6.896 Quantum Complexity Theory 2 December 2008

Lecture 23

Lecturer: Scott Aaronson

Last time,

1. **2-way communication**: exponential separation for promise problem (Raz), quadratic separation for total function, unknown if there's an exponential separation for total function.
2. **1-way communication**: exponential separation for promise problem, unknown if there's any asymptotic separation for total function. Problem that I conjecture gives a quadratic separation: group membership.

In our last class, we considered some examples of separations in quantum one-way and two-way communication. We don't know any total function for which we can prove that quantum one-way communication gives you any asymptotic advantage over classical one-way communication. We do have a candidate for such a problem: group membership. Suppose that there is some finite group G that is known to both Alice and Bob. Alice has a subgroup $H \leq G$ and Bob has some element $x \in G$. Alice can send a message M_H to Bob that encodes information about H. To specify any subgroup, she requires $\log^2 N$ bits, where N is the order of the group, but only $\log N$ qubits. The open problem here is to prove that any classical communication protocol only requires $\log^2 N$ bits. Note that if G is Abelian, then there is no separation between classical and quantum communication in this problem. If such a separation were to exist, then G would have to be badly non-Abelian.

1 Classical Simulations of Quantum Circuits and Stabilizers Circuits

It turns out that quantum circuits that can be efficiently simulated classically: not quite a unified field, but rather a collection of interesting ideas that people have had. Two reasons I like this area:

- Unlike almost everything else in this course, it actually has some practical applications today! Physicists and chemists care about these sorts of things, particularly density functional theory.
- Illustrates the subtlety of quantum speedups.

It seems that almost all sets of gate we choose are universal, however, this is not necessarily true. We'll start off by considering stabilizer circuits and the Gottesmann-Knill theorem.

Theorem 1 (Gottesmann-Knill) *Any circuit composed of CNOT, Hadamard and phase gates can be efficiently simulated on a classical computereven though such circuits can generate huge amounts of entanglement, and can be used for superdense coding, quantum teleportation, the GHZ paradox, quantum error-correcting codes, etc.*

The idea here is that we can specify a quantum state $|\psi\rangle$ by listing a bunch of unitary matrices that stabilize $|\psi\rangle$, i.e., such that $U|\psi\rangle = |\psi\rangle$. Note that if U and V stabilize $|\psi\rangle$, then UV and U^{-1} also stabilize $|\psi\rangle$. Thus, the set of stabilizers of $|\psi\rangle$ forms a group, called the stabilizer group. We're going to specify a state by giving a set of generators for its stabilizer group. If we start with some initial computational basis state $|00\rangle$, then the actions of the stabilizers gates are:

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle + |10\rangle \\ &\rightarrow |00\rangle + |11\rangle \\ &\rightarrow |00\rangle + i|11\rangle \end{aligned} \tag{1}$$

for a Hadamard, CNOT, and phase gate, respectively. You'll notice that we can only produce equal superpositions over some affine subspace using these gates.

If a state can be generated (starting from $|00\ldots00\rangle$) by CNOT, Hadamard, and phase gates, it turns out that its stabilizer group consists of particularly simple unitaries: namely, tensor products of Pauli matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2}$$

The squares of these matrices resolve the identity

$$X^2 = Y^2 = Z^2 = I, \tag{3}$$

and their products are closed under cyclic permutation

$$\begin{aligned} XY &= iZ = -YX \\ YZ &= iX = -ZY \\ ZX &= iY = -XZ. \end{aligned} \tag{4}$$

They behave exactly as quarternions, in case you've seen those.

As an example, let's look at the two-state computational basis. Their stabilizers are given by:

Gate	Stabilizer Set
$\|0\rangle$	$\{I, Z\}$
$\|1\rangle$	$\{I, -Z\}$
$\frac{1}{\sqrt{2}}(\|0\rangle \pm \|1\rangle)$	$\{I, \pm X\}$
$\frac{1}{\sqrt{2}}(\|0\rangle \pm i\|1\rangle)$	$\{I, \pm Y\}$

The two-qubit initial state is stabilized by $\{ZZ, IZ, ZI, II\}$, so it's stabilizers representation is $\{ZI, IZ\}$. In our classical simulation of a quantum circuit, this list of generators is going to be our succinct representation of the quantum state. How many bits does that representation require, for an n-qubit state? Well, each Pauli matrix takes 2 bits, so each generator requires $2n$ bitsactually $2n+1$, since there might be a minus sign in front. And it turns out we always have exactly n generators (yielding a stabilizer group of order $2n$). So, $n(2n+1)$ bits total.

