An Introduction to Quantum Algorithms

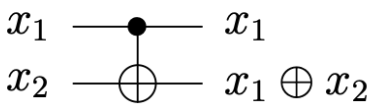
(Note: This document closely follows [1])

Boolean Circuits

A Boolean circuit consists of gates such as AND, OR, and NOT. A set of gates is said to be universal if any Boolean function can be realized with these gates. AND, OR, and NOT gates form a universal set. NAND alone forms a universal set.

A Boolean gate is said to be reversible if it has the same number of
inputs as outputs, and its mapping from input strings to output strings is a bijection. It is desirable to have reversible gates (and circuits) since they correspond to closed physical systems.

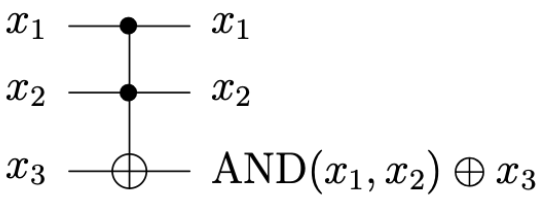
An example of a reversible gate is CNOT (controlled-NOT) which is defined as follows:



Bra-ket notation: A bit will be denoted as $|0\rangle$ or $|1\rangle$ from hereon. A string will also denoted similarly, e.g., $|0100\rangle$. CNOT has the following truth table:

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

Both NOT and CNOT are their own inverses. A CCNOT gate is defined as follows:

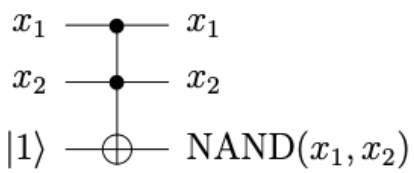


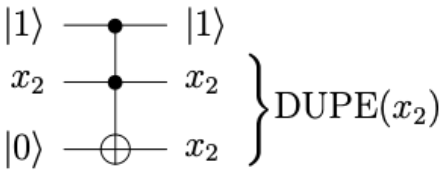
The truth table for CCNOT is:

Input	Output
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|101\rangle$

$\|110\rangle$	$\|111\rangle$
$\|111\rangle$	$\|110\rangle$

CCNOT can be used to simulate NAND and DUPE gates as shown below. A DUPE gate is used to make copies of a bit.



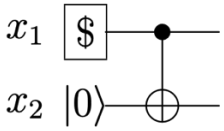


In the above simulations we have used constants $|0\rangle$ and $|1\rangle$. They are referred to as ancillas. In the NAND simulation, our only goal is to get NAND(x_1, x_2). However, we are also getting x_1 and x_2 as additional (unwanted outputs). These are referred to as garbage. It is easy to see that we can generate $|0\rangle$ from $|1\rangle$ using a CCNOT gate. As a result, we can verify that CCNOT together with ancilla inputs (all set to $|1\rangle$) is universal.

In a reversible circuit that realizes a function $f: \{0,1\}^n \rightarrow \{0,1\}^m$, the following holds: n + the number of ancillas = m + the number of garbage outputs.

Randomized Circuits

A randomized circuit can be thought of as a Boolean circuit in which we can use a coin flip gate (in addition to the other standard gates). This gate (called COIN or \$) has no input and its output is a single bit that could be $|0\rangle$ with probability ½ or $|1\rangle$ with probability ½. We use the notation ½$|0\rangle$ + ½$|1\rangle$ to characterize the output of COIN. An example for a randomized circuit is:



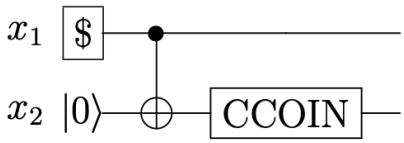
In this circuit, x_1 is initialized to \$ and x_2 is initialized to $|0\rangle$. The output of this circuit is $|00\rangle$ with probability ½ and the output is $|11\rangle$ with probability ½. This output can also be denoted as ½$|00\rangle$ + ½$|11\rangle$.

Another gate called CCOIN is defined as follows:

CCOIN:

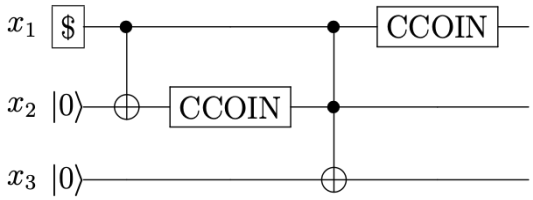
input	output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\begin{cases} \|0\rangle & \text{with prob. } \frac{1}{2} \\ \|1\rangle & \text{with prob. } \frac{1}{2} \end{cases}$

Consider the following circuit:



What is the output of this circuit? Before the CCOIN gate, the output is ½|00⟩ + ½|11⟩. What is the output after CCOIN? We see that it is: ½|00⟩ + ½(½|10⟩ + ½|11⟩) = ½|00⟩ + ¼|10⟩ + ¼|11⟩. Assume that there is another register x_3 in the system that is initialized to |0⟩. Then the state of the entire system is ½|000⟩ + ¼|100⟩ + ¼|110⟩.

