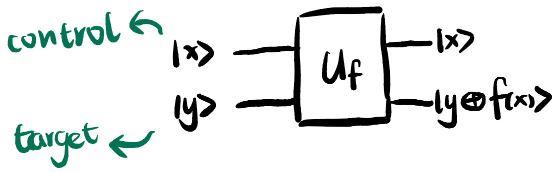
Deutch-Josza Algorithm

I. The Quantum Oracle



$U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$

1. f is a binary function $f: \mathbb{Z}_2 \to \mathbb{Z}_2$
2. There are four possible functions

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	1	0	1
1	0	0	1	1

3. f is constant if $f(0) = f(1)$

   $f_1(x)$ & $f_4(x)$

4. f is balanced if $f(0) \oplus f(1) = 1$

   $f_2(x)$ & $f_3(x)$

Notation: $\oplus$ is addition modulo 2.

$a \oplus b := a + b \pmod 2$

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

Cheat Sheet

- $x \oplus 0 = x$
- $x \oplus 1 = !x$, we say x is flipped

$x = 0$ or $x = 1$

II. Task

Determine if f is constant or balanced using as few queries to the Quantum Oracle shown above as possible.

III. When $|x\rangle$, $|y\rangle$ are Computational Basis

$U_f(|0\rangle|0\rangle) = |0\rangle|f(0)\rangle$

$U_f(|1\rangle|0\rangle) = |1\rangle|f(1)\rangle$

$U_f(|0\rangle|1\rangle) = |0\rangle|!f(0)\rangle$

$U_f(|1\rangle|1\rangle) = |1\rangle|!f(1)\rangle$

Case 1: $f = f_1$	Case 2 $f = f_2$	Case 3 $f = f_3$	Case 4 $f = f_4$
$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$
$\|1\rangle\|0\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|1\rangle\|1\rangle$
$\|0\rangle\|1\rangle$	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|0\rangle$
$\|1\rangle\|1\rangle$	$\|1\rangle\|1\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|0\rangle$

By querying the Quantum Oracle twice, we can determine if f is constant or balanced. Could we do better?

IV Navigation

1. When only control is in a superposition state, e.g., $|x\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

$$U_f(|+\rangle|0\rangle) = U_f\left(\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|0\rangle\right) = U_f\left(\frac{|00\rangle+|10\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}[U_f(|00\rangle)+U_f(|10\rangle)] = \frac{1}{\sqrt{2}}[|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle]$$

$$U_f(|+\rangle|1\rangle) = U_f\left(\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|1\rangle\right) = U_f\left(\frac{|01\rangle+|11\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}[U_f(|01\rangle)+U_f(|11\rangle)] = \frac{1}{\sqrt{2}}[|0\rangle|!f(0)\rangle+|1\rangle|!f(1)\rangle]$$

$$U_f(|-\rangle|0\rangle) = U_f\left(\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\otimes|0\rangle\right) = U_f\left(\frac{|00\rangle-|10\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}[U_f(|00\rangle)-U_f(|10\rangle)] = \frac{1}{\sqrt{2}}[|0\rangle|f(0)\rangle-|1\rangle|f(1)\rangle]$$

$$U_f(|-\rangle|1\rangle) = U_f\left(\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\otimes|1\rangle\right) = U_f\left(\frac{|01\rangle-|11\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}[U_f(|01\rangle)-U_f(|11\rangle)] = \frac{1}{\sqrt{2}}[|0\rangle|!f(0)\rangle-|1\rangle|!f(1)\rangle]$$

Reasoning analogously as before, we can analyze each output state when $f\in\{f_1, f_2, f_3, f_4\}$.

Let's use $U_f(|+\rangle|0\rangle) = \frac{1}{\sqrt{2}}[|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle]$ as an example.

Case 1: $f=f_1$

$$U_f(|+\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle) = |+\rangle|0\rangle = |\psi_1\rangle$$

Case 2: $f=f_2$

$$U_f(|+\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) = |\psi_2\rangle$$ entangled!

Case 3: $f=f_3$

$$U_f(|+\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) = |\psi_3\rangle$$ entangled!

Case 4: $f=f_4$

$$U(|+\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|01\rangle+|11\rangle) = |+\rangle|1\rangle = |\psi_4\rangle$$

However $\langle\psi_1|\psi_2\rangle = \frac{1}{2}$, this means $|\psi_1\rangle$ and $|\psi_2\rangle$ are indistuishable. Or in other words, there is no measurement that we could make to distinguish $|\psi_1\rangle$ from $|\psi_2\rangle$. Reasoning analogously $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle, |\psi_4\rangle\}$ are pair-wise indistinguishable. Hence we could not tell from the measurements if we have a constant function or a balanced function.

