The Deutsch Jozsa Algorithm

`Input`: A function f on $\Sigma^n \rightarrow \Sigma$ which is either balanced or constant.

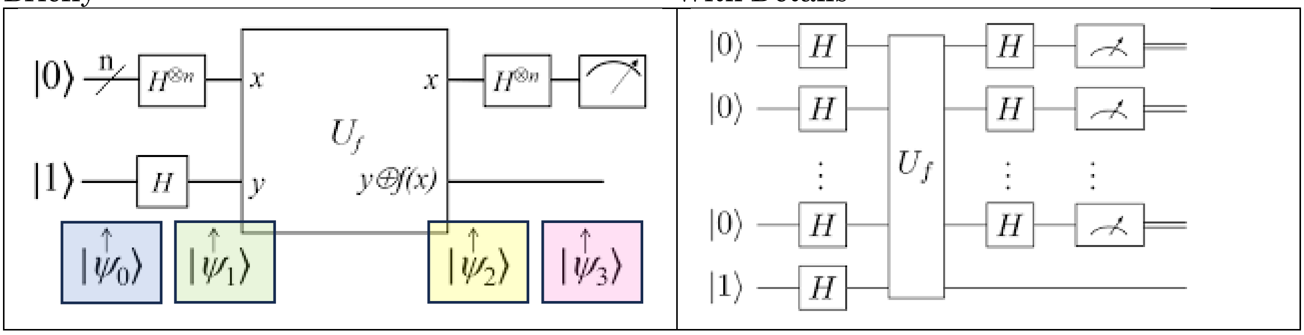
[`Constant`: $f(x) = 0$ for all values of x OR $f(x) = 1$ for all values of x;

`Balanced`: $f(x) = 0$ for half of the inputs and $f(x) = 1$ for the other half of the inputs]

`Output`: "1" if f is constant, "0" if it is balanced using a single query to an oracle that computes $U_f(|x\rangle\,|y\rangle) \rightarrow |x\rangle|y \oplus f(x)\rangle$

The Circuit:

Briefly — With Details



The steps are as follows:

$$|\psi_0\rangle = |0\rangle^{\otimes n}\,|1\rangle$$

Each of the qubits in $|\psi_0\rangle$ is acted upon by a Hadamard gate,

$$|\psi_1\rangle = H|0\rangle^{\otimes n}\,H|1\rangle$$

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

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n - 1} |x\rangle\,(|0\rangle - |1\rangle)$$

Now we apply the unitary operation U_f to $|\psi_1\rangle$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n - 1} U_f(|x\rangle\,(|0\rangle - |1\rangle))$$

After applying U_f,

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n - 1} (|x\rangle\,(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle))$$

Since $(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) = (-1)^{f(x)}(|0\rangle - |1\rangle)$, (as studied in the class), therefore

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n - 1} (-1)^{f(x)}\,|x\rangle\,(|0\rangle - |1\rangle)$$

At this stage we apply a Hadamard to $\sum_{x=0}^{2^n-1} |x\rangle$ where x represents all possible strings over Σ^n.

Since

$$H(|0\rangle) = (|0\rangle + (-1)^0|1\rangle) \ / \ \sqrt{2}\ ,$$

$$H(|1\rangle) = (|0\rangle + (-1)^1|1\rangle) \ / \ \sqrt{2}\ ,$$

and therefore,

$$H|x\rangle = ((-1)^{0.x}\,|0\rangle + (-1)^{1.x}\,|1\rangle) / \sqrt{2}$$

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} (-1)^{xz}\,|z\rangle$$

However, consider the situation when x is an n bit string, i.e., x has n bits, i.e., $x_1, x_2, \ldots, x_n$.

In that case,

$$H|x\rangle = H|x_1\rangle\, H|x_2\rangle \ldots H|x_n\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{z_1=0}^{1} (-1)^{x_1 z_1}\,|z_1\rangle \ \frac{1}{\sqrt{2}} \sum_{z_2=0}^{1} (-1)^{x_2 z_2}\,|z_2\rangle \ \ldots \frac{1}{\sqrt{2}} \sum_{z_n=0}^{1} (-1)^{x_n z_n}\,|z_n\rangle$$