Now add the gate CCNOT(x_1, x_2, x_3) at the end of the current circuit. The output after this gate will be ½|000⟩ + ¼|100⟩ + ¼|111⟩. Now add the gate CCOIN(x_1):



The output is: ½|000⟩ + ¼(½|000⟩ + ½|100⟩) + ¼(½|011⟩ + ½|111⟩)
=(5/8)|000⟩ + (1/8)|100⟩ + (1/8)|011⟩ + (1/8)|111⟩.

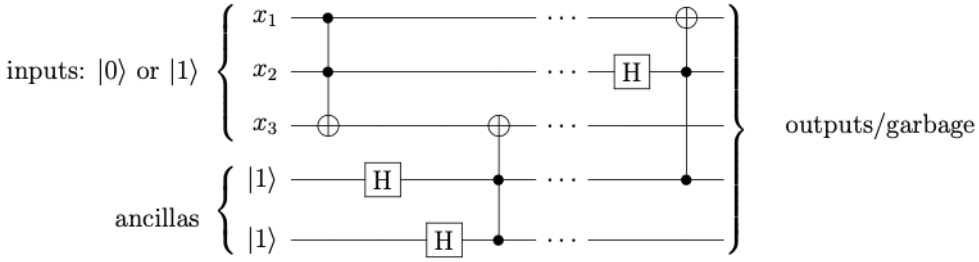
In general, the state of n r-bit (random bit) registers, at any time, can be expressed as $\sum_{x\in\{0,1\}^n} p_x|x\rangle$, where the probabilities p_x are non-negative and sum to 1.

Note: When we observe (or measure) the output of a randomized circuit, each register will have a specific value.

Quantum Circuits

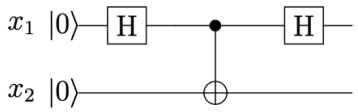
A quantum circuit could utilize Hadamard gates in addition to the gates allowed for a random circuit. Also, instead of bits we will deal with quantum bits or qubits. A Hadamard gate takes as input one qubit and it outputs a qubit. We'll denote qubits with kets as well. If the input is |0⟩, the output will be $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Note that the coefficient of |0⟩ is $\frac{1}{\sqrt{2}}$ and the coefficient of |1⟩ is also the same. In a quantum circuit these coefficients are called amplitudes and can be negative. The interpretation of this output is that, the output will be |0⟩ with a probability of $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$. The output will be |1⟩ with the same probability. If the input to a Hadamard gate is |1⟩, the output will be $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. In general, the state of a qubit at any time can be represented as $\alpha_0|0\rangle + \alpha_1|1\rangle$. Here the amplitudes α_0 and $\alpha_1$could be negative and satisfy: $\alpha_0^2 + \alpha_1^2 = 1$. α_0^2 is the probability

that the state of the qubit is $|0\rangle$ and α_1^2 is the probability that the state of the qubit is $|1\rangle$. Here is an example of a quantum circuit with 5 qubit registers:



Similar to a random circuit, we can determine the joint state of the 5 qubits at any time. In general, the state of a register might be a function of the states of the other registers at any time. I.e., the registers might be correlated. These correlations are referred to as entanglement in the case of qubits. Like in a randomized circuit, we can represent the joint state of the 5 qubits at any time as $\alpha_0|00000\rangle + \alpha_1|00001\rangle + \alpha_2|00010\rangle + \cdots + \alpha_{31}|11111\rangle$. Here $\alpha_0, \alpha_1, \cdots, \alpha_{31}$ are the amplitudes for the states and they satisfy: $\alpha_0^2 + \alpha_1^2 + \cdots + \alpha_{31}^2 = 1$. Also, α_0^2 is the probability that the joint state is $|00000\rangle$, α_1^2 is the probability that the joint state is $|00001\rangle$, etc.

Consider the following circuit:



To begin with the state of the system is $|00\rangle$, After the first Hadamard gate, the state is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$. After the CNOT gate the state becomes $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. After the second Hadamard gate, the state is: $\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$. If we measure the state after the second Hadamard gate, it will be one of the following with an equal probability of ¼: $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$.

The difference between a randomized circuit and a quantum circuit is this: In a randomized circuit, the bits will have specific values and we may not know what they are a priori. In a quantum circuit, we assume that nature keeps track of all of the 2^n amplitudes (when we have an n-bit system).

A complex number is of the form $a + ib$, where a and b are real numbers and $i^2 = -1$. A complex number corresponds to a point in the complex plane. In polar coordinates this number can be thought of as having a magnitude of $\sqrt{a^2 + b^2}$ and an angle $\theta = \tan^{-1}\left(\frac{b}{a}\right)$. If we have two complex numbers with magnitudes z_1 and z_2 and angles θ_1 and θ_2, then their product has a magnitude of $z_1 z_2$ and an angle of $\theta_1 + \theta_2$.

