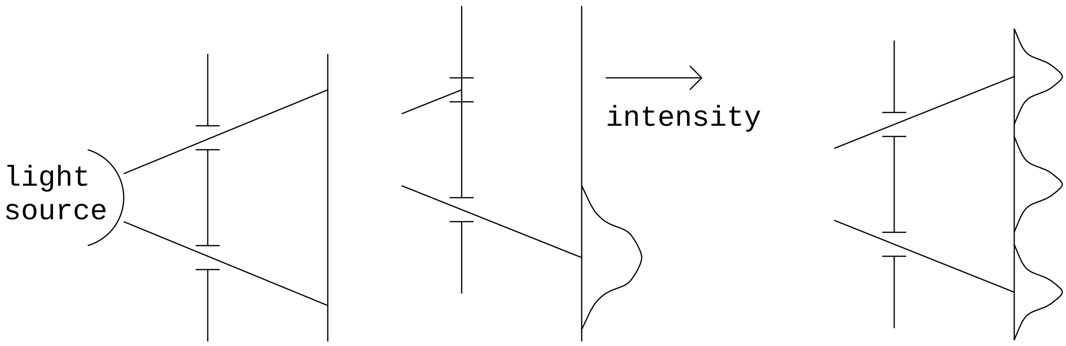
18.405J/6.841J Advanced Complexity Theory	March 13, 2001
Lecture 10	
Lecturer: Dan Spielman	*Scribe: Christopher D. Avrich*

Quantum Computation

This lecture is an introduction to quantum computation. Quantum computation is motivated in part by the field of Physics, and experiments such as the following:



Take a light source and shine it through an opaque barrier with two slits, as shown in the first figure above. If you cover either slit, the intensity of the light against the backdrop forms a predictable pattern, as in the second figure. However, if you allow the light to shine through both slits, you get a somewhat unexpected intensity pattern, as shown in the third figure. The implication of this is that the knowledge of which slit each unit of light has passed through has an effect on where it is possible to observe it striking the backdrop. Quantum computation seeks to capture this phenomenon.

The Church-Turing Thesis states that a Turing Machine can compute any function computable by any reasonable physical device. Modern Theoretical Computer Scientists usually take this to mean "a Turing Machine can compute any function computable by any reasonable physical device, with polynomial slowdown." Quantum computers violate this assumption.

1 Quantum Bits

1.1 One Quantum Bit

Definition 1 *A quantum bit, or qbit, is a linear combination of basis states. These basis states are denoted* $|0\rangle$*, for the vector* $\binom{1}{0}$*, and* $|1\rangle$*, for the vector* $\binom{0}{1}$*. Each qbit has a state* $\alpha|0\rangle + \beta|1\rangle$*, where* α*,* $\beta \in \mathcal{C}$ *(the set of complex numbers), and* $|\alpha|^2 + |\beta|^2 = 1$*. When we measure a qbit, we see* $|0\rangle$ *with probability* $|\alpha|^2$*, and* $|1\rangle$ *with probability* $|\beta|^2$*.*

1.2 Two Quantum Bits

With two quantum bits, the basis states are $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, corresponding to the basis vectors $\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$, $\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$, $\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$, and $\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$, respectively. The state of two qbits is then $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, where $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. (That is, the norm of the vector is 1.)

If we measure both bits, we will see $|ij\rangle$ with probability $|\alpha_{ij}|^2$. If we measure only the first bit, we see 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, and 1 with probability $|\alpha_{10}|^2 + |\alpha_{11}|^2$. If we see 0, our qbits then end up in state

$$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

and if we see 1, our qbits end up in state

$$\frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

For example, if we have $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, we see 0 with probability $\frac{1}{2}$, landing in state $|00\rangle$, and 1 with probability $\frac{1}{2}$, landing in state $|11\rangle$.

If we have $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle$, we see 0 with probability $\frac{3}{4}$, landing in state $\sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|01\rangle$, and 1 with probability $\frac{1}{4}$, landing in state $|10\rangle$.

1.3 n Quantum Bits

With n quantum bits, basis states are $|\bar{x}\rangle$, where $\bar{x} \in \{0,1\}^n$. Similarly to our earlier definitions, the state of n qbits is $\sum_{\bar{x}\in\{0,1\}^n} \alpha_{\bar{x}}|\bar{x}\rangle$, a vector with norm $\sum_{\bar{x}} |\alpha_{\bar{x}}|^2 = 1$. The span of $|0 **...*\rangle$ is a vector space of dimension 2^{n-1}, so to find the probability of seeing 0 on measurement of the first bit, we simply project the state onto the span of $|0 **...*\rangle$, take the norm of the resulting vector, and square it. To find the next state, we project the current state onto the span of$|0 **...*\rangle$, and normalize the resulting vector.

