Quantum computers:

The idea of quantum computing is to replace classical bits, which can be either 0 or 1, by quantum bits (qubits) that can be in superpositions of the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{with} \quad |\alpha|^2 + |\beta|^2 = 1$$

The qubits are manipulated using a quantum circuit, which are built from different quantum gates. For example, the Hadamard gate is a single-qubit gate with the matrix representation $\underline{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and it acts as follows:

$$\alpha|0\rangle + \beta|1\rangle \;\text{---}\boxed{H}\text{---}\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Another important gate is the controlled-NOT (or CNOT) gate, which is a two-qubit gate that flips the second qubit <u>conditioned</u> on the first qubit being 1. It can be expressed as $\text{CNOT}\,|\alpha\rangle|\beta\rangle \to |\alpha\rangle|\alpha \oplus \beta\rangle$, where $\oplus$ denotes addition modulo 2.

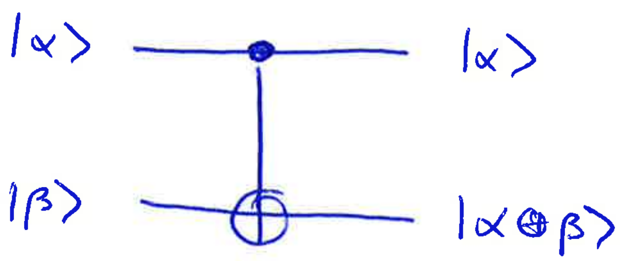
The "truth table" of the CNOT gate is

$$|0\rangle|0\rangle \to |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \to |0\rangle|0\oplus 1\rangle = |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \to |1\rangle|1\oplus 0\rangle = |1\rangle|1\rangle$$
$$|1\rangle|1\rangle \to |1\rangle|1\oplus 1\rangle = |1\rangle|0\rangle$$

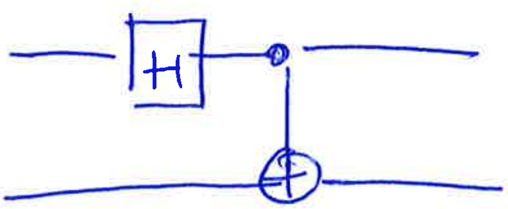
The matrix representation of the CNOT gate is

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The circuit representation of the CNOT gate is



Together with the Hadamard gate, we can generate entanglement with the circuit



If we input $|0\rangle|0\rangle$, we get

$$|0\rangle|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \xrightarrow{CNOT} \underbrace{\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)}_{\text{entangled state!}}$$

Deutsch's algorithm:

Let's consider Deutsch's algorithm from 1985, which is (possibly) the first quantum algorithm that could outperform a (simple) classical algorithm. The algorithm seeks to determine if a given boolean function $f: \{0,1\} \to \{0,1\}$ is constant or not, in other words, is $f(0) = f(1)$ or is $f(0) \neq f(1)$?

Classically, we need to call the function twice, that is, we need to evaluate $f(0)$ and $f(1)$, and then compare the results.

Quantum-mechanically, we proceed as follows. We start by preparing two qubits in the state

$$|\psi_0\rangle = |0\rangle|1\rangle$$

We then apply Hadamard gates to each qubit:

$$\underline{\underline{H}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \quad \underline{\underline{H}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}; \quad \underline{\underline{H}}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\underline{\underline{H}}\,\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad \underline{\underline{H}}\,\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

We then obtain

$$|\psi_1\rangle = (\hat{H}\otimes\hat{H})\,|0\rangle|1\rangle$$
$$= \frac{1}{2}\Big[|0\rangle + |1\rangle\Big]\Big[|0\rangle - |1\rangle\Big]$$
$$= \frac{1}{2}\Big[|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\Big]$$

