6.896 Quantum Complexity 2008-11-25

Lecture 22

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

(Plan of the remaining classes: next Tuesday on classical simulation of quantum circuits, next Thursday Quantum Open House for topics you'd like to hear more about, next next Tuesday project presentation.)

Last time we talked about several results in the setting of one-way communication, which is perhaps the simplest form. Of course we also care about two-way communication, and will discuss problems in both settings today. Basically Alice and Bob each hold some string and want to collectively accomplish some job; we are concerned with how much information they must communicate, rather than the computational feasibility.

We talked about Holevo's theorem, which shows the perhaps surprising result that qubits cannot encode asymptotically more classical bits. We have also seen random access coding, where Bob is only interested in a single bit of Alice's string. But even when Bob only needs to find a single bit of his choice unknown to Alice, asymptotic separation—if exists at all—is no more than a logarithmic additive factor. Today we'll see some separation results.

Notation. $D^1(f), R^1(f), Q^1(f)$ are the one-way deterministic, bounded-error randomized, and bounded-error quantum (respectively) communication complexities. $D(f), R(f), Q(f)$ are the two-way deterministic, bounded-error randomized, and bounded-error quantum (respectively) communication complexities.

Remark. $D^1(f)$ is simply the number of distinct rows in the communication matrix. It can be shown that the definition of R^1 is not changed if zero-error is required. There can be exponential separation between D^1 and R^1, e.g. for "equality of two n-bit strings",

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

Clearly $D^1(\mathrm{EQ}) = n$, $R^1(\mathrm{EQ}) \in \Theta(\log n)$ as we have seen last lecture.

Remark. While looking at asymptotic separation, we can safely confine our attention to pure states (for the qubits to transfer), as any mixed state can be represented by a pure state with twice as many qubits. Mixed states sometimes *do* save a factor of 2, e.g. for EQ. As a side note, we can show $Q^1(\mathrm{EQ}) \in \Omega(\log n)$ by a counting argument. Let $|\psi_x\rangle$ denote the qubits Alice sends to Bob. For every $x \neq x'$ we want $|\psi_x\rangle$ and $|\psi_{x'}\rangle$ to be sufficiently different. How many k-qubit states are there where no two of them have small inner product? The number is in the order of 2^{2^k}. The intuition is to see states as 2^k-bit strings and consider error correcting codes. So with k asymptotically below $\log n$, k qubits cannot help distinguish $2^{2^{\log n}}$ different values of x.

We have seen exponential separation between R^1 and D^1. Is there such separation between Q^1 and R^1? Today we know the answer to be affirmative for partial functions, as partial functions provide much leeway in the definition. But for total functions we are still clueless.

Exponential separation between Q^1, R^1 for partial f

Gavinsky et al. found some partial f where $R^1(f) \in \Theta(\sqrt{n})$ but $Q^1(f) \in O(\log n)$, based on prior work of Bar-Yossef, Jayram and Kerenidis.

Suppose Alice knows the gender $x_1, \ldots, x_n$ of n people where half are male and half female, Bob knows a perfect matching in which either (i) boys are matched to boys, girls to girls, or (ii) every boy is matched to a girl. How much must Alice send, to help Bob decide which case (orientation)?

Remark. If Bob can communicate to Alice he can simply send a pair in the matching using $\log n$ bits to hear back if they are gay.

If Alice sends genders of a random set of people, how large must the set be to contain at least some pair in Bob's matching? This is the birthday paradox, so $R^1(f) \in O(\sqrt{n} \log n)$. The $\log n$ factor used to store the index can in fact be eliminated, giving $R^1(f) \in O(\sqrt{n})$.

Let Alice simply send the equal superposition of all x_i (superposition of basis states $|i\rangle$ phase-shifted by x_i):

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$$

Let $\mathcal{M}$ denote Bob's matching. Bob makes up some function satisfying $g(i) = g(j)$ iff $(i, j) \in \mathcal{M}$, and computes

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle |g(i)\rangle$$

Measuring the first qubit in a basis containing $\frac{|i\rangle + |j\rangle}{\sqrt{2}}, \frac{|i\rangle - |j\rangle}{\sqrt{2}}$ for any $(i, j) \in \mathcal{M}$ will collapse the state to

$$\frac{(-1)^{x_i}|i\rangle + (-1)^{x_j}|j\rangle}{\sqrt{2}}$$

for some $(i, j) \in \mathcal{M}$. Then $x_i \oplus x_j$ (i.e. gay or straight) can be readily found by measuring in Hadamard basis. We can see that this $O(\log n)$ protocol is zero-error.

The hard part of the separation proof is, as usual, to show the lower bound $\Omega(\sqrt{n})$ for $R^1(f)$. This is also from Gavinsky et al.

No strong separation when Bob's input is small

It turns out (Aaronson 2004) that $D^1(f) \in O(mQ^1(f) \log Q^1(f))$ for all partial and total f, where m is the length of Bob's input. The proof technique is the same as in the argument that $\mathbf{BQP}/qpoly \subseteq \mathbf{PostBQP}/poly$ where we start with a maximally mixed state. In this setting Alice has to specify each input bit of Bob, that is why there is a factor of m. This result implies that m must be large for any function to provide strong separation between Q^1 and D^1. For large m, there can indeed be exponential separation as we saw above.

The Inner Product Problem

This is a problem that seems specifically designed to maximize communication complextixy. Alice and Bob hold vectors x and y; they want to find the inner product mod 2.

