Theorist's Toolkit **Spring 2019**

Lecture 12: Quantum

Scribe: Vishnu Iyer, Robert Wang May 10

12.1 Qubits, and Entanglement

The basic unit of information in a quantum computer is a qubit, which is a quantum particle that, when measured, can take on one of two possible states 0 or 1, which we denote as the basis states, $|0\rangle$ and $|1\rangle$. For example, a qubit could be an electron and the basis states could be the direction of the electron's spin. Alternatively, a qubit could be a photon, and the basis states could be it's polarization. If we don't measure the state of a qubit, then it is an a superposition of both basis states, which we can represent as a linear combination of the basis states. We call the state of the superposition the general state of the qubit. Thus, we can write a qubit, ψ, as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ are called the amplitudes of the basis states, respectively. Moreover, if our system consists of n qubits, then it is in a superposition of 2^n possible basis states, each with it's own amplitude. Thus, we can write the qubit as $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$. If we were to measure the state of the qubit, then the probability of observing it in the basis state $x \in \{0,1\}^n$ is $|\alpha_x|^2$. This means that the amplitudes must satisfy $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$. If we observe a system of qubits in the basis state x, then we have collapsed it's superposition to state x, which means each subsequent observation of the system will be in state x. Two examples of important qubits are:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Note that for each of these two qubits, the probability of observing them in either basis state is $1/2$.

12.1.1 Vector Representation

We can represent the state of the superposition of a system of qubits as a vector in $\mathbb{C}^{2^n}$, with respect to the orthonormal basis, $\{|x\rangle, \forall x \in \{0,1\}^n\}$. For a single qubit, we can represent the basis as:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

And if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ then:

$$|\psi\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$$

Similarly, the basis states for a two qubit system are:

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} |10\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} |01\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

By convention, we call $|x\rangle$ as *"ket x"*. And we also have $\langle x| = |x\rangle^\top$, which we call *"bra x"*. Naturally, we use the notation $\langle x|y\rangle$ to denote the dot product between the amplitudes of qubits x and y. This means that in order for x to be a valid qubit, we must have $\langle x|x\rangle = 1$.

If we have a system of multiple qubits whose states are independent of each other then the resulting superposition is the tensor product of the superpositions of each qubit. That is, if $|xy\rangle = |x\rangle \otimes |y\rangle$. This means that measuring one qubit in the system tells us nothing about the states of the other qubits in the system. For example, consider the system of two qubits in the $|+\rangle$ state:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

By taking the square of each entry, we see that if both qubits are uniformly distributed over it's two possible basis states, then the system of two qubits is uniformly distributed over all four possible basis states.

12.1.2 Entanglement

Intuitively, we can think of entangled qubits as being not independent. Formally if a system of qubits is entangled, then their superposition cannot be decomposed into tensor products of the superpositions of each individual qubit.

Definition 12.1. *(Entanglement) If qubits $x_1, ...x_n$ are entangled, then $|x_1x_2...x_n\rangle \neq |x_1\rangle \otimes |x_2\rangle \otimes ... |x_n\rangle$*

An example of entanglement in a two-qubit system is the Bell state:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Note that measuring the first qubit will collapse the whole system and complete determine the state of not only the first qubit, but also the second qubit.

12.2 Quantum Circuits

In a quantum circuit, qubits pass through gates, which alter the state of their superposition. Since we can represent the state of a system of qubits as a vector, we can represent a process that alters the state of a system of qubits as a linear operator, which can be represented by a squre matrix. For example, if U is a gate in a quantum circuit, then it maps $|x\rangle$ to $U|x\rangle$. The operator must satisfy the following properties:

- **Linear:** $U(a|x\rangle + b|y\rangle) = aU|x\rangle + bU|y\rangle$
- **Unitary:** $U^\top U = I$

We need the operator to be unitary because the resulting state, $U|x\rangle$ must be a valid qubit state, meaning that $(U|x\rangle)^\top U|x\rangle = \langle x|U^\top U|x\rangle = \langle x|x\rangle = 1$. Thus, $U^\top U = I$. Note that passing a system of qubits through multiple gates, $U_1, U_2, ...U_n$ is the same as multiplying by the matrix $U_1U_2...U_n$. The following are a few examples of quantum gates. Note that since each gate is a linear transformation, we can determine the behavior of each gate based on its behavior on the basis states.