The complex conjugate of $z = a + ib$ is $a - ib$ and is denoted as $\overline{z}$.

Two most common states of a qubit are $|0\rangle$ and $|1\rangle$. A crucial difference between a bit and a qubit is that a qubit can be in linear combinations of states. A quantum state can be expressed as $|\psi\rangle =$

$\alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. Note that α and β are complex numbers. $|\psi\rangle$ can be thought of as a vector in the complex plane spanned by the basis states $|0\rangle$ and $|1\rangle$.

Two other popular states are $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.
A quantum system in general has multiple qubits. The state of a system with 2 qubits can be expressed as $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, with $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. A special case is when all the four amplitudes are equal (to ½). In this case we have a uniformly mixed state. As another example, $\alpha_{00} = \frac{1}{\sqrt{2}}, \alpha_{01} = 0, \alpha_{10} = 0, \alpha_{11} = \frac{1}{\sqrt{2}}$. In this case, the qubits are correlated.

We can also think about a qudit system where there are *d* basis states. The state of a qudit can be expressed as $|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_d|d\rangle$, where $|\alpha_1|^2 + |\alpha_2|^2 + \cdots + |\alpha_d|^2 = 1$.

Vector Representation of States

The state of a qubit can be represented as a unit vector in the complex plane. The basis states $|0\rangle$ and $|1\rangle$ correspond to column vectors: $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. The general state of the system can be expressed as: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$.
We refer to a quantum state $|\psi\rangle$ as a ket. Its vector dual is denoted as $\langle\psi|$ and we call this a bra. $\langle\psi|$ is nothing but the conjugate transpose of $|\psi\rangle$. If $|\psi\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$, then $\langle\psi| = [\bar{\alpha} \quad \bar{\beta}]$.

If $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$ are two quantum states, we can define the inner product of these two states as $\langle\psi_1| \cdot |\psi_2\rangle = \overline{\alpha_0}\,\beta_0 + \overline{\alpha_1}\,\beta_1$. Note that $\langle\psi_1| \cdot |\psi_1\rangle = \overline{\alpha_0}\alpha_0 + \overline{\alpha_1}\,\alpha_1 = |\alpha_0|^2 + |\alpha_1|^2 = 1$.

The outer product of two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$ is defined as $|\psi_1\rangle \cdot \langle\psi_2|$ and is often written as $|\psi_1\rangle\langle\psi_2|$. By this definition, $|\psi_1\rangle\langle\psi_2| = \begin{bmatrix}\alpha_0\\\alpha_1\end{bmatrix} . [\overline{\beta_0} \quad \overline{\beta_1}] = \begin{bmatrix}\alpha_0\overline{\beta_0} & \alpha_0\overline{\beta_1}\\\alpha_1\overline{\beta_0} & \alpha_1\overline{\beta_1}\end{bmatrix}$.

$\langle 0|1\rangle = [1 \quad 0]\begin{bmatrix}0\\1\end{bmatrix} = 0$. Likewise, we can verify that $\langle +|-\rangle = 0$. As a result, $|0\rangle$ and $|1\rangle$ form an orthonormal basis for the complex plane and so do $|+\rangle$ and $|-\rangle$. Any quantum state can be expressed using either basis.

Multiple qubit systems

If $|x\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|y\rangle = \beta_0|0\rangle + \beta_1|1\rangle$ are two qubits the joint state of these qubits can be represented using tensor product as follows: $|x\rangle \otimes |y\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \alpha_0\beta_0|0\rangle \otimes |0\rangle + \alpha_0\beta_1|0\rangle \otimes |1\rangle + \alpha_1\beta_0|1\rangle \otimes |0\rangle + \alpha_1\beta_1|1\rangle \otimes |1\rangle$. If we think of $|0\rangle \otimes |0\rangle$ as $|00\rangle$, $|0\rangle \otimes |1\rangle$ as $|01\rangle$, etc., $|x\rangle \otimes |y\rangle$ seems like a linear combination of the basic states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Also, $|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 + |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = (|\alpha_0|^2 + |\alpha_1|^2)(|\beta_0|^2 + |\beta_1|^2) = 1$.

Thus, $\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$ is a valid description of the joint state of the two qubits.

In matrix form, $|x\rangle \otimes |y\rangle = \begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} \otimes \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix} = \begin{bmatrix}\alpha_0\begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\\ \alpha_1\begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{bmatrix}$.

Not all states in a multi qubit system can be written in the above form (namely product states form). For example, if the state of a 2 qubit system is $\frac{1}{\sqrt{2}}|00\rangle\frac{1}{\sqrt{2}}|11\rangle$, we will not be able to express this as a tensor product of two quantum states. The states that cannot be expressed as the tensor product of two other states are known as entangled states.

