6.896 Quantum Complexity 2008-11-25

Lecture 21

Lecturer: Scott Aaronson *Scribe: Jia Zheng (Colin)*

Last time we introduced the advice "operator" and quantum complexity classes with quantum advice. We proved that **BQP**/*qpoly* is contained in **PostBQP**/*poly*, by showing that the maximally mixed state need only be refined (iteratively) for polynomially many steps, so outcomes of the polynomially many inputs can be encoded in the advice and post-selected.

Let us consider **QMA**/*qpoly*: how much more power does quantum advice bring? Scott's paper upper bounds it by **PSPACE**/*poly*. The kernel of the proof is to show the chain of inclusions **QMA**/*qpoly* $\subseteq$ **BQPSPACE**/*qpoly* $\subseteq$ **PostBQPSPACE**/*qpoly* = **PSPACE**/*qpoly* (by Savitch's hierarchy theorem). The first inclusion is non-trivial, as the *qpoly* "operator" does not necessarily commute.

What about **PostBQP**/*qpoly*? It is easy to see **PostBQP**/*qpoly* = **PostBQP**/*rpoly* = **ALL**: for any boolean function f, we can encode it in the advice $\frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle$, measure it in standard basis to get $(x, f(x))$ for some random x, and post-select on getting the x we are interested in.

Today we move on to quantum communication complexity.

Quantum state learning

Given a distribution $\mathcal{D}$ over measurements, $E_1, \ldots, E_m \in \mathcal{D}$, some n-qubit state $|\phi\rangle$ and $P_i = \Pr[E_i \text{ accepts } |\phi\rangle]$, we can ask the following: How many measurement samples are enough to learn $|\phi\rangle$? Or how many classical bits are needed to describe $|\phi\rangle$?

Theorem. *$O(n)$ measurement samples suffice to learn a n-qubit state $|\phi\rangle$.*

Still, just like problems in **QMA**, finding the $|\phi\rangle$ consistent with all E_i is hard.

Holevo's theorem

Consider the scenario where Alice holds an n-bit string x, how many qubits must Alice transfer, in order for Bob to output x?

Theorem. *(Holevo, 1973) n qubits can represent no more than n classical bits.*

This is a surprising result, contrasting the many scenarios where quantum computing/information is inherently more powerful than classical.

Holevo's theorem assumes that Alice and Bob do not share entangled qubits. When they do share EPR pairs, still it can be shown that at least $n/2$ qubits are needed (the $n/2$ technique is called *superdense coding*, described below).

Superdense coding

With a shared EPR pair between Alice and Bob, a single qubit may convey 2 bits of information. Alice simply sends her part of the EPR pair altered according to the 2 bits,

such that the EPR pair becomes one of:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|10\rangle + |01\rangle}{\sqrt{2}}, \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \frac{|10\rangle - |01\rangle}{\sqrt{2}}$$

each corresponding to one of the possibilities of 2 classical bits. Since they are orthogonal pure states, Bob can recover x by measuring simply in this basis. With n shared EPR pairs n qubits can convey $2n$ bits of information. It can be shown that the factor is 2 is tight.

Quantum random access codes

Suppose Alice holds an n-bit string x, and Bob holds some integer i. How many qubits must Alice transfer, so that Bob can find x_i with high probability? (The two-way communication version is less interesting as Bob can send i with $\log n$ bits and Alice sends back x_i.) Quantumly, one can have a factor-of-2 saving with bounded error, without requiring entanglement (contrast this with Holevo's theorem and superdense coding). The qubits sent by Alice are called *quantum random access codes* as they let Bob retrieves x_i for any i, but information about x_j for $j \neq i$ are lost due to measurement.

It is not known whether better than constant-factor saving can be achieved quantumly, but Scott so conjectures (i.e. this is a total function separating quantum and classical communication complexity).

