6.896 Quantum Complexity Theory 30 October 2008

Lecture 17

Lecturer: Scott Aaronson

Last time, on *America's Most Wanted Complexity Classes*:

1. QMA vs. QCMA; QMA(2).
2. IP: Class of languages $L \subseteq \{0,1\}^*$ for which there exists an interaction protocol between BPP verifier and an omnipotent prover s.t. $\forall x$:
   (a) $x \in L \implies \exists$ a prover strategy that causes verifier to accept w.p. $> 2/3$
   (b) $x \notin L \implies \forall$ prover strategies, verifier accepts w.p. $\leq 1/3$.
3. **Theorem 1 (LFKN, Shamir)** IP = PSPACE.

Everything we've been discussing so far involved one-shot proof systems where Merlin (or Merlins) send some quantum states to Arthur, and then Arthur verifies those states. But one can also study quantum interactive proof systems (QIP), where Arthur and Merlin send quantum messages back and forth.

1 Classical Interactive Proofs

First of all, what do we know about classical interactive proof systems (IP)? Let IP be the class of problems for which a 'yes' answer can be verified (with constant error) by an interactive protocol in which a polynomial-time Arthur exchanges messages with an omniscient Merlin. Here 'omniscient' means that Merlin can do an unlimited amount of computation, but is unaware of the questions Arthur will ask in the future and subsequently commits to his answers without knowledge of Arthur's responses. The intuition behind the power of interactive proofs is not surprising. From our day-to-day experience, we know that reading a proof is usually more difficult than simply asking its author for details. In complexity theory, we have strong evidence that this process is more powerful than static provers. We reached this conclusion when we looked at AM and MA, where proofs in the former are not accessible in the latter (AM $\subseteq$ IP), and the complexity of the graph isomorphism problem (GNI $\in$ IP).

A famous result of Lund, Fortnow, Karloff, and Nisan (finished off by Shamir) says that this class is incredibly big: IP = PSPACE, meaning that the optimal strategy for the prover can be computed in polynomial space. For example, if a super-intelligent alien came to earth, it could convince us that White has the win in chess. The theorem suggests that there is a protocol by which the alien *could* convince us that White has to win in chess. We'd do that by transforming chess into a different game involving polynomials over finite fields. In the new game, the best strategy for one of the two players is to move randomly. If in this randomnization scenario, the alien wins, we should be convinced that the alient could win against *any* player.

Before moving on to QIP, we will very briefly consider the LFKN simpler result that coNP $\subseteq$ IP, i.e., one can prove through an interactive protocol that a Boolean formula is 'unsatisfiable.' Note that this is surprising because $\exists$ an oracle A s.t. $\text{coNP}^A \not\subseteq \text{IP}^A$. This means that the proof of

coNP $\subseteq$ IP must be a non-relativizing proof. This is one of the few examples we have of a proof that exploits enough about the structure of computation that they would actually fail in the real world where there is such an oracle.

Theorem 2 (LFKN) coNP $\subseteq$ IP.

Proof: [Sketch] The idea here is that we have some Boolean formula $\phi(x_1, \ldots, x_n)$ that Merlin wants to convince Arthur it is non-satisfiable. Here we 'arithmetize' the expression by replacing all the Boolean variables with finite field elements $x_1, x_2, x_3 \in \mathbb{F}_p$, and all the Boolean operations with arithmetic operations over $\mathbb{F}_p$. For example, a 3-bit OR arithmetizes to

$$x_1 \vee x_2 \vee x_3 = 1 - (1 - x_1)(1 - x_3)(1 - x_3), \tag{1}$$

which is a polynomial over the field of $\mathbb{F}_3$.

As as a result, our goal here is to convince Arthur that

$$\sum_{\substack{x \in \{0,1\}^* \\ x_1, \ldots, x_n}} p(x) = 0. \tag{2}$$

The omnipotent Merlin can easily verify this statement is true for some Boolean string x and tell Arthur the result. However, Arthur isn't so gullible. He requires convincing. Instead, Merlin performs the sum over the last $n - 1$ variables such that

$$q_1(x_1) = \sum_{x_2, \ldots, x_n} p(x_1, x_2, \ldots, x_n). \tag{3}$$

Merlin sends Arthur all the coefficients, and Arthur can check for himself that $q_1(0) + q_1(1) = 0$.

