Quantum Information Processing and Quantum Computing 06/11/2015

Lecture 8: Quantum Computing; Deutsch and Deutsch-Jozsa Algorithms

Instructor: Goutam Paul *Scribe: Arka Rai Choudhuri*

1 Introduction

Consider the evaluation of a boolean function f at the point $x \in \{0,1\}$, i.e. we want $f(x)$ where

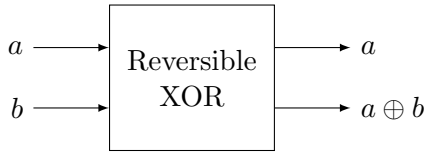
$$f : \{0,1\}^n \to \{0,1\}$$

If we can implement any such function f, then we can implement any algorithm. This follows from the fact that any algorithm at the lowest level is just a sequence of boolean functions. As with the classical domain, we are not bothered with how f is implemented.

In general f is not reversible, specifically when there is a domain reduction. The natural question to ask is how one could make such a function reversible.

To illustrate this, consider $f(a,b) = a \oplus b$. From the truth table we observe that it is not possible to directly revert the function. Instead, we output some addition information (variable a in this case), as shown below to construct a "Reversible XOR".

a	b	$a \oplus b$	a
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1



We state below a theorem, without proof, which will be used extensively

Theorem 1.1 *For any boolean function f, $\exists$ a unitary transformation U_f such that*

$$|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle \tag{1}$$

for $x \in \{0,1\}^n$ and $y \in \{0,1\}$. ■

In the quantum domain, for any f, we assume U_f exists and take this to be a black box.

2 Deutsch Algorithm

Consider a 1-variable boolean function f. We know that there are $2^{2^1} = 4$ such possible functions. We list them out below,

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
0	0	0	1	1
1	0	1	0	1

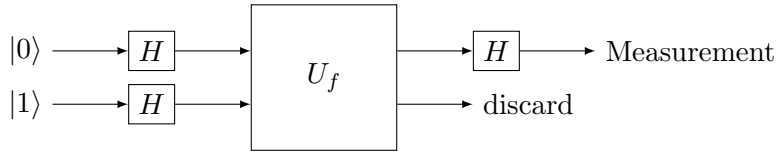
Suppose we are interested in determining which of the two alternatives hold:

1. f is **constant**, or
2. f is **balanced**.

A function f is said to be *balanced* if each output appears equal number of times. Specifically, from the table above, f_0 and f_3 are constant, while f_1 and f_2 are balanced.

In the classical domain, we would require exactly 2 queries to conclude if it were balanced or constant. We now consider this problem in the quantum domain in an attempt to improve on the number of queries.

To this end, we present the **Deutsch Algorithm** in the figure below.



Note that the actual query is $|0\rangle$, while $|1\rangle$ is an auxiliary bit.

The joint input state $|w\rangle$ to U_f is,

$$\begin{aligned} |w\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{aligned}$$

Before we proceed, we state a couple of rules,

Rule 1: $U_f|xy\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$

Rule 2: $|y\rangle - |1 \oplus y\rangle = (-1)^y(|0\rangle - |1\rangle)$

The first rule follows from the theorem stated earlier, and the second rule can easily be verified to be true. Now,

$$\begin{aligned}
U_f|w\rangle &= \frac{1}{2}(U_f|00\rangle - U_f|01\rangle + U_f|10\rangle - U_f|11\rangle) \\
&= \frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle) \\
&= \frac{1}{2}(|0\rangle(|f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|f(1)\rangle - |1 \oplus f(1)\rangle)) \\
&= \frac{1}{2}\left(|0\rangle\left[(-1)^{f(0)}(|0\rangle - |1\rangle)\right] + |1\rangle\left[(-1)^{f(1)}(|0\rangle - |1\rangle)\right]\right) \\
&= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= |w_1\rangle \otimes |w_2\rangle
\end{aligned}$$

Here each $|w_i\rangle$ is a 1-qubit state. In our diagram for the algorithm, we're discarding $|w_2\rangle$ and only considering $|w_1\rangle$. Now,

$$\begin{aligned}
H|w_1\rangle &= H\left[\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)\right] \\
&= (-1)^{f(0)}H\left[\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right)\right] \qquad (2)
\end{aligned}$$

We now state our third rule, which can easily be verified to be true.