Next, we need a quantum implementation of f which we define as

addition modulo 2

$$\hat{U}_f\,|x\rangle|y\rangle = |x\rangle|f(x)\oplus y\rangle$$

Applying $\hat{U}_f$, we then get

$$|\psi_2\rangle = \hat{U}_f\,|\psi_1\rangle$$
$$= \frac{1}{2}\Big[|0\rangle|f(0)\oplus 0\rangle - |0\rangle|f(0)\oplus 1\rangle + |1\rangle|f(1)\oplus 0\rangle - |1\rangle|f(1)\oplus 1\rangle\Big]$$

$$= \frac{1}{2}\Big[|0\rangle\big(|f(0)\rangle - |f(0)\oplus 1\rangle\big) + |1\rangle\big(|f(1)\rangle - |f(1)\oplus 1\rangle\big)\Big]$$

$$= \frac{1}{2}\Big[|0\rangle(-1)^{f(0)}\big(|0\rangle - |1\rangle\big) + |1\rangle(-1)^{f(1)}\big(|0\rangle - |1\rangle\big)\Big]$$

$$= \frac{1}{2}\Big[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big]\Big[|0\rangle - |1\rangle\Big]$$

$$= \frac{1}{\sqrt{2}}(-1)^{f(0)}\Big[|0\rangle + (-1)^{(f(0)\oplus f(1))}|1\rangle\Big)\,\frac{1}{\sqrt{2}}\Big[|0\rangle - |1\rangle\Big]$$

Now, we again apply Hadamard gates to both qubits and find

$$|\psi_3\rangle = \hat{H} \otimes \hat{H} \, |\psi_2\rangle$$

$$= (-1)^{f(0)} \, |f(0) \oplus f(1)\rangle \, |1\rangle$$

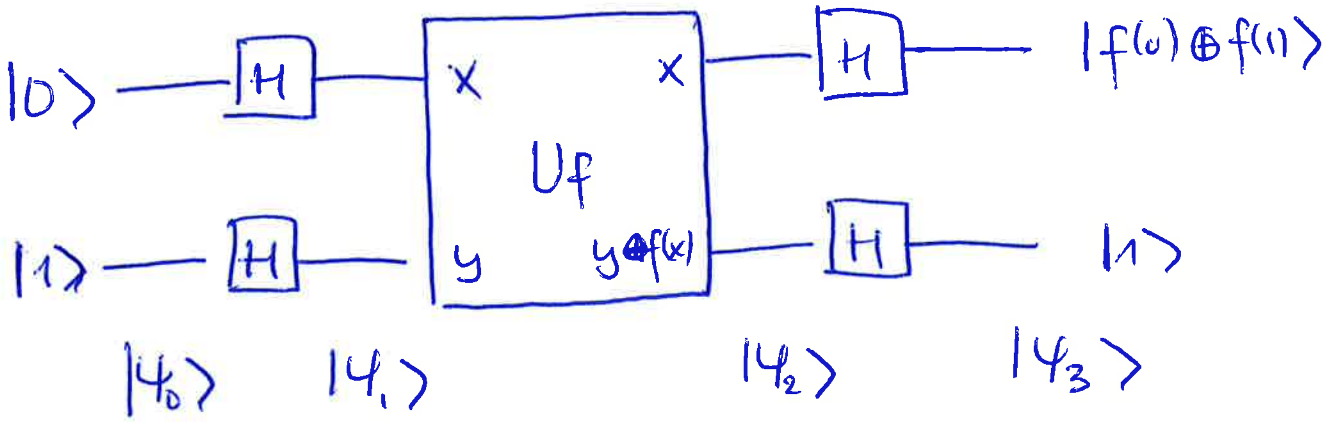
Finally, by measuring the first qubit, we obtain the value of $f(0) \oplus f(1)$.

If $f(0) = f(1) = \begin{cases} 0 \\ 1 \end{cases}$, we find $f(0) \oplus f(1) = 0$.

If $f(0) \neq f(1)$, we find $f(0) \oplus f(1) = 1$

Thus, from this measurement we can determine whether or not f is constant, although the function is only called once!

The quantum circuit that implements Deutsch's algorithm can be written as



Grover's search algorithm:

Imagine that you have received a phone number of someone and you want to figure out the person's name. You only have an old phone book at your disposal. The N entries of the phone book are sorted alphabetically according to the names, however, you are searching for a specific phone number. On average, you would have to look through N/2 entries in the book before you would find the right person. In 1997, Grover showed that you can accomplish this task by accessing the phone book only $\mathcal{O}(\sqrt{N})$ times, if you exploit the principles of quantum mechanics. To this end, assume that each name and phone number are represented by a state of the form $|number\rangle \otimes |name\rangle$.