Arthur must verify that the Merlin has determined the above sum correctly. Arthur evaluates $q_1(x_1)$ at some random $x_1 = r_1 \in \mathbb{F}_p$. From this point on, Merlin must use some fixed value of x_1 that Arthur has picked, and then returns

$$q_2(x_2) = \sum_{x_3, \ldots, x_n} p(r; x_2, \ldots, x_n) \tag{4}$$

for which Arthur can verify that $q_2(0) + q_2(1) = q_1(r)$. The process iterates, and Arthur picks another $r_2 \in \mathbb{F}_k$ and Merlin returns

$$q_3(x_3) = \sum_{x_4, \ldots, x_n} p(r_1, r_2; x_3 \ldots, x_n). \tag{5}$$

Arthur and Merlin continue until $q_n(x_n)$ and all the values have been fixed. Arthur can check that $p(r_1, \ldots, r_n)$ is the required value.

However, if Merlin is lying, Arthur can catch him with constant probability. To show this we use the following fact that *a d-polynomial has at most d roots* (the Fundamental theorem of algebra). If we have two d-degree polynomials that are not equal, they can only be equal on at most d inputs. This means that the polynomials q and p can only agree on a polynomial number of elements. Therefore, if Arthur picks a random r_1, the verified polynomial will almost certainly disagree if Merlin is lying. s $\square$

2 Quantum Interactive Proofs

Just as you'd expect, one can also define QIP: Quantum Interactive Proofs. Here the prover and verifier can exchange quantum messages, and the prover is limited only by the laws of quantum physics. The protocol is show in Figure 1 below.

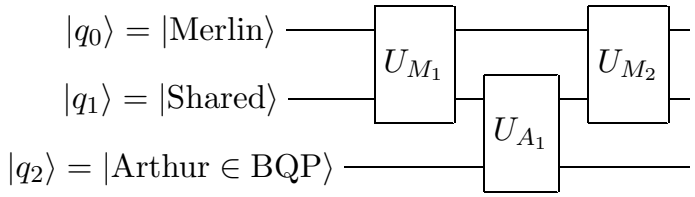

Figure 1: Merlin-Arthur QIP protocol using a polynomial number of gates. To simplify the illustration, each set of private and shared qubits used by Merlin and Arthur are tensored together a polynomial number of times. For example, $|q\rangle = \otimes_i^{p(n)} |i\rangle$.

QIP is defined as the class of languages $L \subseteq \{0,1\}^*$ for which there exists an interaction protocol between BQP verifier (Arthur) and an omnipotent prover (Merlin) s.t. $\forall x$:

1. $x \in L \implies \exists\ M_1$ and M_2 causing Arthur to accept w.p. $> 2/3$
2. $x \notin L \implies \forall\ M_1$ and M_2 Arthur accepts w.p. $\leq 1/3$.

Certainly IP $\subseteq$ QIP; that is, quantum interactive proof systems can simulate classical ones. Thus PSPACE $\subseteq$ QIP. However, it turns out that something new and extremely interesting happens in the case of quantum interactive protocols.

Theorem 3 (Kitaev,Watrous00) *Any QIP protocol can be made three-round. In other words, all QIP rounds are given by* $\text{QIP}(1) = \text{QMA}$*,* $\text{QAM} \subseteq \text{QIP}(2)$*, and* $\text{QIP}(3) = \text{QIP}$*.*

Proof: [Sketch] To illustrate, lets just show how to do PSPACE with three rounds (PSPACE $\subseteq$ QIP (3)). Assume without loss of generality that Arthurs messages to Merlin are all just uniform random bits. Then Merlin can send Arthur a (claimed) superposition over all possible conversations that they could have had:

$$\frac{1}{\sqrt{2^T}} \sum_{a_1,\ldots,a_T} |a_1\rangle\,|a_2\rangle \cdots |a_T\rangle\,|m_1\rangle\,|m_2\rangle \cdots |m_T\rangle \tag{6}$$

For reasons we'll see later, Merlin also keeps a copy of the $|a_T\rangle$ registers for himself. Arthur can now check, in superposition, whether or not the conversation would have caused him to accept. The trouble is, what if Merlin cheated by picking $|a_T\rangle$'s that werent truly random—and were instead concentrated on the tiny fraction where he can get away with lying?