Note: For multiple qbits, each basis state corresponds to the tensor ($\otimes$ operator) of its component single-qbit basis states. This means, for example, $|01\rangle = |0\rangle \otimes |1\rangle$. The $\otimes$ operator is defined:

Definition 2 *For vectors $\bar{a}$ and $\bar{b}$, the tensor of $\bar{a}$ and $\bar{b}$, $\bar{a}\otimes\bar{b}$, equals:*

$$\begin{pmatrix}a_1\\\vdots\\a_n\end{pmatrix} \otimes \begin{pmatrix}b_1\\\vdots\\b_m\end{pmatrix} = \begin{pmatrix}a_1b_1\\\vdots\\a_1b_m\\a_2b_1\\\vdots\\a_2b_m\\\vdots\\a_nb_1\\\vdots\\a_nb_m\end{pmatrix}$$

For matrices A and B, where A is n by m, $A \otimes B$ equals:

$$\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nm}B \end{pmatrix}$$

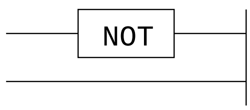
Therefore, $|01\rangle = |0\rangle \otimes |1\rangle$, since $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$.

2 Quantum Gates

Definition 3 *A quantum gate on n qbits is a 2^n by 2^n unitary matrix. (A matrix U is unitary if $\bar{U}^t \cdot U = I$, where $\bar{U}^t$ is the conjugate transpose of U.) When qbits are passed through a gate, we multiply the qbits' state vector by the gate's matrix to obtain the qbits' new state.*

2.1 Not Gate

For a one-qbit not gate, we want $|0\rangle \to |1\rangle$ and $|1\rangle \to |0\rangle$. The matrix is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Consider the following quantum circuit (the vertical bar represents taking a measurement):

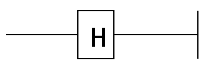


For this circuit, we want $|00\rangle \to |10\rangle$, $|01\rangle \to |11\rangle$, $|10\rangle \to |00\rangle$, and $|11\rangle \to |01\rangle$. The matrix for this circuit is $\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, which is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

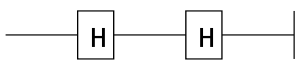
2.2 Hadomard Gate

Definition 4 *A Hadomard gate is a one-qbit gate with matrix $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.*

This gate causes $|0\rangle \to \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, and $|1\rangle \to \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. Consider the following quantum circuit:



If we input $|0\rangle$ into this circuit, we obtain $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Measuring the qbit at the vertical line will therefore show 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. Now consider this circuit:

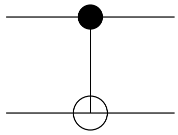


Interestingly, if we input $|0\rangle$ into this circuit, we will measure 0 with probability 1. This is because $H \cdot H = I$, the identity matrix. (The first Hadomard gate gives us $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, and the second gives us $\frac{1}{2}|0\rangle + \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle - \frac{1}{2}|1\rangle$, which is equal to $|0\rangle$).

For n Hadomard gates in parallel (on n qbits), with input $\bar{x} \in \{0,1\}^n$, output becomes

$$\sum_{\bar{y} \in \{0,1\}^n} 2^{-n/2} (-1)^{\bar{x} \cdot \bar{y}} |\bar{y}\rangle$$

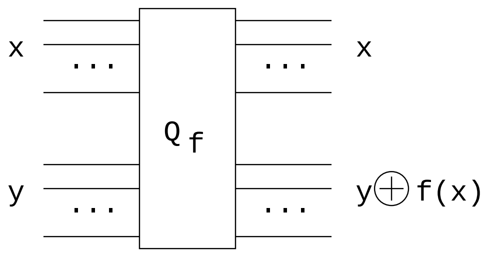
2.3 Controlled Not Gate



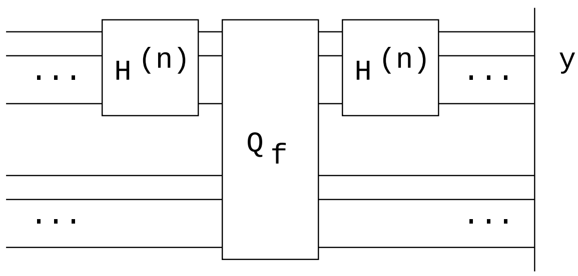
A controlled not gate is a 2-qbit gate (as shown above). The first (top) qbit is the control bit, which determines whether or not the second (bottom) qbit is negated. This gate causes $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |01\rangle$, $|10\rangle \rightarrow |11\rangle$, and $|11\rangle \rightarrow |10\rangle$, and has matrix $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

