Lecture 4 - Quantum Oracles and Deutsch's Algorithm

The Eigensolvers

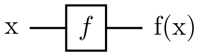
July 8, 2021

Recall from previous lectures that the quantum computing model is reversible, which means that function mapping from input space to output space is bijective. This means that all quantum circuit must have the same number of inputs and outputs. However, it is possible to only measure a subsets of the output qubits.

1 Quantum Oracle

Many quantum algorithms employs the use of an oracle, which is a black box function whose exact composition is unknown but actions is well-defined.

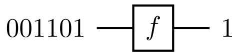
In the classical setting, oracles takes in an arbitrary input x and return the output $f(x)$. The function f takes the form of the oracle.



For example, let the input x be the binary string '001101'. The actions defined by the oracle is defined as

$$f(x) = \begin{cases} 0 \text{ if } x \text{ is even} \\ 1 \text{ if } x \text{ is odd} \end{cases}$$

From this, we can get the output



- Note that the input and output can be of different sizes.

Quantum oracles works in much the say way as their classical counterparts, except that they are reversible. The simplest quantum oracle consists of two qubits, one data qubit and one target qubit. The data qubit also called the input bit, and is unaffected by the oracle. The target qubit is necessary for reversibility and is set to a fixed classical state.

Recall that $\oplus$ performs the action of the classical XOR. Below is the truth table of $\oplus$ on all the basis states.

$\|y\rangle$	$\|f(x)\rangle$	$\|y \oplus f(x)\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

However, quantum computing also allows for $\oplus$ superposition of basis states. We simply perform the actions independently on each basis states, and combines them with the correct amplitudes.

$$\begin{aligned} |0\rangle \oplus (\alpha |0\rangle + \beta |1\rangle) &= \alpha(|0 \oplus 0\rangle) + \beta(|0 \oplus 1\rangle) \\ &= \alpha |0\rangle + \beta |1\rangle \end{aligned}$$

$$\begin{aligned}|1\rangle \oplus (\alpha |0\rangle + \beta |1\rangle &= \alpha(|1 \oplus 0\rangle) + \beta(|1 \oplus 1\rangle) \\ &= \alpha |1\rangle + \beta |0\rangle\end{aligned}$$

With these information in mind, we can dive into our first quantum algorithm.

2 Deutsch's Algorithm

2.1 Some Definitions

A classical function is unary if it takes in one bit as input.

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

A unary function is said to be constant if it gives the same output for all inputs. We have two classical constant functions constant-0 and constant-1, denoted as [0] and [1].

x	Constant-[0]
0	0
1	0

x	Constant-[1]
0	1
1	1

A unary function is said to be balanced if it returns the same number of 1 as it does 0. We also have two classical balanced functions: identity and negation, denoted I and X. These are also quantum gates, because they satisfy reversibility. Once again,

x	Identity
0	0
1	1

x	Negation
0	1
1	0

In summary,

- Constant-[0]: $f(x) = 0$
- Constant-[1]: $f(x) = 1$
- Identity: $f(x) = x$
- Negation: $f(x) = \overline{x}$

2.2 Problem Statement

Suppose we are given a unary function in a black box. We want to determine whether it is constant or balanced in a single query.

2.3 Classical Approach

Because our function is in a black box, we don't know its exact composition. However, we can get insight about its action by passing some inputs and look at the outputs. In classical computing, we need two queries to find out if our oracle is constant or balanced.

Input	Output	Possible Functions	Constant or Balanced
0	0	[0] or I	Undecidable
0	1	[1] or X	Undecidable
1	0	[0] or X	Undecidable
1	1	[1] or I	Undecidable

For each of the input-output pairs, we can infer two possible functions that fit the description. We would need another input to decide for certain whether the oracle is constant or balanced.

2.4 Quantum Approach / Deutsch's Algorithm

Using a quantum computer, we can determine whether a unary function is constant or balanced with a single query. With our recent understanding of quantum oracle, let us try to motivate the Deutsch's algorithm from scratch. Recall a few important facts,

- XOR Identities
$$0 \oplus a = a, 1 \oplus a = \overline{a}$$
- X Basis Vectors
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle,$$
- Oracle Actions
$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

Now let's work through some basic examples with the oracle,

- $y = 0$
$$\begin{aligned} U_f|x\rangle|0\rangle &= |x\rangle|0 \oplus f(x)\rangle \\ &= |x\rangle|f(x)\rangle \end{aligned}$$
- $y = 1$
$$\begin{aligned} U_f|x\rangle|1\rangle &= |x\rangle|1 \oplus f(x)\rangle \\ &= |x\rangle\left|\overline{f(x)}\right\rangle \end{aligned}$$
- $y = -$
$$\begin{aligned} U_f|x\rangle|-\rangle = U_f|x\rangle\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \\ = \frac{1}{\sqrt{2}}U_f|x\rangle|0\rangle - \frac{1}{\sqrt{2}}U_f|x\rangle|1\rangle \\ = \frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle\left|\overline{f(x)}\right\rangle \end{aligned}$$

At this point, we can make two observations:

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

Overall, for an arbitrary binary output in $f(x)$

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

Keeping with $|y\rangle = |-\rangle$, we are going to try a few more examples with different values for $|x\rangle$

- $x = 0$

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

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

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

- $x = 1$

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

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

$$= (-1)^{f(1)}\left|1\right\rangle\left|-\right\rangle$$

- $x = +$

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

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

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

The states the we just obtained can tell us more about the nature our oracle function $f(x)$. For each of the four cases of unary function, we have a different output.

