}}$$

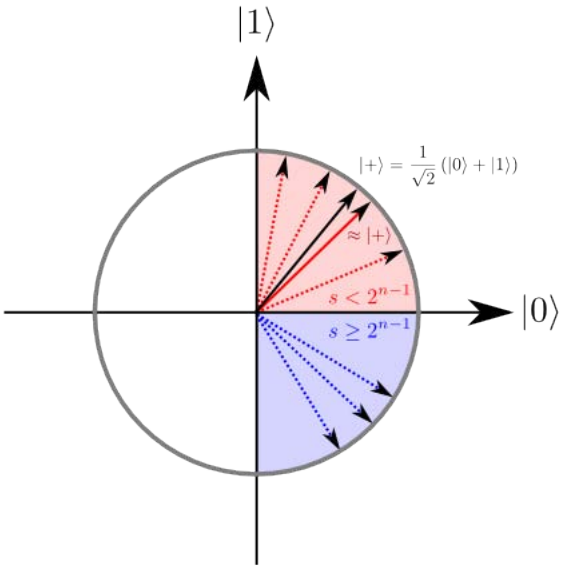

Figure 1: Different values of s

This means that, by applying a Hadamard conditioned on the first qubit, we can also prepare the state

$$\frac{\alpha\,|0\rangle\,|\psi\rangle + \beta\,|1\rangle\,H\,|\psi\rangle}{\sqrt{\alpha^2+\beta^2}}$$

Note that

$$H\,|\psi\rangle = \frac{\frac{1}{\sqrt{2}}2^n\,|0\rangle + \frac{1}{\sqrt{2}}(2^n-2s)\,|1\rangle}{\sqrt{(2^n-s)^2+s^2}}$$

Accordingly, we postselect on the second qubit being 1:

$$|\psi_{\alpha,\beta}\rangle = \alpha s\,|0\rangle + \beta\frac{2^n-2s}{\sqrt{2}}\,|1\rangle$$

If s is appropriately large, the second term is negative, otherwise it is positive. We can find out which by varying $\frac{\alpha}{\beta}$ in a certain way. We do need to be clever here, because we have to postselect based on the outcome of a measurement, we can't just postselect on some non-measurable condition like negative amplitude. Pick β and α from the set:

$$\beta/\alpha = \{2^{-n},\ldots,1/2,1,2\ldots,2^n\}$$

The vectors corresponding to $\frac{\alpha}{\beta}$ and different values of s are shown on the unit circle below in Figure 2.1.

2.1.1 First Case:

Assume α,β positive. If $s < 2^{n-1}$, then both amplitudes will be positive. So we keep varying alpha, beta, and measure in the Hadamard basis. This gets us very close to $|+\rangle$, which we can detect with non-trivial probability.

2.1.2 Second Case:

If $s \geq 2^{n-1}$, then we're in the fourth quadrant. For some $\frac{\alpha}{\beta}$, we are close to $|-\rangle$, so we can discern the relative value of s.

□

3 Classical Results from Quantum Lower Bounds

It is a bit strange that PostBQP = PP, in that the latter class has been part of classical complexity theory for many years, while the former has only recently emerged. The fact that they are equal gives rise to the hope that we may be able to use results in quantum complexity theory to better inform our understanding of classical complexity theory. This is not altogether surprising, though, given the efficacy of probabilistic methods in proving classical results that ultimately have little to do with probability.

"Quantum generosity - giving back to the classical world."

Theorem 3 (Beigel-Reingold-Spielman, 1991 [1]) *PP is closed under intersection:*

$$L_1, L_2 \in PP \Rightarrow L_1 \cap L_2 \in PP$$

This is a non-trivial result, showing that the AND of two large majorities can itself be modeled as the AND of a single large majority. Put another way, this takes two PP computations and models it as a single computation - how to do this is not at all obvious, and naive approaches fail accordingly.

However, the equality of PostBQP and PP gives rise to a very simple quantum theoretic proof of the same result.

Theorem 4 *PostBQP is closed under intersection.*

Proof: Given two computations with two postselection criterion, postselect on them both being true, and then run the computations, accepting if both computations accept. □

Remark 4 *It might seem that could lead to answer whether $PP = P^{PP}$, using PostBQP. However, we have to be careful when reasoning about P with a PostBQP oracle. Well, we can't really chain the way that we want to, because P doesn't let us discard bad outcomes, which could create bad chains.*

Next time: time travel. Chosen by democracy!

References

[1] Richard Beigel, Nick Reingold, and Daniel Spielman. Pp is closed under intersection. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 1–9, New York, NY, USA, 1991. ACM.

[2] R. Cleve, P. Hyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of 19th IEEE Conference on Computational Complexity*, pages 236–249, 2004.

6.845 Quantum Complexity Theory
Fall 2010