3 Simon's Algorithm (1994)

Claim 5 *For any function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ that is computable with a conventional circuit of G gates, we can build a quantum circuit $Q_f : \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^n \times \{0,1\}^m$ which will compute $(x, y) \rightarrow (x, y \oplus f(x))$, and which will have $O(G)$ quantum cost:*



Theorem 6 *Given a circuit computing function $f : \{0,1\}^n \rightarrow \{0,1\}^n$, and a promise that either f is $1:1$, or f is $2:1$ (meaning $\exists t : \forall x, f(x) = f(x \oplus t)$), we can determine which case is true in quantum polynomial time. Additionally, in the $2:1$ case, we can find t.*



Proof We use the above quantum circuit to make this determination. Each bundle of wires is n wide, and we input $|00...0\rangle$ to each. Q_f is as mentioned above. In the $1:1$ case, the upper output y will be uniform in $\{0,1\}^n$, but in the $2:1$ case, y will be uniform among $\{y | y \cdot t \equiv 0 \bmod 2\}$. We'll run this circuit 2n times.

Start with input

$$|00...0\rangle \otimes |00...0\rangle$$

Run through first Hadomard gate to obtain:

$$\sum_{\bar{x}\in\{0,1\}^n} 2^{-n/2}|\bar{x}\rangle \otimes |00...0\rangle$$

Run through Q_f to obtain:

$$\sum_{\bar{x}\in\{0,1\}^n} 2^{-n/2}|\bar{x}\rangle \otimes |f(\bar{x})\rangle$$

Run through second Hadomard gate to obtain our final output:

$$\sum_{\bar{y}\in\{0,1\}^n} \sum_{\bar{x}\in\{0,1\}^n} 2^{-n}(-1)^{\bar{x}\cdot\bar{y}}|\bar{y}\rangle \otimes |f(\bar{x})\rangle$$

In the $1:1$ case, each state of the form $|\bar{y}\rangle \otimes |f(\bar{x})\rangle$ will appear once, with coefficient $\pm 2^{-n}$. So, each output on 2n bits has probability 2^{-2n} of appearing, meaning that we have a uniformly random distribution of outputs.

For the $2:1$ case, examine sum terms $2^{-n}(-1)^{\bar{x}\cdot\bar{y}}|\bar{y}\rangle \otimes |f(\bar{x})\rangle$ and $2^{-n}(-1)^{(\bar{x}\oplus t)\cdot\bar{y}}|\bar{y}\rangle \otimes |f(\bar{x}\oplus t)\rangle$. $|f(\bar{x})\rangle$ and $|f(\bar{x}\oplus t)\rangle$ are equal, so the terms come in pairs. If $t\cdot\bar{y}\equiv 0 \bmod 2$, then $(-1)^{\bar{x}\cdot\bar{y}}$ and $(-1)^{(\bar{x}\oplus t)\cdot\bar{y}}$ will give the same sign, and the resulting coefficient for this $|\bar{y}\rangle \otimes |f(\bar{x})\rangle$ will be $\pm 2\cdot\frac{1}{2^n}$, or $\pm\frac{1}{2^{n-1}}$. If, instead, $t\cdot\bar{y}\equiv 1 \bmod 2$, the two terms will cancel out, and this $|\bar{y}\rangle \otimes |f(\bar{x})\rangle$ will not be present in the final state. Therefore, the probability of each output is $\frac{1}{2^{2n-2}}$, and there are 2^{2n-2} possible states. So, we again have a uniformly random distribution of outputs. Also, in each possible output state, $t\cdot\bar{y}\equiv 0 \bmod 2$.

To determine which case we have, examine the 2n output $\bar{y}$'s. In the $1:1$ case, odds are they span $\{0,1\}^n$, since they are uniformly random. In the $2:1$ case, $t\cdot\bar{y}\equiv 0 \bmod 2$ will hold for all $\bar{y}$'s, and odds are t is the only vector that satisfies this, again since the $\bar{y}$'s are uniformly random. We can test for which of the above is true, and in the $2:1$ case find t, through simple linear algebra.

■