Assignment-1: Oracle for Simon's Algorithm

Jessica John Britto

July 15, 2022

1 Finding Unitary Matrix for the Oracle

For a **single qubit**, the oracle should output the following for the input qubit-

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

So, we get the matrix as - $U_{f1} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 1 \\ \\ \frac{1}{\sqrt{2}} & 0 \end{bmatrix}$

For **two qubits**, the oracle should output the following for the input qubits-

1. $U_f\left|00\right\rangle = \frac{1}{2}(\left|11\right\rangle + \left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle)$
2. $U_f\left|10\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|01\right\rangle)$
3. $U_f\left|01\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|10\right\rangle)$
4. $U_f\left|11\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)$

So, we get the matrix as - $U_{f2} = \begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \\ \frac{1}{2} & 0 & \frac{1}{\sqrt{2}} & 0 \\ \\ \frac{1}{2} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \\ \frac{1}{2} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}$

Finding U_{f2} by taking the tensor product of U_{f1} gives -

$$U_{f2}^{'} = U_{f1} \otimes U_{f1} = \begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 1 \\ \\ \frac{1}{2} & 0 & \frac{1}{\sqrt{2}} & 0 \\ \\ \frac{1}{2} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \\ \frac{1}{2} & 0 & 0 & 0 \end{bmatrix}$$

Clearly, U_{f2} is not same as U'_{f2}.

For **three qubits**, the oracle should output the following for the input qubits-

1. $U_f\left|000\right\rangle = \frac{1}{2\sqrt{2}}(\left|000\right\rangle+\left|001\right\rangle+\left|010\right\rangle+\left|011\right\rangle+\left|100\right\rangle+\left|101\right\rangle+\left|110\right\rangle+\left|111\right\rangle)$
2. $U_f\left|001\right\rangle = \frac{1}{2}(\left|000\right\rangle + \left|010\right\rangle + \left|100\right\rangle + \left|110\right\rangle)$
3. $U_f\left|010\right\rangle = \frac{1}{2}(\left|000\right\rangle + \left|001\right\rangle + \left|100\right\rangle + \left|101\right\rangle)$
4. $U_f\left|011\right\rangle = \frac{1}{2}(\left|000\right\rangle + \left|011\right\rangle + \left|100\right\rangle + \left|111\right\rangle)$
5. $U_f\left|100\right\rangle = \frac{1}{2}(\left|000\right\rangle + \left|001\right\rangle + \left|010\right\rangle + \left|011\right\rangle)$
6. $U_f\left|101\right\rangle = \frac{1}{2}(\left|000\right\rangle + \left|010\right\rangle + \left|101\right\rangle + \left|111\right\rangle)$
7. $U_f\left|110\right\rangle = \frac{1}{2}(\left|000\right\rangle + \left|001\right\rangle + \left|110\right\rangle + \left|111\right\rangle)$
8. $U_f\left|111\right\rangle = \frac{1}{2}(\left|000\right\rangle + \left|011\right\rangle + \left|101\right\rangle + \left|110\right\rangle)$

So, we get the matrix as - $U_{f3} = \begin{bmatrix} \frac{1}{2\sqrt{2}} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2\sqrt{2}} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ \frac{1}{2\sqrt{2}} & \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{1}{2\sqrt{2}} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \frac{1}{2\sqrt{2}} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 \\ \frac{1}{2\sqrt{2}} & 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2\sqrt{2}} & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2\sqrt{2}} & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$

2 Circuit for Simon's Algorithm

When input is "011", we get the following circuit as shown in figure-1.

The input bit string has to be reversed to follow Qiskit's ordering. The occurrence of the first non-zero string bit of the reversed input string must

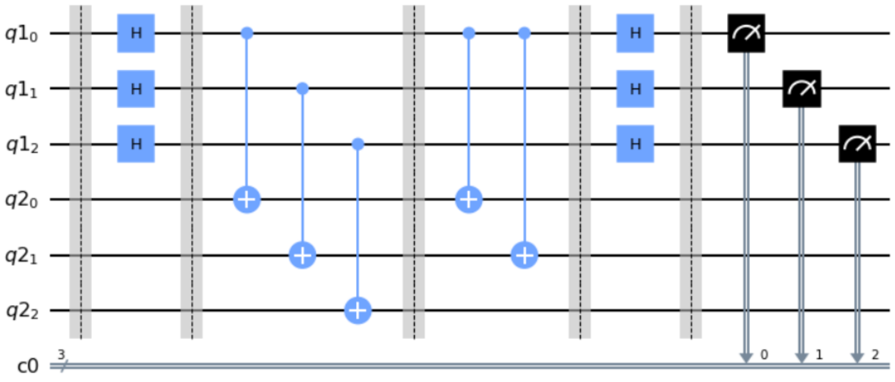

Figure 1: Circuit for Simon's Algorithm

be stored in a variable [called *flagbit*].

Its oracle is implemented by first copying the qubits of input register to that of the second register using CNOT gates, i.e, $q1_a \longrightarrow q2_a$. Then, whenever, we have a non-zero string bit occuring in the reversed string, we perform a $CNOT$ operation with control as input register qubit whose index corresponds to *flagbit* and target as second register qubit whose index corresponds to the index of the occurrence of a non-zero bit string in the reversed input string.

Code for the oracle -

```
for i in range(n):
    qc.cx(q1[i],q2[i])
qc.barrier()

if flagbit != -1:
    for ind, bit in enumerate(b_rev):
        if bit == "1":
            qc.cx(flagbit, q2[ind])
```

3 References

1. Exploring Simon's Algorithm with Daniel Simon