Plugging in this expression in place of $|x\rangle$ in $|\psi_2\rangle$, we get,

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \frac{1}{\sqrt{2}} \sum_{z_1=0}^{1} (-1)^{x_1 z_1}\,|z_1\rangle \ \frac{1}{\sqrt{2}} \sum_{z_2=0}^{1} (-1)^{x_2 z_2}\,|z_2\rangle \ldots \frac{1}{\sqrt{2}} \sum_{z_n=0}^{1} (-1)^{x_n z_n}\,|z_n\rangle\,(|0\rangle - |1\rangle)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{n+1}}} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \sum_{z_1 z_2 \ldots z_n = 0}^{1} (-1)^{f(x)} (-1)^{x_1 z_1} (-1)^{x_2 z_2} \ldots (-1)^{x_n z_n}\ |z_1\rangle|z_2\rangle\ldots|z_n\rangle$$

$$\boldsymbol{|\psi_3\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{z_1 z_2 \ldots z_n = 0}^{1} (-1)^{f(x) + x_1 z_1 + x_2 z_2 + x_n z_n}\,|z\rangle}\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\ \boldsymbol{\textit{where}}\ |z\rangle = |z_1\rangle|z_2\rangle\ldots|z_n\rangle.$$

We can discard the lower qubit $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

and measure the top qubit(s) only which are:

$$\boldsymbol{\frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{z_1 z_2 \ldots z_n = 0}^{1} (-1)^{f(x) + x_1 z_1 + x_2 z_2 + x_n z_n}\,|z\rangle.}$$

What is the probability of measuring the state $|z\rangle = |00\ldots0\rangle$, i.e, $z_1 = z_2 = \ldots = z_n = 0$?

It is given by:

$$P(\text{Measuring all 0s}) = \Big(\frac{1}{2^n} \sum_{x=0}^{2^n - 1} (-1)^{f(x)} \Big)^2$$

Observe that if $f(x)$ is constant, then either $f(x) = 0$ for all values of x, leading to

$$P = \frac{1}{2^n} \big((-1)^0 + (-1)^0 + \ldots (-1)^0 \big)^2 = 2^n / 2^n = 1.$$

Or $f(x) = 1$ for all values of x leading to,

$$P = \frac{1}{2^n} \big((-1)^1 + (-1)^1 + \ldots (-1)^1 \big)^2 = 2^n / 2^n = 1.$$

So if $f(x)$ is constant, there is a 100% probability of measuring all 0s the first n qubits.

What happens if $f(x)$ is balanced.

In that case, whenever $f(x) = 0$, $(-1)^{f(x)} = 1$, and

Whenever $f(x) = 1$, $(-1)^{f(x)} = -1$,

Therefore, the probability is,

$P = \frac{1}{2^n} ((-1)^0 + (-1)^1 + \ldots (-1)^0)$ **(this is –1 for half of the inputs and +1 for the other half)**

$= 0 / 2^n = 0.$

Hence if $f(x)$ is balanced, there is no chance of measuring all 0s.

This completes the analysis of the algorithm.

The Bernstein-Vazirani Algorithm

To get an idea of the Bernstein-Vazirani Algorithm, we will workout an example here.

Although the Bernstein-Vazirani Problem is somewhat different as compared to Deutsch-Jozsa Problem, the solution is almost similar.

Consider a two-bit string u = ______________ (Choose any string that you would like).

Now create a function on a two-bit string i.e., $x = x_1 x_2$ such that

$f(x) = u \cdot x = u_1 x_1 \oplus u_2 x_2$

Example: Suppose $u = 10$.

Then the following function: $f(00) = 0$, $f(01) = 0$, $f(10) = 1$, $f(11) = 1$ satisfies the above condition.

Note that not all functions on two bits are of this type (i.e. there exists a u that satisfies the dot-product condition).

The Bernstein Vazirani Problem states that:

[Promise] Suppose we are given a function on $\Sigma^n \rightarrow \Sigma$ which can be expressed as a dot product of a string u and the input x. Can you find u, and if yes, using how many queries to f?

Write, discuss and think the Classical Solution here:

Quantum Solution: It turns out, that the quantum solution requires only 1 query to the oracle and is surprisingly similar to the Deutsch Jozsa Algorithm. It is as follows:

1. Start with the state: $|0\rangle^{\otimes n}|1\rangle$
2. Apply $H|0\rangle^{\otimes n}\ H|1\rangle$
3. Now apply the oracle to this state to get $\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\ |x\rangle\ (\,|0\rangle - |1\rangle\,)$
4. Now apply Hadamard to the top n qubits to get $\frac{1}{2^n} \sum_{x=0}^{2^n-1}\ \sum_{z_1 z_2 \ldots z_n=0}^{1} (-1)^{f(x) + x_1 z_1 + x_2 z_2 + x_n z_n}\ |z\rangle$
5. Finally measure the top n qubits.
6. The result of the measurement is your answer u.
7. Try it now for the above two bit function!