The phone book is represented by the state

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{\text{numbers}} |\text{number}\rangle \otimes |\text{name}\rangle$$

Thus, if we measure the correct number, we can subsequently measure the name.

To simplify the notation let us forget about the name, and write the state as

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle,$$

where the sum runs over all N entries.

The particular number we are looking for is denoted by $|w\rangle$.

Grover's algorithm uses the following two operators defined as

$$\hat{U}_s = 2|s\rangle\langle s| - \hat{1}$$

$$\hat{U}_w = \hat{1} - 2|w\rangle\langle w|$$

The search algorithm consists of repeated applications of the product $\hat{U}_s \hat{W}_w$

First, we see that

$$\hat{U}_W |x\rangle = \left(1 - 2|w\rangle\langle w|\right)|x\rangle = \begin{cases} |x\rangle, & \text{if } x \neq w \\ -|x\rangle, & \text{if } x = w. \end{cases}$$

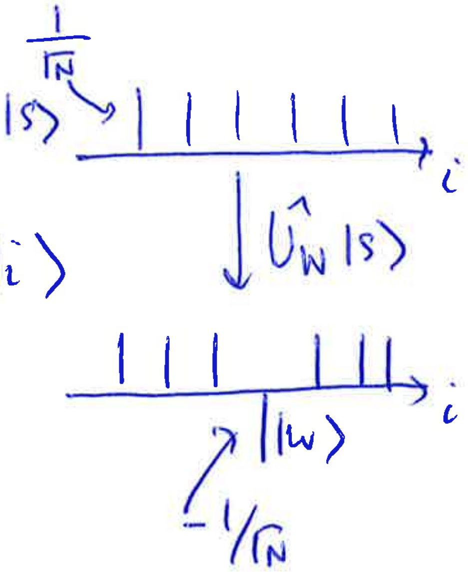
Thus, this operator flips the sign if it acts on the correct state $|w\rangle$.

By applying $\hat{U}_W$ to $|s\rangle$, we find

$$\hat{U}_W |s\rangle = \left(1 - 2|w\rangle\langle w|\right)|s\rangle$$

$$= |s\rangle - 2|w\rangle\langle w| \frac{1}{\sqrt{N}} \sum_i |i\rangle$$

$$= |s\rangle - \frac{2}{\sqrt{N}}|w\rangle$$



Next, we apply $\hat{U}_s$ and find

$$\hat{U}_s \hat{U}_W |s\rangle = \left(2|s\rangle\langle s| - 1\right)\left(|s\rangle - \frac{2}{\sqrt{N}}|w\rangle\right)$$

$$= |s\rangle - \left(2|s\rangle\langle s| - 1\right)\frac{2}{\sqrt{N}}|w\rangle$$

$$= |s\rangle - \frac{4}{N}|s\rangle + \frac{2}{\sqrt{N}}|w\rangle$$

$$= \left(1 - \frac{4}{N}\right)|s\rangle + \frac{2}{\sqrt{N}}|w\rangle$$

We can now calculate the probability to measure $|w\rangle$ after the first iteration:

$$P_1(w) = \left| \langle w | \hat{U}_s \hat{U}_w | s \rangle \right|^2$$

$$= \left| \left(1-\frac{4}{N}\right) \langle w | s \rangle + \frac{2}{\sqrt{N}} \langle w | w \rangle \right|^2$$

$$= \left(\frac{1}{\sqrt{N}} \left(1-\frac{4}{N}\right) + \frac{2}{\sqrt{N}} \right)^2$$

$$= \frac{1}{N} \left(3 - \frac{4}{N} \right)^2 = 9 \, \frac{\left(1-\frac{4}{3N}\right)^2}{N}$$

Notice how the probability has increased from $P_0(w) = \frac{1}{N}$ to $P_1(w) = \frac{9}{N}\left(1-\frac{4}{3N}\right)^2$. An interesting case is $N=4$ for which we have

$$\hat{U}_s \hat{U}_w | s \rangle = | w \rangle \quad \text{and} \quad P_1(w) = 1 \quad !$$

Thus, for a phone book with only $N=4$ entries, we can find the correct phone number in the first attempt. The algorithm even gives the correct answer for sure.

