Quantum Computing Lab

Assignment on Bernstein-Vazirani algorithm

Haricharan B
EP21B015

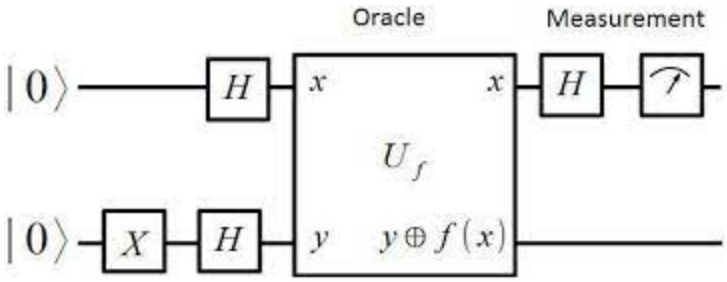
The Deutsch Algorithm

Consider a classical function $f : \{0, 1\} \rightarrow \{0, 1\}$. Now, we are told that the function is either

- Constant
- Balanced, i.e. 0 for half the inputs and 1 for the rest

Classically, we would need two function calls to determine what the function is. But, using the power of quantum mechanics, we can do it in one function call.

Let the function (called an *oracle*) be represented by some matrix U, where U is a unitary matrix.



Consider the quantum circuit as above. Now, the input to the oracle will be:

$$\boxed{\frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle)}$$

For various values of the function, the output would be:

- $f(x) = 0$

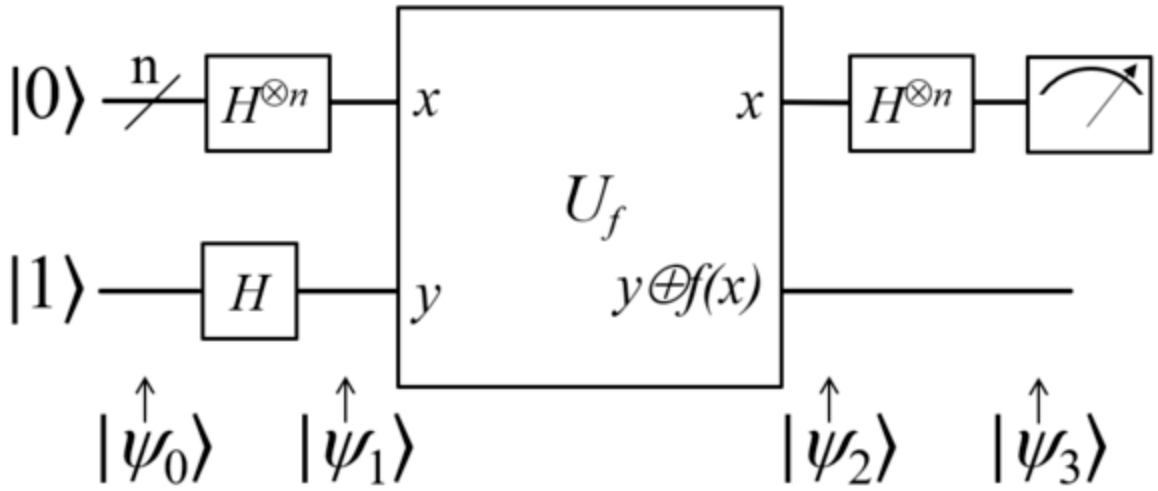
- $\boxed{\frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle)}$
  - On passing the first qubit through a Hadamard gate, the function will be $|0\rangle \oplus |-\rangle$
  - On measuring the first qubit, we get the state $|0\rangle$ always.
- $f(x) = 1$
  - $\boxed{\frac{1}{2}(|01\rangle + |11\rangle - |00\rangle - |10\rangle)}$
  - On passing the first qubit through a Hadamard gate, the function will be $|0\rangle \oplus -|-\rangle$
  - On measuring the first qubit, we get the state $|0\rangle$ always.
- $f(0) = 0, f(1) = 1$
  - $\boxed{\frac{1}{2}(|00\rangle + |11\rangle - |01\rangle - |10\rangle)}$
  - The above state is actually $|-\rangle \oplus |-\rangle$
  - On passing the first qubit through a Hadamard gate, the function will be $|1\rangle \oplus |-\rangle$
  - On measuring the first qubit, we get the state $|1\rangle$ always.
- A similar pattern can be observed for $f(0) = 1, f(1) = 0$ also.

Conclusion

On measuring the first qubit,

- If we get $|0\rangle$ with probability 1, the function is constant
- The function is a balanced function otherwise.

The Deutsch-Josza Algorithm



The above Deutsch algorithm can be extended to a function $f : \{0,1\}^n \to \{0,1\}$, and the modified algorithm is called *Deutsch-Josza algorithm.* This can be used to determine if a function is balanced or constant.

Note that in this case, we want our Oracle to be from $f : \{0,1\}^n \to \{0,1\}^n$, but our function has only one output. So, our oracle will be the of the following form: for instance, if $n = 4$, $\text{Oracle}(a, b, c, d) = (a, b, c, d \oplus f(x))$.

By considering an analogy with the above Deutsch Algorithm, we measure the first n qubits:

- If we get $|0\rangle^{\otimes n}$ with probability 1, the function is constant
- The function is a balanced function otherwise.

So, we have an efficient algorithm to determine if a function is balanced or constant by using only one function call!

Bernstein-Vazirani Algorithm

Let's define the dot product $f : \{0,1\}^n \to \{0,1\}$ of an input bit-string x (of length n) and a secret string s (also of length n) to be the following:

$$\boxed{f(x) = x \cdot s = x_1 s_1 \oplus x_2 s_2 \oplus \cdots \oplus x_n s_n}$$

Now, our aim is to determine the secret string s.

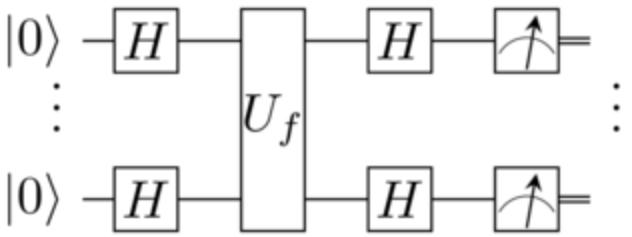
Classical Solution

$$
\begin{aligned}
f(1000\cdots0_n) &= s_1 \\
f(0100\cdots0_n) &= s_2 \\
f(0010\cdots0_n) &= s_3 \\
&\vdots \\
f(0000\cdots1_n) &= s_n
\end{aligned}
$$

We pass in inputs in which only one bit is 1 and all the other bits are 0. The output we get will be the nth bit of the secret string. This will give us the respective secret string in n function calls. In the quantum case, we can do it using a single function call!

Quantum Solution

Note that our oracle U_f is defined as above, i.e. the first $n-1$ bits are same as the input, and the nth bit is $x_n \oplus f(x)$.



Schematic Diagram

Steps:

- We start with the state $|0\rangle^{\otimes n}$
- We pass it through $H^{\otimes n}$, to generate $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$
- On passing the above state through U_f, we get $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$
- Now, we apply $H^{\otimes n}$ on the above state. We will get $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$
- Note that, this state is identically equal to $|s\rangle$ with probability 1! This is because, we have a $(-1)^{f(x)+x \cdot y}$ in the above equation, and $f(x) = x \cdot s$. So, the summation

is equal to 1 if and only if $s = y$, and is 0 otherwise.

So, if we just measure the output state, it will be identically equal to $|s\rangle$ with probability 1. This is amazing, as this let's us determine the secret string in a single function call.