A quantum circuit is used to change the states of a quantum system. I.e., a quantum circuit can be thought of as a mapping of states to states. For any gate if the input is a quantum state, the output is also a quantum state. A state $|x\rangle$ gets mapped to $U|x\rangle$ by the gate, where U is the mapping. U has to map a quantum state into another and also it has to be linear. For any two states $|x_1\rangle$ and $|x_2\rangle, U(|x_1\rangle + |x_2\rangle) = U|x_1\rangle + U|x_2\rangle$. The first condition implies that for any state $|x\rangle$, $\langle x|x\rangle = 1\ and\ \overline{U|x\rangle}\,U|x\rangle = 1$. The second equality implies that $\overline{|x\rangle}\,\overline{U}U|x\rangle = 1, i.e., \langle x|\overline{U}U|x\rangle = 1$. This implies that $\overline{U}U = I$, i.e., U is unitary.

Unitary operations are invertible (and hence reversible). The inverse of a unitary operation is its conjugate transpose. Also, unitary operations are equivalent to basis changes.

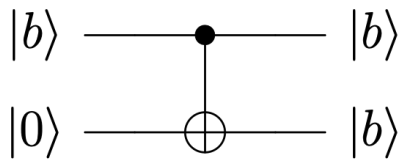
Let $\{|u_1\rangle, |u_2\rangle, \cdots, |u_d\rangle\}$ be any orthonormal basis for the d-dimensional complex space. Let $|v_1\rangle = U|u_1\rangle, |v_2\rangle = U|u_2\rangle, \cdots, |v_d\rangle = U|u_d\rangle$, then $\{|v_1\rangle, |v_2\rangle, \cdots, |v_d\rangle\}$ is also an orthonormal basis. Specifically, $\langle u_i|u_j\rangle = \langle v_i|v_j\rangle = \begin{cases}1 : i = j\\ 0 : i \neq j\end{cases}$.

Any unitary operation U can be expressed as $U = \sum_{i=1}^{d}|v_i\rangle\langle u_i|$ where $\{v_i\}\ and\ \{u_i\}$ are orthonormal bases of the d-dimensional space. Clearly, $U|u_j\rangle = \sum_{i=1}^{d}|v_i\rangle\langle u_i||u_j\rangle = |v_j\rangle$.

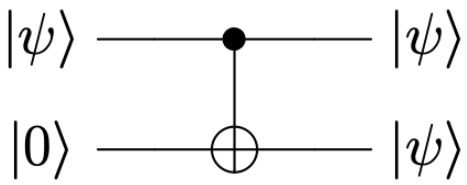
On Measurements of multi qubit systems: Consider a 2 qubit system whose current state is $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. If measurements are made, $|00\rangle$ will be observed with a probability of $|\alpha_{00}|^2$, $|01\rangle$ will be observed with a probability of $|\alpha_{01}|^2$, etc. We could also make partial measurements. For instance, assume that Alice and Bob have a qubit each. Assume that Alice measures her qubit. Probability that Alice observes $|0\rangle$ is $|\alpha_{00}|^2 + |\alpha_{01}|^2$. Probability that she observes $|1\rangle$ is $|\alpha_{10}|^2 + |\alpha_{11}|^2$.

Copying Information

In classical computing, copying information is easy. See for example:



On the other hand, let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be a qubit. Is it possible to copy $|\psi\rangle$? Say we attempt to use a CNOT gate as before:

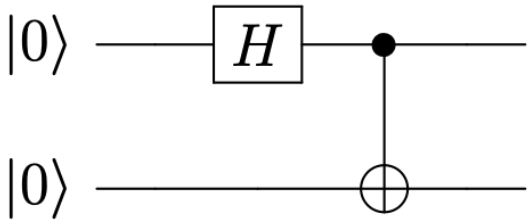


The joint state of the qubits before the CNOT gate is $\alpha|00\rangle + \beta|10\rangle$. After the CNOT gate, the joint state is $\alpha|00\rangle + \beta|11\rangle$. Our desired state is $|\psi\rangle \otimes |\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$. As a result, the CNOT gate is not able to copy the qubit.
In reality, there does not exist a quantum circuit that can copy a qubit even if ancillas in the input and garbage in the output are allowed. The following theorem is due to Wootters and Zurek (1982):

Theorem: (No cloning theorem): For all $n \in \mathbb{N}$, there exists no quantum circuit that takes as input $|\psi\rangle \otimes |0^{n-1}\rangle$ and outputs $|\psi\rangle \otimes |\psi\rangle \otimes f(|\psi\rangle)$, where the garbage $f(|\psi\rangle)$ is a possibly entangled state of *n*-2 qubits.