12.2.1 Hadamard Gate:

For a one-qubit system, the Hadamard operator can be represented by the following matrix:

$$H_1 = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Now, consider the behavior of the Hadamard operator on the basis states:

$$H_1|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad H_1|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Note that this means if a qubit started in a particular state, after passing through the Hadamard gate, it is equally likely to be in either state. Thus, we can think of the Hadamard gate as the box and the qubit as Schrodinger's cat. For a system of n-qubits, we define H_n recursively as:

$$H_n = \frac{1}{\sqrt{2}}\begin{bmatrix}H_{n-1} & H_{n-1}\\ H_{n-1} & -H_{n-1}\end{bmatrix}$$

Note that applying H_n to a system of n qubits is the same as taking the tensor product of H_1 applied to each individual qubit.

12.2.2 CNOT Gate

The CNOT gate is an operator on a 2-qubit system. It has the matrix representation: C =

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

Note that it has the following behavior on the basis:

$$C|00\rangle = |00\rangle \quad C|01\rangle = |01\rangle \quad C|10\rangle = |11\rangle \quad C|11\rangle = |10\rangle$$

Inuitively, the first qubit acts as a control element (which does not change itself) that determines whether or not to apply the NOT operation to the second bit.

12.2.3 Generation of Bell State

Consider the following quantum circuit:

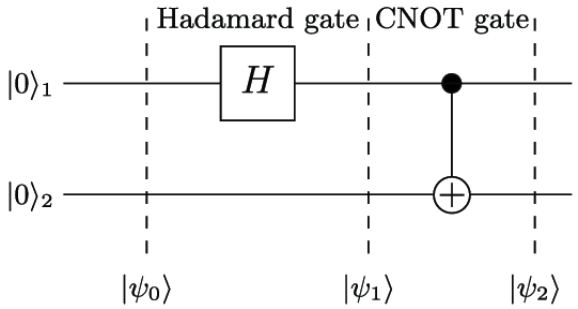

Figure 12.1: example quantum circuit

We can track the evolution of the state throughout the circuit:

$$\begin{aligned}
|\psi_0\rangle &= |0\rangle \oplus |0\rangle \\
|\psi_1\rangle &= H|0\rangle \oplus |0\rangle \\
&= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \oplus |0\rangle \\
&= \frac{|00\rangle + |10\rangle}{\sqrt{2}} \\
|\psi_2\rangle &= \frac{C|00\rangle + C|10\rangle}{\sqrt{2}} \\
&= \frac{|00\rangle + |11\rangle}{\sqrt{2}}
\end{aligned}$$

Thus, using this circuit, we have generated a bell state from the initial basis state: $|00\rangle$.

12.3 Quantum Complexity

Simply arguing that quantum computers are "fast" isn't enough to prove that quantum computers are at least as powerful as classical computers. To do so, one must show that any classical circuit can be implemented by a quantum circuit. In classical computation, the NAND gate is universal, meaning that any circuit can be implemented using only the NAND gate. An analogous quantum gate is the Toffoli gate, also known as the CCNOT gate. The Toffoli gate acts on systems of 3 input qubits. The first two qubits act as control elements, and the last bit is flipped iff the first two qubits are both in the 1 state. The Toffoli gate is universal, meaning that any classical circuit can indeed be implemented by a quantum circuit.

Another question to ask about quantum computers is what problems can be solved efficiently by a quantum computer. For that, we define the class BQP:

Definition 12.2. *(BQP) BPQ is the set of all languages L such that for any input $x \in L$ of size n, there exists a quantum circuit, A, with $O(poly(n))$ gates such that:*

- *if $x \in L$, $A(x) = 1$ with probability at least $\frac{2}{3}$*

- *if* $x \notin L$, $A(x) = 0$ *with probability at least* $\frac{2}{3}$

Note that BQP just the quantum version of BPP, the set of problems that can be solved on a turning machine in polynomial time with bounded error. In fact, since we can use $|0\rangle, |1\rangle$ and $|+\rangle$ to represent 0, 1, and random bits, and since any classical gate can be replicated with quantum gates, we must have

$$BPP \subseteq BQP$$

Moreover, it can be shown that:

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

However, it is not known what the relationship between BQP and NP is.

