The Deutsch Algoritm

April 9, 2019
R. Kezerashvili

This algorithm is a very simple example of a quantum algorithm. The Deutsch algorithm illustrates a key ideas of quantum parallelism and quantum interference that are used in all usefull quantum algoriths.

You have a "black box" or "oracle" we can apply a circuit to this oracle to obtain value of function $f(x)$ for given input x but we cannot gain any information about inner workings of the circuit to learn about the function $f(x)$. The problem is to determine

$$f(0) \oplus f(1).$$

If we determine

$$\boxed{f(0) \oplus f(1) = 0,}$$

then we know that

$$f(0) = f(1)$$

although we do not know the value and we say function is constant.

On the other hand if we determine that $\boxed{f(0) \oplus f(1) = 1}$, then we know that $f(0) \neq f(1)$ and function $f(x)$ is balanced. Therefore determination of

$$f(0) \oplus f(1)$$

allow us to conclude if function constant or balanced.

A reversible implementation of the form

$$(x, c) \to (x, c \oplus f(x))$$

How many queries to the oracle for f must be made classically to determine $f(0) \oplus f(1)$?

Answer: clearly two.

if we compute $f(0)$ using one classical query, then the value $f(1)$ could be 0, making $f(0) \oplus f(1) = 0$, or the value $f(1) = 1$ making $f(0) \oplus f(1) = 1$. Without making the second query to the oracle to determine $f(1)$ we cannot make conclusion about the value $f(0) \oplus f(1)$

TRUTH TABLE

A	B	X
0	0	0
0	1	1
1	0	1
1	1	1

AND

The Deutsch algorithm is a quantum algorithm capable to determine the value $f(0) \oplus f(1)$ by making only a single query to a quantum oracle for f

The given reversible circuit for f can be made into a quantum circuit by replacing every reversible classical gate with analogous unitary quantum gate. This quantum gate can be expressed as a unitary operator

$$U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$$

U_f is defined so that if we set the second qubit in the state $|y\rangle = |0\rangle$, then $|x\rangle = |0\rangle$ in the first input qubit will give $|0 \oplus f(0)\rangle = |f(0)\rangle$ in the second output bit and $|x\rangle = |1\rangle$ in the first input qubit will give you

$$|1 \oplus f(x)\rangle = |f(1)\rangle$$

Therefore we can think of $|x\rangle = |0\rangle$ as a quantum version of the classical input „0" bit and $|x\rangle = |1\rangle$ as a classical input „1" bit.

Of course the state of the input can be a superposition of $|0\rangle$ and $|1\rangle$

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1)$$

Suppose, if we keeping the second qubit, $|y\rangle = |0\rangle$ and the first is in superposition (1) then the two qubit input to operator U_f is

$$|\Psi\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle$$

Remember! $$f(0) \oplus f(1) = \begin{cases} 0 & f(0) = f(1) \text{ constant} \\ 1 & f(0) \neq f(1) \text{ balanced} \end{cases}$$

The output of U_f gate is

$$U_f|\Psi\rangle|0\rangle = U_f(\alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle) =$$

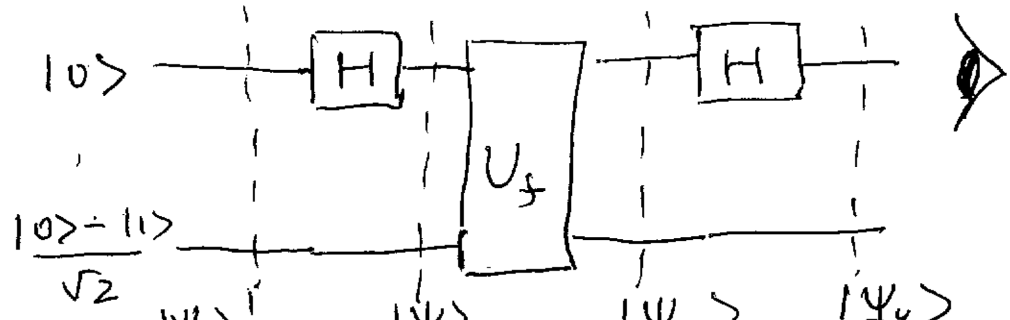
$$\alpha U_f|0\rangle|0\rangle + \beta U_f|1\rangle|0\rangle = \alpha|0\rangle|0 \oplus f(0)\rangle + \beta|1\rangle|0 \oplus f(1)\rangle$$

$$= \alpha|0\rangle|f(0)\rangle + \beta|1\rangle|f(1)\rangle$$

Therefore U_f computed the value of f on both possible inputs 0 and 1. as result of measurments we optain output state in computational basis as $|0\rangle|f(0)\rangle$ with probability α and $|1\rangle|f(1)\rangle$ with probability β. We have succesfully compute two value in superposition but through measurment we got only one in computation basis.