An Entangled Pair

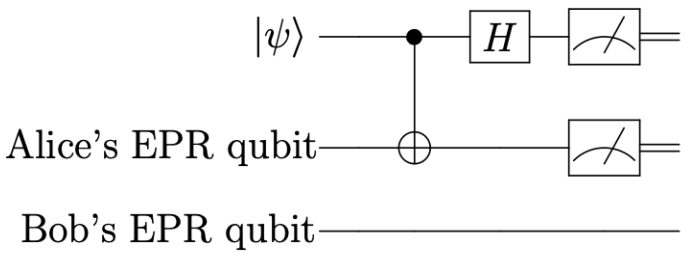
Consider the following circuit:



The joint state of the two qubits after the CNOT gate is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. This pair is said to be entangled and known as an EPR pair (identified by Einstein, Podolsky, and Rosen 1935).

Quantum Teleportation

If Alice has a qubit $|0\rangle$ and Bob has a qubit $|0\rangle$, then EPR is one way of entangling this pair of qubits. Even if Alice and Bob are physically separated, their qubits will be entangled. Assume that Alice has another qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. If she wants to give this qubit to Alice, she can do so from wherever she may be. One possibility is for Alice to determine the values of α_0 and α_1 and give them to Bob. There are two issues: 1) she cannot determine α_0 and α_1 without measurement. In this case, she might lose $|\psi\rangle$; and 2) she might need infinitely many bits of precision to specify α_0 and α_1. Instead, she can use the following approach:



At the beginning, the three qubits are in the joint state of $\frac{\alpha_0}{\sqrt{2}}|000\rangle + \frac{\alpha_0}{\sqrt{2}}|011\rangle + \frac{\alpha_1}{\sqrt{2}}|100\rangle + \frac{\alpha_1}{\sqrt{2}}|111\rangle$. After the CNOT gate, the joint state is $\frac{\alpha_0}{\sqrt{2}}|000\rangle + \frac{\alpha_0}{\sqrt{2}}|011\rangle + \frac{\alpha_1}{\sqrt{2}}|110\rangle + \frac{\alpha_1}{\sqrt{2}}|101\rangle$. After the Hadamard gate, the joint state is: $\frac{\alpha_0}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|100\rangle\right) + \frac{\alpha_0}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|011\rangle + \frac{1}{\sqrt{2}}|111\rangle\right) + \frac{\alpha_1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|010\rangle - \frac{1}{\sqrt{2}}|110\rangle\right) + \frac{\alpha_1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|001\rangle - \frac{1}{\sqrt{2}}|101\rangle\right) = \frac{\alpha_0}{2}|000\rangle + \frac{\alpha_1}{2}|001\rangle + \frac{\alpha_1}{2}|010\rangle + \frac{\alpha_0}{2}|011\rangle + \frac{\alpha_0}{2}|100\rangle - \frac{\alpha_1}{2}|101\rangle - \frac{\alpha_1}{2}|110\rangle + \frac{\alpha_0}{2}|111\rangle$.

Now Alice measures her two bits. The following table shows the different possibilities for the measurements and the corresponding collapsed joint state.

Alice's measurement	Prob. of meas.	Collapsed state
$\|00\rangle$	$\frac{\|\alpha_0\|^2}{4} + \frac{\|\alpha_1\|^2}{4} = \frac{1}{4}$	$\|00\rangle \otimes (\alpha_0\|0\rangle + \alpha_1\|1\rangle)$
$\|01\rangle$	$\frac{\|\alpha_1\|^2}{4} + \frac{\|\alpha_0\|^2}{4} = \frac{1}{4}$	$\|01\rangle \otimes (\alpha_1\|0\rangle + \alpha_0\|1\rangle)$
$\|10\rangle$	$\frac{\|\alpha_0\|^2}{4} + \frac{\|-\alpha_1\|^2}{4} = \frac{1}{4}$	$\|10\rangle \otimes (\alpha_0\|0\rangle - \alpha_1\|1\rangle)$
$\|11\rangle$	$\frac{\|-\alpha_1\|^2}{4} + \frac{\|\alpha_0\|^2}{4} = \frac{1}{4}$	$\|11\rangle \otimes (-\alpha_1\|0\rangle + \alpha_0\|1\rangle)$

To give $|\psi\rangle$ to Bob, Alice calls him and lets him know her partial measurements.
If Alice reports $|00\rangle$, then Bob infers that his qubit is in state $\begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} = |\psi\rangle$.
If Alice reports $|01\rangle$, then Bob applies a NOT gate $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ to his qubit $\begin{bmatrix}\alpha_1\\ \alpha_0\end{bmatrix}$ to get $|\psi\rangle$.
If Alice reports $|10\rangle$, then Bob applies the gate $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ to his qubit $\begin{bmatrix}\alpha_0\\ -\alpha_1\end{bmatrix}$ to get $|\psi\rangle$.
If Alice reports $|11\rangle$, then Bob applies the gate $\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$ to his qubit $\begin{bmatrix}-\alpha_1\\ \alpha_0\end{bmatrix}$ to get $|\psi\rangle$.