Arthur needs to verify that the $|a_T\rangle$'s are random. To do so, he first picks a random time step t, and sends Merlin the $|m_u\rangle$ for all $u > t$. Using his copy of the $|a_T\rangle$ registers, Merlin then uncomputes those $|m_u\rangle$. Finally, Merlin sends Arthur his $|a_T\rangle$ registers. Arthur is now able to measure the $|a_u\rangle$ registers with $u > t$ in the Hadamard basis, and check whether the messages

supposedly from him were really uniformly random. If Merlin was honest, Arthur will now accept with probability 1. The nontrivial thing you have to prove is that if Merlin cheated, Arthur will detect it with $1/\text{poly}(n)$ probability. Furthermore, he can amplify that probability by running the protocol polynomially many times in parallel. □

It's important to note that Merlin will be unable to suddenly swap out his qubits with some other qubits and expect the entanglement he shares with Arthur to remain intact. This fact, known as the 'monogamy of entanglement,' is related to the differences between correlation and entanglement. Here, consider three classical bits x, y, and z, and the correlation $x \sim y \sim z$. By transitivity, if $x \sim y$ and $y \sim z$, $x \sim z$. However, if two variables x and y are entangled, it is not possible to entangle a third variable z with x. This can be shown by taking the partial trace over a sample three-way entangled GHZ state,

$$|xyz\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{7}$$

which results in x and x having statistically-independent distributions.

The remaining question here is the upper bound to QIP. Kitaev and Watrous also showed that QIP $\subseteq$ EXP. They did this by expressing the problem of finding the best possible strategy for the prover as an exponentially-large, semi-definite programming (SDP) problem. SDP is known to be solvable in polynomial time. Let's see how they did this: SDP is basically the problem of finding positive definite matrices that satisfy a set of linear constraints. A general quantum state (i.e. a mixed state) is just a Hermitian positive definite matrix with trace 1. The trace 1 and Hermitian are linear constraints. So, the problem of finding N-dimensional quantum mixed states that satisfy a bunch of linear constraints is an SDP. The question now becomes, how can we formulate the problem of finding the optimal strategy for Merlin in a quantum interactive protocol, as a problem of finding mixed states that satisfy linear constraints? Imagine the circuit depicted in Figure 1 that relates mixed states ρ and σ through the QIP unitary protocol. The problem is to find states ρ,σ such that ρ is a valid initial state, σ is a final state that accepts with maximum probability, and $\text{Tr}_M\left(U\rho U^{-1}\right) = \text{Tr}_M\left(W^{-1}\sigma W\right)$. Here we're using the fact that if $\text{Tr}_M\left(U\rho U^{-1}\right) = \text{Tr}_M\left(W^{-1}\sigma W\right)$, then there must exist a unitary transformation on Merlin's registers only that transforms $U\rho U^{-1}$ to $W^{-1}\sigma W$.

To this day, we dont know exactly where QIP sits between PSPACE and EXP.

2.1 Multi-prover QIP

Finally, many quantum computing people lately have been interested in multi-prover quantum interactive proof systems. In the classical world, putting two people in separate rooms to interrogate them often lets you learn more than if the people could talk to each other. Let MIP be the class of problems for which a 'yes' answer can be efficiently verified with the help of two or more non-communicating provers. Babai, Fortnow, and Lund showed that MIP = NEXP, whereas IP only equals PSPACE. In the quantum world, though, we don't know whether QMIP contains NEXP. What do you think the difficulty is? The provers could be entangled with each other! And indeed, Cleve, Hoyer, Toner, Watrous 2004 gave examples of protocols that are sound when the provers don't share entanglement, but become unsound when they did.

Nor, embarrassing as it is to admit, do we know any upper bound whatsoever on QMIP—the reason being that we don't know *a priori* how much entanglement the provers need in their strategy.

Doherty, Liang, Toner, Wehner 2008 show that if a finite amount of entanglement suffices, then all QMIP languages are at least recursive. (On the other hand, we still dont know if there are situations where a literally infinite amount of entanglement is needed to play optimally!)

Just as BQP is contained in PP, so BQPSPACE is contained in PPSPACE. But Ladner proved that PPSPACE = PSPACE, using the same ideas as in Savitch's Theorem. Hence BQPSPACE = PSPACE.

3 The Future

Quantum computing with closed time-like curves.

6.845 Quantum Complexity Theory
Fall 2010