In the general case $N > 4$, we have to apply the operator $\hat{U}_s \hat{U}_w$ many times.

To this end, we recall that

$$\hat{U}_s \hat{U}_w | s \rangle = \left(1-\frac{4}{N}\right) | s \rangle + \frac{2}{\sqrt{N}} | w \rangle$$

We also find that

$$\hat{U}_s \hat{U}_W |w\rangle = \hat{U}_s \left(-|w\rangle\right)$$

$$= \left(2|s\rangle\langle s| - 1\right)\left(-|w\rangle\right)$$

$$= -\frac{2}{\sqrt{N}}|s\rangle + |w\rangle$$

Thus, in the basis $\{|w\rangle, |s\rangle\}$, we can express $\hat{U}_G \equiv \hat{U}_s \hat{U}_W$ as

$$\underline{\underline{U}}_G = \begin{pmatrix} 1 & \frac{2}{\sqrt{N}} \\ -\frac{2}{\sqrt{N}} & 1-\frac{4}{N} \end{pmatrix}$$

To evaluate $\hat{U}_G^n = (\hat{U}_s \hat{U}_W)^n$, we note that $\underline{\underline{U}}_G$ can be written as

$$\underline{\underline{U}}_G = \underline{\underline{M}}\,\underline{\underline{\Lambda}}\,\underline{\underline{M}}^{-1}, \quad \Rightarrow \quad \underline{\underline{U}}_G^n = \underline{\underline{M}}\,\underline{\underline{\Lambda}}^n\,\underline{\underline{M}}^{-1}$$

where

$$\underline{\underline{M}} = \begin{pmatrix} -i & i \\ e^{it} & e^{-it} \end{pmatrix}; \quad \underline{\underline{M}}^{-1} = \begin{pmatrix} i & e^{it} \\ -ie^{2it} & e^{it} \end{pmatrix} \frac{1}{1+e^{2it}}$$

$$\underline{\underline{\Lambda}} = \begin{pmatrix} e^{2it} & 0 \\ 0 & e^{-2it} \end{pmatrix}, \text{ and } t = \arcsin\left(1/\sqrt{N}\right)$$

$$\Rightarrow \underline{\underline{M}}\,\underline{\underline{\Lambda}}\,\underline{\underline{M}}^{-1} = \begin{pmatrix} 1 & 2\sin t \\ -2\sin t & 2\cos 2t - 1 \end{pmatrix} = \begin{pmatrix} 1 & 2/\sqrt{N} \\ -2/\sqrt{N} & 2\cos 2t - 1 \end{pmatrix} \checkmark$$

We can now evaluate the probability to measure $|w\rangle$ after n iterations:

$$P_n(w) = |\langle w|\hat{U}_G^n|s\rangle|^2$$

This is a lengthy calculation, which eventually leads to the result

$$P_n(w) = \sin^2((2n+1)t)$$

To reach a large probability, we need to choose n such that $(2n+1)t \simeq 2nt \simeq \frac{\pi}{2}$ ($t = \arcsin 1/\sqrt{N} \simeq \frac{1}{\sqrt{N}}$ for $N \gg 1$)

Thus we need $n^* = \frac{\pi}{4}\frac{1}{t} = \frac{\pi}{4}\sqrt{N}$ iterations.

Unlike the classical search, which needs $\sim N/2$ iterations, the quantum algorithm only needs $\sim\sqrt{N}$ iterations! For example, with $N = 10^6$ we have $N/2 \sim 10^6$ and $\sqrt{N} = 10^3$, which is clearly a much smaller number. However, there is a small chance that Grover's algorithm returns a wrong answer. This is not a problem, since we can easily check the result and re-run the algorithm until the correct result is obtained.

It it worth mentioning that other quantum algorithms provide exponential speed-up compared to their classical counterparts.