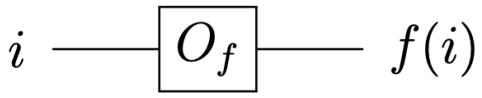
Grover's Algorithm

Problem: Given a sequence $X = x_1, x_2, \cdots, x_N$ and a function $f: X \to \{0,1\}$, the problem is to find an i such that $f(x_i) = 1$.

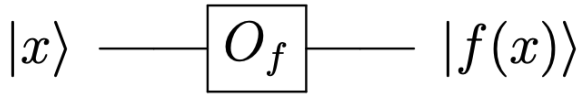
Fact: In traditional computing, this problem needs $\Omega(N)$ time to solve, in the worst case (assuming that X may not be in any sorted order).

Lemma (Grover 1996): This problem can be solved in $O(\sqrt{N})$ time using a quantum circuit. The output of this circuit will be correct with a constant probability.

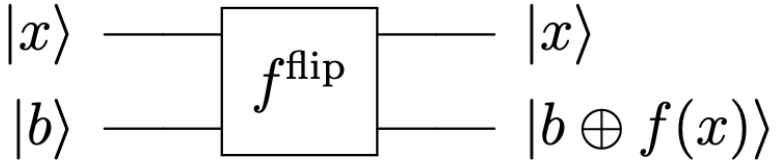
We assume that there exists a gate (or oracle) to compute f:



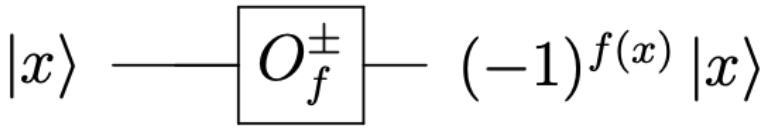
Assume that there exists a unique x^* such that $f(x^*) = 1$. (This can be relaxed and extended). Assume without loss of generality that N is an integral power of 2. Also assume that the data is labelled as n-bit integers where $2^n = N$ and $f: \{0,1\}^n \to \{0,1\}$. In this case, our oracle gate takes the following form:



This gate is not unitary and reversible. We can make it unitary as follows:

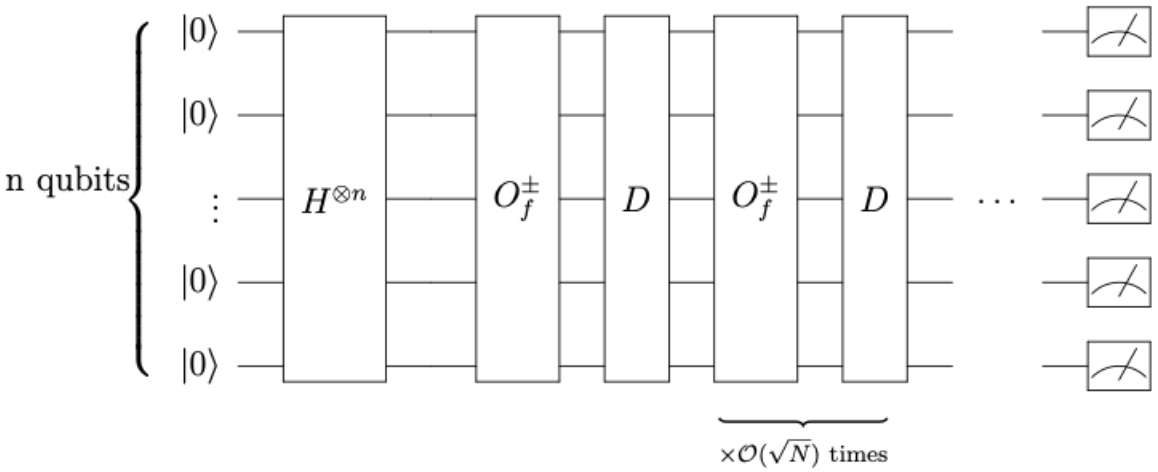


We could let $|b\rangle$ be $|0\rangle$. Another solution is to flip the input if and only if $f(x)$ is 1. On input $|x\rangle$, $O_f^{\pm}$ will output: $(-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle \text{ if } f(x) = 0 \\ -|x\rangle \text{ if } f(x) = 1 \end{cases}$.



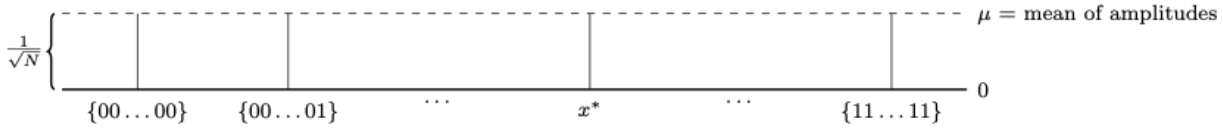
Fact: We can construct $O_f^{\pm}$ from f^{flip}. The idea is to use $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ as the ancilla $|b\rangle$.

