CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Tuesday, February 6 - Lecture 5.1

Today's scribe: Asini

Reading: Chapter 1 of Nielsen and Chuang.

Agenda:

1. Quantum Advantage
2. Quantum Teleportation
3. Deutsch-Jozsa Algorithm

1 Quantum Advantage

$|\psi\rangle \in \mathscr{H}_1 \otimes \mathscr{H}_2$ is **unentangled**, or *separable*, if $|\psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \in \mathscr{H}_1 \otimes \mathscr{H}_2$. Not all states are separable. Non separable states are called *entangled*. An *entangling unitary* is a unitary $U : \mathscr{H}_1 \otimes \mathscr{H}_2 \to \mathscr{H}_1 \otimes \mathscr{H}_2$ that is not of the form $U_1 \otimes U_2$ for some $U_1 : \mathscr{H}_1 \to \mathscr{H}_1$ and $U_2 : \mathscr{H}_2 \to \mathscr{H}_2$.

If we try to do quantum mechanics only with separable or unentangled things, then we would "only" have classical probability at our disposal. So quantum computing might be understood as "applied entanglement", i.e., using entaglement as a computational resource.

On the other hand, quantum information theory (in the narrow sense) is the study of quantum entanglement per se i.e., as a thing we want to quantify in various ways. Quantum information theory seeks to measure entanglement via things like"entanglement entropy" and "entanglement monotones."

Quantum advantage (or proofs that there is no quantum advantage for a certain problem) is the main goal of quantum computing theory (in narrow sense). There are two main domains of well characterized quantum advantage.

- Hidden subgroup problems
- Unstructured search (aka Grover's algorithm)

Hidden subgroup problems

Includes the "quantum part" of Shor's algorithm. Good new is this provides exponential advantage in "query complexity". The bad news is query model is unrealistic (in general).

Unstructured search (aka Grover's algorithm)

Good news here is we can find a needle in a haystack of size N in time $\sqrt{N}$. Bad news is this can't do better than $\sqrt{N}$. Worse error in quantum overhead might negate any advantage!

Other domains

Other frameworks for potential quantum advantage exist but their potential advantage tends to be poorly characterized (by the standards of CS theory, that is):

1. HHL algorithm for matrix inversion, i.e., solving $A\vec{X} = B$ where A is sparse.
2. Quantum optimization/ VQE/ Quantum annealing/ Adiabatic quantum computing. (Use quantum annealing to find minima of energy landscapes)

Also important, but for somewhat different reasons:

- Quantum simulation
- Quantum random walks/Monte Carlo

Quantum advantage is also something that can be explored in information theoretic sense (rather than the computational/algorithmic sense). Examples are

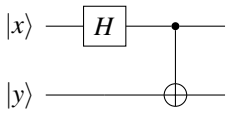
- Bell inequalities
- Entanglement games

2 Quantum Teleportation

Define the four *Bell States* (aka *EPR pairs*) on a pair of qubits as follows:

- $|\beta_{00}\rangle = |00\rangle + |11\rangle$
- $|\beta_{01}\rangle = |01\rangle + |10\rangle$
- $|\beta_{10}\rangle = |00\rangle - |11\rangle$
- $|\beta_{11}\rangle = |01\rangle - |10\rangle$

Theses states come from applying the following circuit to the computational basis:



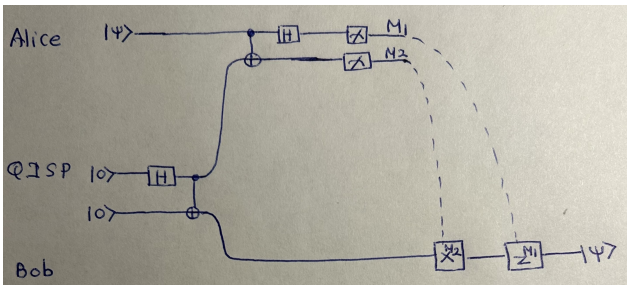
We will now use Bell pairs to do "quantum teleportation."

Claim: To build a quantum network it suffices to have a classical network and some "tubes" that can move individual qubits in Bell states around.

We imagine a scenario where we have three parties: Alice and Bob (who both have quantum computers at home), and also a "Quantum Internet Service Provider" (QISP) who owns the pipes that can be used to move the qubits in Bell pairs around, in particular, sending some to Alice and others to Bob. (We also suppose there is a classical ISP around.)

Suppose Alice wants to send the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob. Critically, we don't want to assume Alice knows the values of α or β (since in that case, she could just call Bob on the phone and tell him, although the phone call might be pretty long depending on how many bits of precision she whats to share). Rather, we want Alice to be able to send $|\psi\rangle$ to Bob simply by sending two bits of *classical* information. Bob We obtain following result from the circuit. Critically, for this to succeed, we need Alice and Bob to each possess one half of a Bell pair, which is where the QISP comes in.

Consider the following circuit.