The idea is very simple, due to Ambainis, Nayak, Ta-Shma and Vazirani (1999). Let Alice send the state $|\phi_x\rangle$ illustrated in the figure:

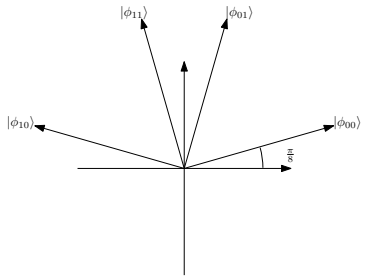

Figure 1: Quantum random access code of 2 classical bits

Bob can learn x_1 by measuring in the standard basis, or learn x_2 in the standard basis rotated $\frac{\pi}{4}$ counterclockwise. In either case probability of the desired outcome is $\cos^2 \frac{\pi}{8} \approx 0.85$. Classically it can be shown that strictly more than $n/2$ bits are needed to have bounded error.

ANTV 1999 has also proved a lower bound $\Omega(n/\log n)$ on any bounded error quantum communication protocol, with the help of Holevo's theorem.

Proof. (Sketch) Suppose a communication protocol below $\Theta(n/\log n)$ exists, with error bound 1/3. Run it $c \log n$ times for some constant c (amplitude amplification), so that error is bounded below $1/n^c$. In this new protocol Alice sends less than $\Theta(n)$ qubits. Now, the "Almost as Good as New" lemma says that if measurement succeeds with probability at least $1 - \epsilon$, then the state is "damaged" (in terms of trace distance) by at most $\sqrt{\epsilon}$. Plugging $1/n^c$ into this lemma, it can be shown that Bob can find x_i for all i, which contradicts Holevo's theorem! □

Remark. Alternatively, we can show the $\Omega(n/\log n)$ bound using last Thursday's argument: $D^1(f) \in O(mQ^1(f)\log Q^1(f))$. (The notations D^1, Q^1 are defined below.) Here $m = 1$, so $Q^1(f)$ below $\Theta(n/\log n)$ implies $D^1(f)$ below $\Theta(n)$ (which is, of course, false).

Communication complexity

Let $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$. Suppose Alice holds some $x \in \{0,1\}^n$, Bob holds some $y \in \{0,1\}^m$ and wants to compute $f(xy)$ with Alice's help.

- The deterministic one-way communication complexity $D^1(f)$ is the minimum number of bits Alice has to send to Bob. $D^1(f)$ is equal to the number of distinct rows in the communication matrix of f.
- The randomized one-way communication complexity $R^1(f)$ is the shortest string sampled from a distribution, that Alice has to send to Bob, so that Bob can find $f(x, y)$ with bounded error.
- The quantum one-way communication complexity $Q^1(f)$ is the minimum number of qubits Alice has to send to Bob, so that Bob can find $f(x, y)$ with bounded error by a measurement. Alice may send a mixed state as in the randomized case. Since each mixed state can be represented by a pure state with qubits doubled, pure states are good enough for asymptotic bounds on Q^1.

Two-way deterministic, randomized, and quantum communication complexity are defined by allowing Bob to send back to Alice, and there is no constraint on number of rounds of communication. In terms of how much we know today, communication complexity is often seen to be between query complexity (where most is known) and computational complexity (where least is known).

Let us consider a simple example, "equality of two n-bit strings":

$$\mathrm{EQ}(x, y) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$$

Like many other functions, the deterministic communication complexity is n. $R^1(\mathrm{EQ})$ however is exponentially smaller in this case. The idea is fingerprinting. Let $A = \{p \text{ prime}, p \leq n^2\}$, for a randomly chosen p from A the probability that $x = y \pmod p$ is $\frac{|\{p \in A, p|(x-y)\}|}{|A|}$. There are at most n prime factors of $x - y$ but $|A| \in \Theta(n^2/\ln^2 n)$ by the prime number theorem. Thus from $y \bmod p$ and p, Bob can decide whether $x = y$ with bounded error, i.e. $R^1(\mathrm{EQ}) = O(\log n)$.

How about $Q^1(\mathrm{EQ})$? We don't know much more other than $Q^1(\mathrm{EQ})$ is $\Omega(\log\log n)$. The central question is, are there functions where R^1 and Q^1 are asymptotically separated? Exponentially separated? How about in the two-way communication setting? We will answer these questions in the next lecture.

6.845 Quantum Complexity Theory
Fall 2010