Grover's Quantum circuit takes the following form:

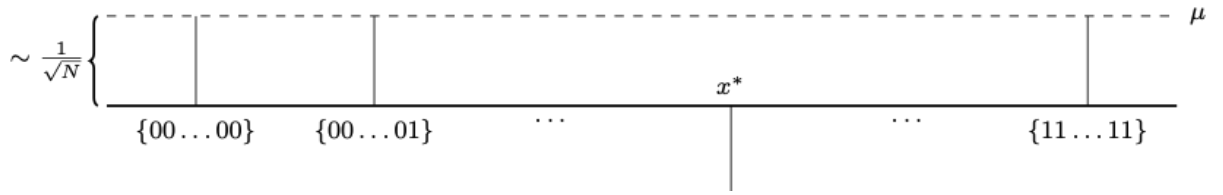


If $f(x^* = 1)$, then, we would like to ensure that the final amplitude of $|x^*\rangle$ is at least some constant (e.g., 0.1), so that when we measure at the end, there is at least a constant probability of measuring $|x^*\rangle$. We ensure this using superposition and amplitude modulation.

We initialize all the n qubits to $|0\rangle$. Here, $2^n = N$. Using a Hadamard gate on each wire, we initialize the state of the system to $\sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{N}} |x\rangle$. Now, every $|x\rangle$ has the same amplitude $\left(\text{of } \frac{1}{\sqrt{N}}\right)$. A plot of the amplitudes will look like:

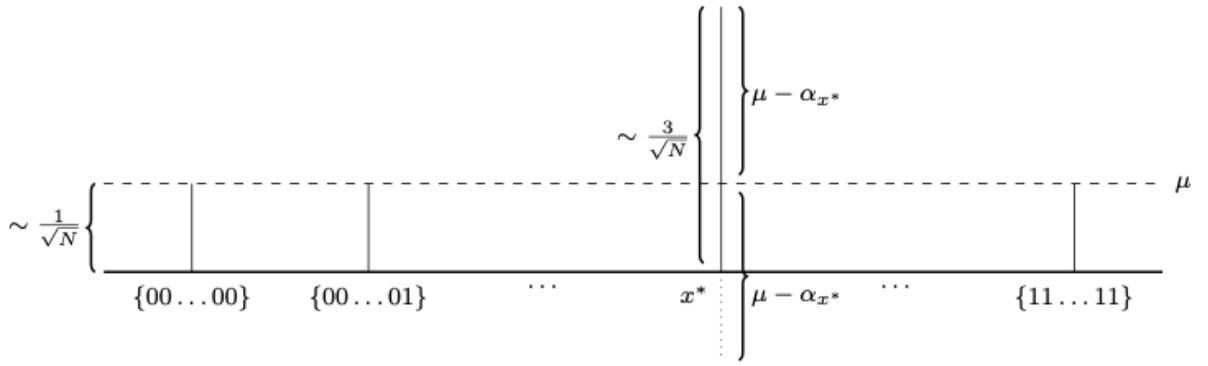


Now we apply the oracle gate. It flips the amplitude of x^* and leaves the others unchanged. We end up with the following state: $-\frac{1}{\sqrt{N}} |x^*\rangle + \sum_{\substack{x\in\{0,1\}^n \\ x\neq x^*}} \frac{1}{\sqrt{N}} |x\rangle$. The amplitudes diagram changes to:



We want to increase the amplitude of $|x^*\rangle$ absolutely. To do this, a diffusion operator is introduced. Let $\mu = \frac{1}{N}\sum_x \alpha_x$. μ is the average amplitude of $x \in \{0,1\}^n$. The diffusion gate has the following mapping: $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \rightarrow \sum_{x\in\{0,1\}^n} (2\mu - \alpha_x)|x\rangle$. This is a linear and unitary operator and hence a valid quantum gate.

When we apply this operator, this is what we get: $\sum_{x\in\{0,1\}^n} \alpha_x = \frac{2^n-1}{\sqrt{N}} - \frac{1}{\sqrt{N}} = \frac{2^n-2}{\sqrt{N}} \approx \frac{1}{\sqrt{N}}$. The amplitude of x^* becomes nearly $\frac{3}{\sqrt{N}}$. The amplitude plot becomes:



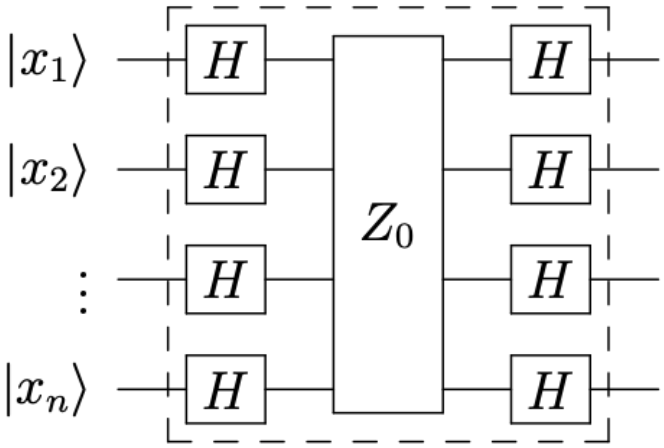
After applying the oracle and diffusion gates one more time, the amplitude of $|x^*\rangle$ goes to nearly $\frac{5}{\sqrt{N}}$ and the others stay at nearly $\frac{1}{\sqrt{N}}$. We can continue to apply these gates as many times as needed. We should stop before the amplitude of $|x^*\rangle$ becomes too large to force the mean amplitude to become negative. We can show that the amplitude of $|x^*\rangle$ will become $>$ 0.1 within $O(\sqrt{N})$ applications of the oracle and diffusion gates. This means that after $O(\sqrt{N})$