Rule 3: $H|y\rangle \rightarrow \frac{|0\rangle+(-1)^y|1\rangle}{\sqrt{2}}$

Note, a consequence of this rule

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

This follows from the fact that the Hadamard transform applied twice to the state returns the original state.

In Eq.(2), we take y to be $f(0) \oplus f(1)$.

$$H|w_1\rangle = (-1)^{f(0)}|f(0) \oplus f(1)\rangle$$

We now perform a measurement in the $\{|0\rangle, |1\rangle\}$ basis. Based on the measurement,

- if $|0\rangle$ is measured, f is **constant**.
- if $|1\rangle$ is measured, f is **balanced**.

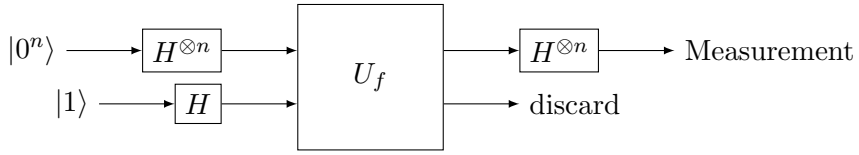
It is important to note that although only a single query is made, we are essentially querying the superposition of $|0\rangle$ and $|1\rangle$ using the Hadamard gate.

3 Deutsch-Jozsa Algorithm

We now extend the problem discussed in the previous section. Here the function f, is defined as

$$f : \{0,1\}^n \to \{0,1\}$$

It is guaranteed that f is either balanced or constant, and we would like to determine the same. In the classical setting, we would require at least $\frac{2^n}{2} + 1$ queries. As before, in an attempt to improve this, we consider the problem in the quantum setting, and describe the **Deutsch-Jozsa Algorithm** using the diagram below,



Here, $H^{\otimes n}$ is defined as

$$H^{\otimes n}|x_1 \cdots x_n\rangle = H|x_1\rangle \otimes \cdots \otimes H|x_n\rangle \tag{3}$$

Let us represent the input state as,

$$|\psi_0\rangle = |0^n\rangle|1\rangle \tag{4}$$

After the Hadamard transform on $|0^n\rangle$ and $|1\rangle$, we get the input to U_f to be,

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{5}$$

Now, applying U_f, similar to before,

$$|\psi_2\rangle = U_f|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{6}$$

For ease of notation, we expand the Hadamard transform on a state $|x\rangle$.

$$H^{\otimes n}|x_1 \cdots x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1,z_2,\cdots,z_n} (-1)^{x_1z_1+\cdots+x_nz_n}|z_1 \cdots z_n\rangle \tag{7}$$

This can be re-written as

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle \tag{8}$$

where $x \cdot z$ is the bitwise inner product of x and z, modulo 2.

As seen from the algorithm, we drop the last bit from $|\psi_2\rangle$ to obtain $|\psi_3\rangle$. Applying the Hadamard transform on $|\psi_3\rangle$, using the notations discussed, we get,

$$|\psi_4\rangle = H|\psi_3\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{\sqrt{2^n}} \left(\sum_{y\in\{0,1\}^n} \frac{(-1)^{x\cdot y}|y\rangle}{\sqrt{2^n}} \right) \tag{9}$$

$$= \sum_{x\in\{0,1\}^n} \sum_{y\in\{0,1\}^n} \frac{(-1)^{f(x)+x\cdot y}|y\rangle}{2^n} \tag{10}$$

Now, we look at the amplitude associated with the state $|0^n\rangle$, given by

$$\sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{2^n}$$

Hence the probability associated with this is

$$\left| \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{2^n} \right|^2$$

As is easily seen, the probability is 1 if f is **constant**. Hence, we get

- f is **constant** if $|0^n\rangle$ is measured.
- f is **balanced** otherwise.

Again, with just one query, we were able to determine if the function f was constant or balanced.

References

[1] Nielsen, Michael A., and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2010.

[2] https://cs.uwaterloo.ca/ watrous/CPSC519/LectureNotes/04.pdf

[3] https://cs.uwaterloo.ca/ watrous/CPSC519/LectureNotes/05.pdf