12.4 Grover's Algorithm

Now, we consider a simple example of a quantum algorithm. Consider the search problem: Given a function, $f : \{0,1\}^n \to \{0,1\}$, and a unique $z \in \{0,1\}^n$ such that:

$$f(x) = \begin{cases} 0 & x = z \\ 1 & x \neq z \end{cases}$$

Clearly, it must take at least $\Theta(N)$ time for a classical algorithm to solve this problem, where $N = 2^n$. However, we will see that a quantum algorithm can solve this problem in $O(\sqrt{N})$ time. To do this, we need two quantum operations. The query box is an operation, $Q : \{0,1\}^n \to \{-1,1\}$ that is analogous to evaluating $f(x)$ on x. We can define Q by defining it's output on the basis, $|x\rangle$, $x \in \{0,1\}^n$:

$$Q|x\rangle = \begin{cases} -1 & x = z \\ 1 & x \neq z \end{cases}$$

The second operation is the Grover Flip, G, defined such that if a qubit, $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$, then $G|\psi\rangle = \sum_{x\in\{0,1\}^n} 2\mu - \alpha_x |x\rangle$, where $\mu = \frac{1}{N}\sum_{x\in\{0,1\}^n} \alpha_x$ is the average amplitude of $|\psi\rangle$. It can be verified that both Q and G are unitary operators. For Q, this is trivial. For G, we can see that

$$\begin{aligned}
\langle\psi| G^\top G |\psi\rangle &= \sum_{x\in\{0,1\}^n} (2\mu - \alpha_x)^2 \\
&= \sum_{x\in\{0,1\}^n} 4\mu^2 - 4\mu\alpha_x + \alpha_x^2 \\
&= 4N\mu^2 - 4\mu \sum_{x\in\{0,1\}^n} \alpha_x + \sum_{x\in\{0,1\}^n} \alpha_x^2 \\
&= 4N\mu^2 - 4N\mu^2 + 1 \\
&= 1
\end{aligned}$$

Intuitively, the algorithm starts with a system of qubits with uniform probability over all 2^n basis states, and then repeatedly applies Q and G to the system until the probability distribution becomes concentrated at $|z\rangle$. Formally:

1. initialize $|x_0\rangle = H|0\rangle \otimes H|0\rangle \otimes ...H|0\rangle$, n times.

2. set $|x_{i+1}\rangle = QG\,|x_i\rangle$
3. sample $|x_{\sqrt{N}}\rangle$

12.4.1 Analysis

First, notice that:

$$|x_0\rangle = \otimes_{i=1}^{n} \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

which means $|x_0\rangle$ has uniform amplitude over each basis state. Thus, we have:

$$Q\,|x_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq z} |x\rangle - \frac{1}{\sqrt{N}}\,|z\rangle$$

$$GQ\,|x_0\rangle = (2\mu_0 - \frac{1}{\sqrt{N}}) \sum_{x \neq z} |x\rangle - (2\mu_0 + \frac{1}{\sqrt{N}})\,|z\rangle$$

Where μ_0 is the average amplitude of the basis states of $Q\,|x_0\rangle$. Moreover, if we let μ_i be the average amplitude of $Q\,|x_i\rangle$, then, the amplitude of the basis state $|z\rangle$ is $2\mu_i + 2\mu_{i-1} + ...2\mu_0 + \frac{1}{\sqrt{N}}$, and the amplitude of basis state of $|x\rangle$, where $x \in 0, 1^n$ and $x \neq z$, is $2\mu_i - 2\mu_{i-1} + ... \frac{1}{\sqrt{N}}$. Also, note that each iteration, the mean does not change too much, so $\mu_i \approx \frac{1}{\sqrt{N}}$ for each iteration, which means that while the amplitude of $|z\rangle$ increases by around $\frac{2}{\sqrt{N}}$ each time, all other amplitudes stay around the same. Since, the probability of sampling a basis state is the square of it's amplitude, after $O(\sqrt{N})$ iterations, the probability of sampling the z state will be constant value close to 1.

While the search problem can be sped up polynomially by a quantum computer, other problems can be exponentially sped up. For example, the fourier transform can be performed in $O(\log n)$ time with a quantum computer, while the fastest classical algorithm, the FFT, takes $\Theta(n \log n)$ time. Using the quantum fourier transform, Shor's algorithm can factor n-bit numbers in $O(poly(n))$ time, while it is generally believed that factoring cannot be solved efficiently on a classical turning machine.