Unsurprisingly, the classical and randomized communication complexities are both $\Omega(n)$. As it turns out, there is an incredibly slick proof that $Q^1(f)$ and $Q(f)$ are also $\Omega(n)$.

Proof. Suppose there is a quantum protocol requiring less than n qubits. Then Bob can run the protocol on superposition of all possible inputs:

$$\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{xy} |y\rangle$$

Given this state, Hadamard it would give Bob the state x, just like the Bernstein-Vazirani problem. This means Bob can learn Alice's input using less than n qubits, contradicting Holevo's theorem. You can prove Holevo's theorem even in the setting of two-way communication, so $Q(f)$ cannot be below $\Theta(n)$. (If Alice and Bob share entangled qubits, we can save a factor of 2 but no more, so the bounds remain). □

Exponential separation between Q, R for partial f

Raz 1999 defined a problem where, albeit highly contrived, qubits exponentially outperform classical bits. Alice holds some $\vec{v} \in \mathbb{C}^n$ and bases of two orthogonal subspaces S_1, S_2 of $\mathbb{C}^n$, Bob holds a unitary matrix U, how much must they communicate to find whether $U\vec{v} \in S_1$ or $U\vec{v} \in S_2$ (provided that one of them holds)? Raz proved that no classical protocol is below $\Omega(n^{1/4}/\log n)$. The quantum protocol is ridiculously simple (and you guessed it): Alice sends $\vec{v}$, Bob sends back $U\vec{v}$!

The Disjointness Problem

To this day we do not know of any total function that asymptotically separates Q^1 and R^1 (Scott conjectures such functions to exist), but we do have a candidate where Q and R are only quadratically related (although we know of no function that exponentially separates them).

The asymptotic separation between Q, R on the Disjointness Problem (or more aptly, the non-disjointness problem) was found by Buhrman-Cleve-Widgerson 1998. Consider the situation where Alice and Bob each have a set of available dates (as n-bit strings x and y); how much must they communicate to find a commonly available date (an i with $x_i = y_i = 1$)? That $D(\text{DISJ}) \in \Omega(n)$ is obvious, $R(\text{DISJ}) \in \Omega(n)$ is proved by Razborov, as well as Kalyasundaram-Schnitger.

In the quantum case, what happens if we just plug in Grover's algorithm?

1. Alice prepares the state $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle|x_i\rangle$ and sends to Bob
2. Bob applies phase shift and sends back $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i y_i}|i\rangle|x_i\rangle$
3. Alice applies Grover's operator on $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i y_i}|i\rangle$ and sends to Bob
4. ...

This "distributed Grover's algorithm" shows that $Q(\text{DISJ}) \in O(\sqrt{n} \log n)$, where the $\log n$ factor is needed to represent an index. In fact Razborov 2002 proved that $Q(\text{DISJ}) =$

$\Omega(\sqrt{n})$, the proof ultimately invokes the polynomial method on multiple variables and applies symmetrization.

Aaronson-Ambainis 2003 showed that the bound is tight by producing a $O(\sqrt{n})$ communication protocol.

This result in Aaronson-Ambainis 2003 comes from the study (in the same paper) of a an unrelated problem: using Grover's algorithm "in practice", in a model where input bits are spatially separated (like turing machine rather than random access machine) but can have any physically realistic layout (i.e. not restricted to the 1-d "tape" layout). Thus to query an input bit the quantum robot (like head of a turing machine) must move to that input bit. If input is a 1-d matrix, Grover's algorithm is no faster than simply walking through the input bits. Likewise if the database is 2-d, as moving to the queried bit requires $O(\sqrt{n})$ steps (along both axes), i.e. $O(n)$ steps for $O(\sqrt{n})$ queries. If the database is a 3-d matrix, one can show that $O(n^{5/6})$ time is needed. On dimension high enough it has been shown that $O(\sqrt{n})$ steps suffice for quantum random walks. Aaronson-Ambainis shows how to archive $O(\sqrt{n})$ time in 3-d. The basic idea is to apply Grover recursively:

Suppose the database is 2-d. Divide it into $\sqrt{n}$ equal subsquares. Each subsquare can be searched in $O(\sqrt{n})$ steps classically, so if we apply Grover to query which of the $\sqrt{n}$ subsquares contains a 1-entry, $O(\sqrt[4]{n}\sqrt{n}) \in O(n^{3/4})$ time is enough. Now let us recursively do this: use the $O(n^{3/4})$ algorithm on each subsquare. This idea will eventually lead to $O(\sqrt{n}\log^2 n)$ running time. (There are more technical concerns, such as taking care of increased error probability due to repeated Grover). On a 3-d database this approach takes $O(\sqrt{n})$ steps.

Aaronson-Ambainis uses this idea to define a $O(\sqrt{n})$ communication protocol, where x and y are treated as 3-d matrices. Rathen than communicate the indices as done in the $O(\sqrt{n}\log n)$ protocol, Alice and Bob communicate their moves in the matrices, which is no more than $O(\sqrt{n})$.

Brief summary

For one-way communication: (i) we do not know of any total function separating Q^1, R^1 asymptotically; (ii) we do know partial functions that separate Q^1, R^1 even exponentially.

For two-way communication: (i) we do know total functions that separate Q, R asymptotically (quadratically), but not exponentially; (ii) we do know partial functions that separate Q, R exponentially.

6.845 Quantum Complexity Theory
Fall 2010