This is called the teleportation protocol. Note that the dashed lines indicate that Alice is sending Bob *classical* information (e.g. over the good ole' classical internet). The thing to check is that Bob really is left with the state $|\psi\rangle$ at the end. This is a relatively simple exercise in algebra, using the following two identities:

$$\begin{aligned}
CNOT_{1,2}(|\psi\rangle|\beta_{00}\rangle) &= CNOT1,2(\alpha|0\rangle+\beta|1\rangle)\otimes(|00\rangle+|11\rangle) \\
&= CNOT_{1,2}(\alpha|000\rangle+\alpha|011\rangle+\beta|100\rangle+\beta|111\rangle) \\
&= \alpha|000\rangle+\alpha|011\rangle+\beta|110\rangle+\beta|101\rangle \\
&= \alpha|0\rangle\otimes(|00\rangle+|11\rangle)+\beta|1\rangle\otimes(|10\rangle+|01\rangle) \\
H(\alpha|0\rangle\otimes(|00\rangle+|11\rangle)+\beta|1\rangle\otimes(|10\rangle+|01\rangle)) &= \alpha|+\rangle\otimes(|00\rangle+|11\rangle)+\beta|-\rangle\otimes(|10\rangle+|01\rangle) \\
&= |00\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)+|01\rangle\otimes(\alpha|1\rangle+\beta|0\rangle) \\
&\quad +|10\rangle\otimes(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\otimes(\alpha|1\rangle-\beta|0\rangle)
\end{aligned}$$

3 Deutsch–Jozsa Algorithm

We will now give another example of the weird power of entanglement called the Deutsch-Jozsa algorithm. It is one of the simpler examples of a class of problems called the *hidden subgroup problem*. (Shor's factoring algorithm is another example of a hidden subgroup problem algorithm, modulo some classical reductions...)

Suppose we're given a boolean function $F:\{0,1\}^n\to\{0,1\}$ which is *promised* to satisfy one of the following two properties:

1. F is constant
2. F is balanced, meaning number of elements in $\{F^{-1}(0)\}$ = number of elements in $\{F^{-1}(1)\}$

Our task is to decide which of the two properties F has. This is called the Deutsch-Jozsa problem.

Before solving this problem using quantum mechanics, let me cop to something: it is *highly* contrived. You are almost surely never going to encouter a function F in "the real world" that is constant or balanced, but you just don't know of the two is the case. Nevertheless, if we have *quantum* access to such a highly contrived F, then we can decide whether it is constant or balance more quickly than *any* classical (deterministic) algorithm. This is surely remarkable and interesting, even if it isn't immediately useful.

So, we must decide which of the two conditions F satisfies. How hard is it to do? With a classical deterministic algorithm, we need at least $2^{n-1}+1$ calls to F to decide. That is,the best we can do is check the value of F on half of its input, plus one. Note that if F is not constant, if we're lucky, we'll see this before having to check so many inputs. But, critically, if we want to be *certain* that F is NOT constant, then, determinastically, the best we can do is check half plus one of its inputs.

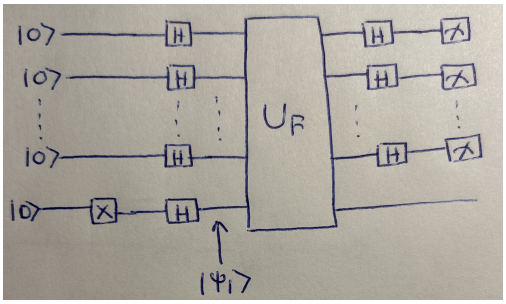
The Deutsch-Jozsa algorithm shows that on a quantum computer with "Quantum oracle access to F", only one call to the oracle is enough to decide with certainty whether F is constant or balanced!

How does this work? First of all, we need *quantum* oracle access to F, which we will assume we have via the "unitary dilation," as we have discussed before:

$$\begin{aligned}
U_F:\ (\mathbb{C}^2)^{\otimes n}\otimes\mathbb{C}^2 &\to (\mathbb{C}^2)^{\otimes n}\otimes\mathbb{C}^2 \\
|b,y\rangle &\mapsto |b,f(b)\oplus y\rangle
\end{aligned}$$

Claim: With only one call to the black box unitary U_F we can determine if F is balanced or constant with certainty.

The algorithm is summed up by the following circuit:



I claim that after measuring the output in the above circuit as indicated, we either see $0\cdots 0$ with probability 1 (in which case F is constant) or we do not see $|0\cdots 0\rangle$ with any probability (in which case F is balanced). Indeed, this follows from a fairly elementary calculation.

Write

$$|\psi_1\rangle = \sum_x |x\rangle \otimes |-\rangle .$$

Then applying U_F to this state we get

$$U_F |\psi_1\rangle = \sum_x |x\rangle \left(|0 \oplus F(x)\rangle - |1 \oplus F(x)\rangle\right) = \sum_x (-1)^{F(x)} |x\rangle \otimes |-\rangle$$

Now apply the last round of Hadamards:

$$H^{\otimes n} \otimes id\left(\sum_x (-1)^{F(x)} |x\rangle \otimes |-\rangle\right) = \sum_{x,z} \frac{(-1)^{x\cdot z + F(x)}}{2^n} |z\rangle \oplus |-\rangle$$

Notice that in the exponent of (-1) here, we're taking the mod 2 dot product $x \cdot z$ and then adding $F(x)$ to it (mod 2).

Finally, let's compute the amplitude of $|0\cdots 0\rangle \otimes |-\rangle$ on our output state:

$$\sum_x \frac{(-1)^{x\cdot 0 + F(x)}}{2^n} = \begin{cases} (-1)^{F(x)} & \text{if } F(x) \text{ is constant} \\ 0 & \text{if } F(x) \text{ is balanced} \end{cases}$$

Staring hard and thinking about what this means if we measure in teh computational basis, we come to the following conclusion: if we measure the first n bits of the output of the above circuit, then the probability that we see all 0's is 1 if F is constant, and 0 if F is balanced. In other words, after measuring the output of the above circuit, if we see all zeroes, then we can be certain that F is constant, and if we do not see all zeroes, then we can be certain that F is balanced. Thus, we only had to query U_F once to decide if F is constant or balanced. Wild stuff!