Recall, the Deutsch algorithm is not optaining a value of f(x), but dereruining the value of $f(0) \oplus f(1)$, and one can use the quantum interferece to optain such global information about the function f

The Deutsch algorithm circuit is show in Fig. 1



The first qubit in state $|0\rangle$ and the second qubit in superposition state $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Let us analyze this algorithm through the state at each stage of the circuit

① The input state

$$|\Psi_0\rangle = |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} ;$$

② After the Hadamard gate is applied to the first qubit the state is

$$|\Psi_1\rangle = H|\Psi_0\rangle = H|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) =$$

$$= \frac{1}{\sqrt{2}}|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

③ after applying U_f gate on $|\Psi_1\rangle$ we have to use phase kick back algorithm.

$$U_f|\Psi_1\rangle = ?$$

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

$$|\Psi_2\rangle = U_f|\Psi_1\rangle = U_f\left(\frac{|0\rangle}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)+\frac{|1\rangle}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right)=$$

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

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

$$=(-1)^{f(0)}\left(\frac{|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

We used here that $(-1)^{f(0)}\cdot(-1)^{f(1)}=(-1)^{f(0)\oplus f(1)}$

4 If f is constant $f(0)\oplus f(1)=0$ then we have

$$|\Psi_2\rangle=(-1)^{f(0)}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

Hadamard gate applied on $|\Psi_2\rangle$

$$|\Psi_3\rangle=H|\Psi_2\rangle=H(-1)^{f(0)}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=$$

$$=(-1)^{f(0)}|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

The square norm of the first qubit is 1. This means that for a constant function a measurment of the first qubit is certain to return value $0=f(0)\oplus f(1)$.

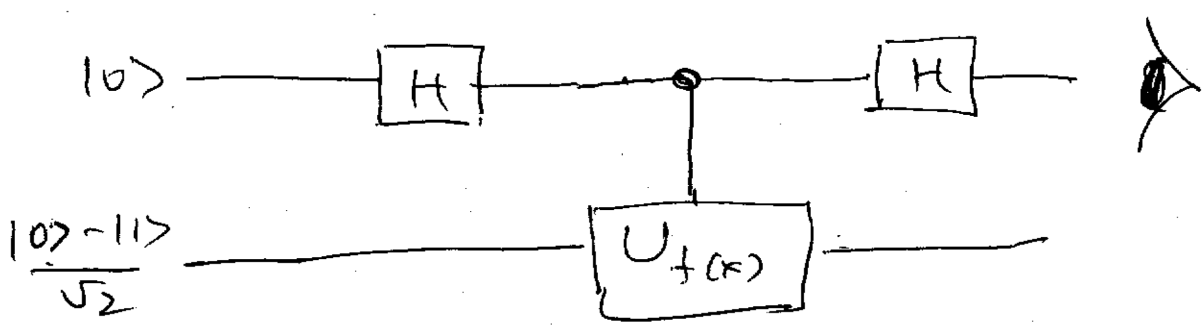
If f is balanced function $f(0)\oplus f(1)=1$ then we have

$$|\Psi_3\rangle=H|\Psi_2\rangle=H(-1)^{f(0)}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=(-1)^{f(0)}|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

In this case the square norm of the basis state $|1\rangle$ in the first qubit is 1. This means that for the balanced function the measurement of the first qubit is certain to return the value $1 = f(0) \oplus f(1)$.

Therefore, the measurement of the first qubit at the end of Deutsch algorithm determines the value $f(0) \oplus f(1)$ and whether the function is constant of balanced.

The Deutsch algorithm can be generalized that the operator $U_f|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$ in the Deutsch algorithm can be seen as a single-qubit operator $U_{f(x)}$ whose action can be control by the first qubit.



The state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ is the eigenstate with eigenvalue $(-1)^{f(x)}$. By encoding this eigenvalue in the phase factor of the first qubit we are able to determine $f(0) \oplus f(1)$ by determining the relative phase factor between $|0\rangle$ and $|1\rangle$