The key question, of course, is how to update this representation when a CNOT, Hadamard, or phase gate is applied. Rather than prove rigorously what happens, I'll just illustrate the rules through examples. Let's apply these gates to an initial tensor product state $|00\rangle$ and see what happens,

Gate	Stabilizer Generators
$\|00\rangle$	$\{IZ, ZI\}$
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|0\rangle$	$\{XI, IZ\}$
$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)\|0\rangle$	$\{YI, \pm IZ\}$
$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)\|0\rangle$	$\{-XI, \pm IZ\}$

In general, after Hadamarding the ith qubit, we go through the ith column of the matrix swapping X's with Z's, and Y's with Y's. For the phase gate, go through the ith column mapping X to Y to X to Y. For the CNOT gate, $XI \rightarrow XX$, $IX \rightarrow IX$, $ZI \rightarrow ZI$, and $IZ \rightarrow ZZ$. From these rules, we can show that $YI \rightarrow YX$.

One thing I haven't told you is how to handle measurement. Given a stabilizer state, every measurement of a qubit in the standard basis returns the outcome $|1\rangle$ with probability either 0, 1, or 1/2. Our task is to figure out which. Well, if the ith row contains an X or Y, then the probability is going to be 1/2. Why? Because if the ith qubit were either definitely $|0\rangle$ or definitely $|1\rangle$, it couldn't possibly be stabilized by X or Z. If the ith row contains only I's and Z's, then the probability is going to be either 0 or 1. Why? Because in that case, one can prove that either $IIZII$ or $IIZII$ (i.e., a Z at the ith qubit and I's everywhere else) must be in the stabilizer group. If $IIZII$ stabilizes the state, then the measurement outcome has to be $|0\rangle$, while if $IIZII$ stabilizes it, then the measurement outcome has to be $|1\rangle$. So we just have to figure out which. But this is a linear algebra problem, which is solvable in polynomial time using Gaussian elimination! Total running time: $O(n)$ per CNOT, Hadamard, phase gate, $O(n^3)$ to simulate a measurement.

In 2004, I decided to implement the Gottesman-Knill simulation algorithm for a course project, but I didn't feel like implementing Gaussian elimination. So Gottesman and I developed a better algorithm, which uses only $O(n^2)$ time to simulate a measurement. We also proved that the problem of simulating a stabilizer circuit is complete for the class $\oplus L$, a subclass of P (under L-reductions). To put it another way, stabilizer circuits have exactly the same computational power as circuits with CNOT gates only. So they're presumably not even universal for classical computation.

2 Match Gates

For a given $n \times n$ matrix A, we can define the *permanent* and the *determinant*,

$$\text{per}(A) = \sum_{\sigma} \prod_{i=1}^{n} a_{i\sigma(i)} \longleftrightarrow \det(A) = \sum_{\sigma} (-1)^{\text{sign}(\sigma)} \prod_{i=1}^{n} a_{i\sigma(i)}. \tag{5}$$

Theorem 2 (Valiant) *Permanent is #P-complete.*

Since BQP$\subseteq$P$^{\#\text{P}}$, this means in particular that the problem of simulating a quantum computer can always be reduced to computing the Permanent of some matrix. Well, but that doesn't help much, since the Permanent is #P-complete! As we know, determinant is computable in classical polynomial time (using Gaussian elimination).

So, if only there were some interesting subclass of quantum computations that reduced to the determinant instead of the permanent! Indeed there is such a subclass—Valiant called them matchcircuits, and wrote a paper developing the theory of them purely mathematically. Then something funny happened: Terhal and DiVincenzo wrote a follow-up paper pointing out that what Valiant had essentially done is rediscovered fermions.

So far in this course, we haven't had to say anything about particles, but it turns out that particles come in two types: bosons and fermions. Bosons are generally force particles like photons; fermions are generally matter particles like quarks. Mathematically, the crucial difference between them has to do with how you add up amplitudes. Let's say we have 2 identical particles that don't interact with each other, and we just want to know the amplitude for them evolving into some new configuration. How can we calculate that configuration? Well, we can take the amplitude for this particle going here multiplied by the amplitude for that particle going there. What else do we need to consider? Right: the cross term. So we get $ab + cd$. Seems obvious! And indeed, that's exactly what happens with bosons.

But there's another possibility, which is realized by fermions: that we have to take $ab - cd$. (You might wonder, why not $cd - ab$? Well, we can only determine the amplitude up to a sign, but amplitudes are only ever determined up to a sign anyhow!) In general, suppose we have n identical, non-interacting particles, and let a_{ij} be the amplitude for particle i going to position j. Form the matrix $A = (a_{ij})$. Then if the particles are bosons, the amplitude for this whole process is $\operatorname{per}(A)$, while if they're fermions, the amplitude for this whole process is $\det(A)$.

3 The Future

Open problems!

6.845 Quantum Complexity Theory
Fall 2010