2. When only target is in a superposition state, e.g., $|y\rangle = |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

$$U_f(|0\rangle|+\rangle) = U_f\left(|0\rangle\otimes\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\right) = U_f\left(\frac{|00\rangle+|01\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}U_f(|00\rangle+|01\rangle) = \frac{1}{\sqrt{2}}[U_f(|00\rangle)+U_f(|01\rangle)] = \frac{1}{\sqrt{2}}[|0\rangle|f(0)\rangle+|0\rangle|!f(0)\rangle]$$

$$U_f(|1\rangle|+\rangle) = U_f\left(|1\rangle\otimes\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\right) = U_f\left(\frac{|10\rangle+|11\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}U_f(|10\rangle+|11\rangle) = \frac{1}{\sqrt{2}}[U_f(|10\rangle)+U_f(|11\rangle)] = \frac{1}{\sqrt{2}}[|1\rangle|f(1)\rangle+|1\rangle|!f(1)\rangle]$$

$$U_f(|0\rangle|-\rangle) = U_f\left(|0\rangle\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right) = U_f\left(\frac{|00\rangle-|01\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}U_f(|00\rangle-|01\rangle) = \frac{1}{\sqrt{2}}[U_f(|00\rangle)-U_f(|01\rangle)] = \frac{1}{\sqrt{2}}[|0\rangle|f(0)\rangle-|0\rangle|!f(0)\rangle]$$

$$U_f(|1\rangle|-\rangle) = U_f\left(|1\rangle\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right) = U_f\left(\frac{|10\rangle-|11\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}U_f(|10\rangle-|11\rangle) = \frac{1}{\sqrt{2}}[U_f(|10\rangle)-U_f(|11\rangle)] = \frac{1}{\sqrt{2}}[|1\rangle|f(1)\rangle-|1\rangle|!f(1)\rangle]$$

Reasoning analogously as before, we can analyze each output state when $f\in\{f_1, f_2, f_3, f_4\}$.

Let's use $U_f(|0\rangle|-\rangle) = \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle - |0\rangle|!f(0)\rangle$ & $U_f(|1\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|1\rangle|f(1)\rangle - |1\rangle|!f(1)\rangle]$ as examples.

Case 1: $f=f_1$

$$U_f(|0\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|0\rangle|0\rangle - |0\rangle|1\rangle] = |0\rangle|-\rangle \qquad U_f(|1\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|1\rangle|0\rangle - |1\rangle|1\rangle] = |1\rangle|-\rangle$$

Case 2: $f=f_2$

$$U_f(|0\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|0\rangle|1\rangle - |0\rangle|0\rangle] = -|0\rangle|-\rangle \qquad U_f(|1\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|1\rangle|0\rangle - |1\rangle|1\rangle] = |1\rangle|-\rangle$$

Case 3: $f=f_3$

$$U_f(|0\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|0\rangle|0\rangle - |0\rangle|1\rangle] = |0\rangle|-\rangle \qquad U_f(|1\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|1\rangle|1\rangle - |1\rangle|0\rangle] = -|1\rangle|-\rangle$$

Case 4: $f=f_4$

$$U_f(|0\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|0\rangle|1\rangle - |0\rangle|0\rangle] = -|0\rangle|-\rangle \qquad U_f(|1\rangle|-\rangle) = \frac{1}{\sqrt{2}}[|1\rangle|1\rangle - |1\rangle|0\rangle] = -|1\rangle|-\rangle$$

$$U_f(|x\rangle|-\rangle) = U_f\left(\frac{|x\rangle|0\rangle - |x\rangle|1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\left(U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle\right) = \frac{1}{\sqrt{2}}[|x\rangle|f(x)\rangle - |x\rangle|!f(x)\rangle] = (-1)^{f(x)}|x\rangle|-\rangle \quad (*)$$

3. When both control and target are in superpositions.

Let's consider $|x\rangle = |+\rangle$ and $|y\rangle = |-\rangle$:

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

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

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

Case 1 or Case 4 : When $f=f_1$ or $f=f_4$, i.e, when f is constant.

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

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

→ global phase could be omitted.

Case 2 or Case 3 : When $f=f_2$ or $f=f_3$ i.e, when f is balanced

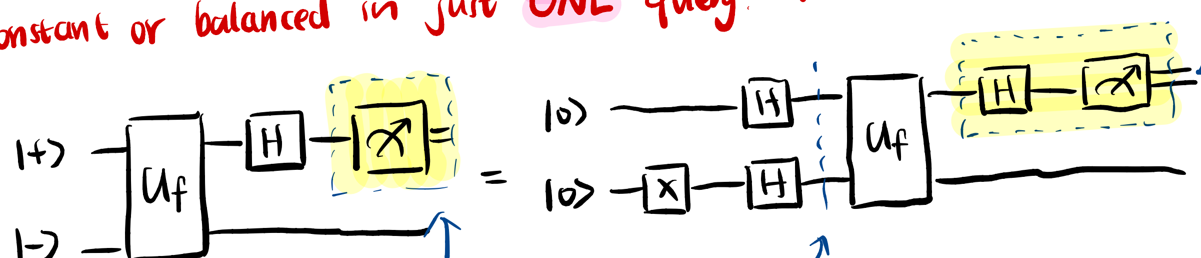
$f(1) - f(0) = 1$ or -1

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

→ global phase could be omitted.

Note: $(-1)^1 = (-1)^{-1} = -1$

Hence, measuring the control qubit in the X basis tells us whether the function is constant or balanced in just ONE query. A visualization is shown below.



Measure the control qubit in the X basis

Measure the control qubit in the z basis.

The state of the inputs to Uf are $|+\rangle|-\rangle$.