1 Introduction

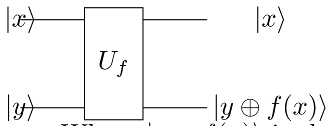
This document explain the behavior of the Deutsch Algorithm, this algorithm is a proof of the Quantum Supremacy, it is a single algorithm that can be solved in a quantum computer and can prove that the quantum computer is faster than a classical computer. By solving a classical algorithm that has a time complexity of $O(2^n)$ in a quantum computer that has a time complexity of $O(1)$.

2 Problem

The problem that has been used in the Deutsch Algorithm is the Constant/Equilibrium problem of a function. The problem is defined as follows: Take a function $f : \{0,1\}^n \to \{0,1\}$, and we want to know if the function is constant or equilibrium. A constant function is a function that returns the same value for all the inputs, and an equilibrium function is a function that returns 0 for half of the inputs and 1 for the other half.

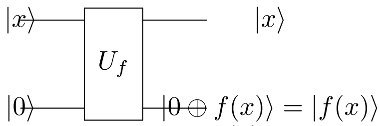
3 Oracle Circuit

This is the circuit for two qubits $|x\rangle$ and $|y\rangle$:

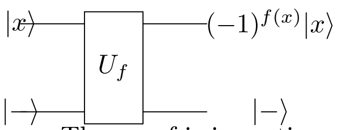


Where $|y \otimes f(x)\rangle$ is the modulo 2 sum of y and $f(x)$. This circuit is called an oracle.

If we set y to $|0\rangle$ and x to $|0\rangle$ we will have the following circuit:



Instead of the $|0\rangle$ we can use the $|-\rangle$ value that equals $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:



The proof is in section 4

4 Proof of the oracle circuit with 0 and -

$$\begin{aligned}
|\psi_0\rangle &= |x\rangle|-\rangle \\
|-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
\implies |\psi_0\rangle &= \frac{1}{\sqrt{2}}(|x\rangle|0\rangle - |x\rangle|1\rangle) \\
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(U_f(|x\rangle|0\rangle) - U_f(|x\rangle|1\rangle)) \\
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle)
\end{aligned} \tag{1}$$

f is a function that returns 0 or 1 so $1 \oplus f(x)$ is the invert of $f(x)$ that is noted $\overline{f(x)}$

$$\implies |\psi_1\rangle = \frac{1}{\sqrt{2}}(|x\rangle|f(x)\rangle - |x\rangle|\overline{f(x)}\rangle) \tag{2}$$

$$\begin{cases} \text{If } f(x) = 0: & |\psi_1\rangle = \frac{1}{\sqrt{2}}(|x\rangle|0\rangle - |x\rangle|1\rangle) = |x\rangle|-\rangle \\ \text{If } f(x) = 1: & |\psi_1\rangle = \frac{1}{\sqrt{2}}(-|x\rangle|0\rangle + |x\rangle|1\rangle) = -|x\rangle|-\rangle \end{cases}$$

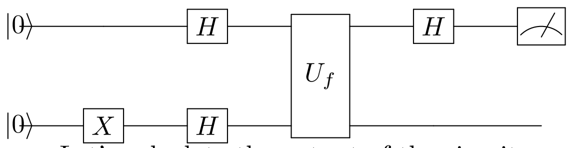
$$\implies |\psi_1\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

Because $(-1)^0 = 1$ and $(-1)^1 = -1$

(3)

5 Deutsch Circuit

The actual Deutsch circuit is the following:



Let's calculate the output of the circuit:

$$\begin{gathered} \text{Beginning state:} \\ \implies |\psi_0\rangle = |0\rangle|0\rangle \end{gathered} \tag{4}$$

Applying the first X gate of the second qubit:

$$\implies |\psi_1\rangle = |0\rangle X|0\rangle = |0\rangle|1\rangle \tag{5}$$

Applying the H gate of the two qubits:

$$\begin{aligned} &|\psi_2\rangle = H|0\rangle H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ \Longrightarrow &|\psi_2\rangle = |+\rangle|-\rangle \end{aligned} \tag{6}$$

Applying $f(x)$ to all the qubits:

$$|\psi_3\rangle = U_f(|+\rangle|-\rangle)$$
$$|\psi_3\rangle = U_f(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle)$$
$$|\psi_3\rangle = U_f(\frac{1}{\sqrt{2}}(|0\rangle|-\rangle + |1\rangle|-\rangle))$$
$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(U_f|0\rangle|-\rangle + U_f|1\rangle|-\rangle)$$
$$|\psi_3\rangle = \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle|-\rangle + (-1)^{f(1)}|1\rangle|-\rangle)$$
$$|\psi_3\rangle = \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)|-\rangle$$

We can delete $|-\rangle$ because it will not being used anymore and we will not be mesured :

$$\Longrightarrow |\psi_3\rangle = \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \tag{7}$$

If $f(x)$ is constant then $f(0) = f(1)$ and $(-1)^{f(0)} = (-1)^{f(1)}$ so the state will be:

$$\begin{cases} \text{If } f(x) = 0: & |\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \\ \text{If } f(x) = 1: & |\psi_3\rangle = \frac{1}{\sqrt{2}}(-|0\rangle - |1\rangle) = -|+\rangle \end{cases} \tag{8}$$

Else:

$$\begin{cases} \text{If } f(0) = 0 \text{ and } f(1) = 1: & |\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \\ \text{If } f(0) = 1 \text{ and } f(1) = 0: & |\psi_3\rangle = \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) = -|-\rangle \end{cases} \tag{9}$$

Finally We can say that:

$$\begin{cases} \text{If } f(x) \text{ is constant:} & |\psi_3\rangle = \pm|+\rangle \\ \text{If } f(x) \text{ is equilibrium:} & |\psi_3\rangle = \pm|-\rangle \end{cases} \tag{10}$$

Applying H to the first qubit:

$$
\begin{aligned}
H|-\rangle &= \frac{1}{\sqrt{2}}(H|0\rangle - H|1\rangle) \\
&= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) \\
H|-\rangle = |1\rangle \\
H|+\rangle &= \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) \\
&= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) \\
H|+\rangle &= |0\rangle \\
&\begin{cases} \text{If } f(x) \text{ is constant:} & |\psi_4\rangle = H|\psi_3\rangle = \pm H|-\rangle \\ \text{If } f(x) \text{ is equilibrium:} & |\psi_4\rangle = H|\psi_3\rangle = \pm H|+\rangle \end{cases} \\
\Longrightarrow &\begin{cases} \text{If } f(x) \text{ is constant:} & |\psi_4\rangle = \pm|1\rangle \\ \text{If } f(x) \text{ is equilibrium:} & |\psi_4\rangle = \pm|0\rangle \end{cases}
\end{aligned} \tag{11}
$$

6 Conclusion

We can see that if $f(x)$ is constant then the first qubit will be $|1\rangle$ and if $f(x)$ is equilibrium then the first qubit will be $|0\rangle$. So if we measure the first qubit we will know if $f(x)$ is constant or equilibrium. This is the proof of the Deutsch Algorithm and the Quantum Supremacy.