- If f is constant-[0], where $f(x) = 0$, then

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

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

$$= \left|+\right\rangle\left|-\right\rangle$$

- If f is constant-[1], where $f(x) = 1$, then

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

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

$$= -\left|+\right\rangle\left|-\right\rangle$$

  Note that the negative sign is global phase.

- If f is the identity function, where $f(x) = x$

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

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

$$= \left|-\right\rangle \left|-\right\rangle$$

- If f is the negation function, where $f(x) = \overline{x}$

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

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

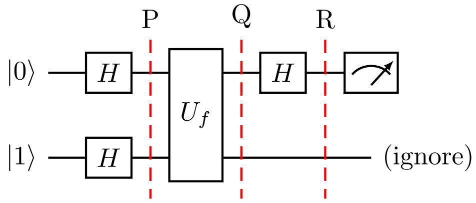
$$= -\left|-\right\rangle \left|-\right\rangle$$

  Again, the negative sign here is a global phase

Looking at the output for the of each of the four cases, we can see that if our oracle function f is constant, the first qubit will result in $\left|+\right\rangle$. On the other hand, if our oracle function f is balanced, the first qubit will result in $\left|-\right\rangle$. However, since our machine will always measure in the Z-basis, we cannot distinguish between $\left|+\right\rangle$ and $\left|-\right\rangle$. Therefore, we will apply a Hadamard gate to the first qubit to transform it back to the Z-basis. This will have the following action.

$$H\left|+\right\rangle = \left|0\right\rangle, \quad H\left|-\right\rangle = \left|1\right\rangle$$

Taking what we have done, now we implement it on a quantum circuit. The Deutsch's algorithm takes the following shape.



To recap, at point P, applying Hadamards on both qubits give us the state $\left|+\right\rangle\left|-\right\rangle$. At Q, after applying the oracle to both qubits, we have

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

Depending on whether our oracle is constant or balanced, our top qubits will be either $\left|+\right\rangle$, or $\left|-\right\rangle$. We apply the Hamadard gate at R, to distinguish these two states, and determine our oracle type. All in all, if we measure a $\left|0\right\rangle$, our oracle is balanced, and if we measure a $\left|1\right\rangle$, our oracle is constant.

This takes advantage of two techniques:

1. Quantum Parallelism:

   Non-trivial superposition can explore all basis states at the same time. Applying the Hadamard gates to bring calculations out of the Z-basis has this effect. Quantum entanglement also plays a big part within the oracle implementation.

2. Phase Kickback:

   Information of $f(x)$ from B is transferred to A. The process includes transforming both A & B to the X-basis, where phase-kickback could occur. When this is done, A will respond differently to constant and balanced function. This effect is visible when brought back to the Z-basis.

2.5 Designing the Oracles

There are four unary functions that we can implement as part of our oracle:

1. Constant-[0]
2. Constant-[1]
3. Identity
4. Negation

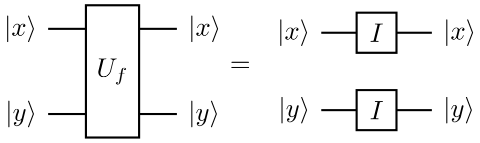
Here, we will only cover the first three functions, the negation function will be left as an exercise to the readers in the problem sets.

Constant-[0]

Recall that this function is defined as $f(x) = 0$. In terms of the oracle actions, we have

$$U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus 0\rangle = |x\rangle\,|y\rangle$$

This is easy because we can just pass both our input $|x\rangle$ and $|y\rangle$, through to the output without applying any gates.

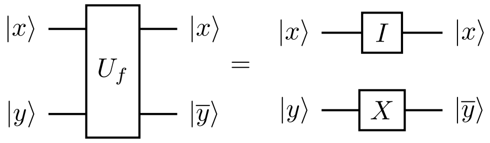


Constant-[1]

The constant-[1] function is defined as $f(x) = 1$. In terms of the oracle actions, we have

$$U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus 1\rangle = |x\rangle\,|\overline{y}\rangle$$

By inspection, we can see that the $|x\rangle$ state is unaffected by oracle, whereas the $|y\rangle$ is bit-flipped.

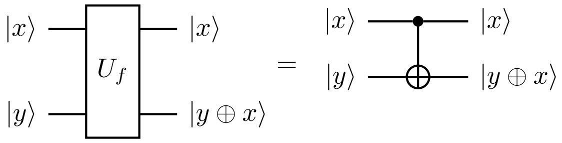


Identity

In this case, our oracle function is defined as $f(x) = x$. Equivalently,

$$U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus x\rangle$$

Coincidentally, this the classic actions of the standard $CNOT$ gate.

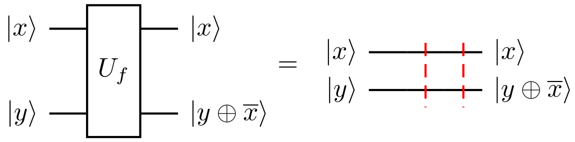


Hints for the Negation oracle

The negation oracle has the action $f(x) = \overline{x}$. Equivalently,

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus \overline{x}\rangle$$

In circuit form, we see something very similar to the case of the identity function. We only need to make a small modifications to the above circuit to get the answer.


$|x\rangle$
$|y\rangle$
U_f
$|x\rangle$
$|y \oplus \overline{x}\rangle$
$=$
$|x\rangle$
$|y\rangle$
$|x\rangle$
$|y \oplus \overline{x}\rangle$