iterations, if we measure, the probability of finding x^* is >0.01. Call this one pass through the circuit. If we repeat this pass a constant number of times, we can boost the probability of seeing x^* to any constant of interest.

Diffusion Gate

Grover's diffusion gate is based on the following gate: $Z_0 = 2|0^n\rangle\langle 0^n| - I$. If the input to this gate is 0^n, the output will be $Z_0|0^n\rangle = 2|0^n\rangle\langle 0^n|0^n\rangle - |0^n\rangle = |0^n\rangle$. If the input is any $|x\rangle$ other than $|0^n\rangle$, the output will be $Z_0|x\rangle = 2|0^n\rangle\langle 0^n|x\rangle - |x\rangle = -|x\rangle$. We can characterize Z_0 as follows: $Z_0|x\rangle = \begin{cases} |x\rangle \text{ if } |x\rangle = |0^n\rangle \\ -|x\rangle \text{ if } |x\rangle \neq |0^n\rangle \end{cases}$.

The diffusion gate D is nothing but: $H^{\otimes n}Z_0H^{\otimes n} = H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n} = 2\left((H|0\rangle)^{\otimes n}\overline{(H|0\rangle)^{\otimes n}}\right) - H^{\otimes n}H^{\otimes n} = 2|+^n\rangle\langle +^n| - I$. The corresponding circuit looks like:



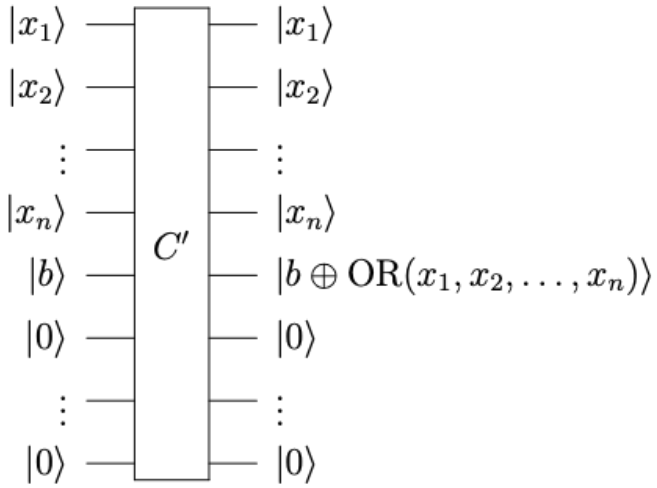
Consider an arbitrary input $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$ to D. We have: $D|\psi\rangle = (2|+^n\rangle\langle +^n| - I)|\psi\rangle = 2|+^n\rangle\langle +^n|\psi\rangle - |\psi\rangle$.

Note that $\langle +^n| = \left(\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right)^{\otimes n} = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{N}}\langle x|$. Thus, $\langle +^n|\psi\rangle = \sum_{x\in\{0,1\}^n} \frac{\alpha_x}{\sqrt{N}}\langle x|x\rangle = \sum_{x\in\{0,1\}^n} \frac{\alpha_x}{\sqrt{N}} = \mu\sqrt{N}$.

$$D|\psi\rangle = 2|+^n\rangle\langle +^n|\psi\rangle - |\psi\rangle = 2|+^n\rangle\mu\sqrt{N} - |\psi\rangle = 2\left(\sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{N}}|x\rangle\right)\mu\sqrt{N} - |\psi\rangle$$

$$= 2\left(\sum_{x\in\{0,1\}^n} \mu|x\rangle\right) - |\psi\rangle = \sum_{x\in\{0,1\}^n} (2\mu - \alpha_x)|x\rangle.$$

Finally, here is one way of constructing Z_0:



If we send $|x\rangle \otimes |-\rangle \otimes |0^m\rangle$ into C' the output will be $(-1)^{OR(x_1,x_2,\cdots,x_n)}(|x\rangle \otimes |-\rangle \otimes |0^m\rangle)$.

In summary, the gate complexity of the Grover circuit is $O(\log N)$. The run time is $O(\sqrt{N})$.

Reference

1. R. O'Donnell and J. Wright, Quantum Computation and Information, Lecture Notes, 2015, CMU, https://www.cs.cmu.edu/~odonnell/quantum15/.