Week 3:
Oracle Based Algoritms

Quantum Oracle

- An oracle is a “black box” containing information about an unknown binary string $X = X_1X_2\cdots X_N$
- In the quantum setting the oracle containing unknown string $X = X_1X_2\cdots X_N$ acts as $O\,|i\rangle\,|a\rangle \longrightarrow |i\rangle\,|a \oplus X_i\rangle.$
- If we set ancilla qubit $|a\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. the oracle acts as $O_f\,|i\rangle\,|-\rangle \longrightarrow (-1)^{X_i}\,|i\rangle\,|-\rangle.$ This is called “Phase Kickback”.

Quantum Oracles

- Oracles are linear operators.
- Oracles can also represent a Boolean functions.
- Oracles can be implemented as quantum circuits.
- For example the function $f(x) = x_1 \cdot x_2$, we can implement the function using the CCNOT gate where the control qubits are the query qubits and the target qubit is the output qubit.

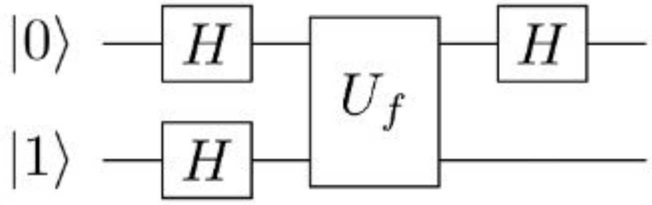
Deutsch Algorithm

Given a Boolean function $f : \{0,1\} \longrightarrow \{0,1\}$, Deutsch algorithm helps us check if the function is balanced or constant.

- Classically it take two queries to the function.
- But in a quantum setting we need just a single query!
- Deutch algorithm uses the concept on interferene to obtain this speedup.

Deutsch Algorithm

- The circuit for the Deutsch algorithm is as below



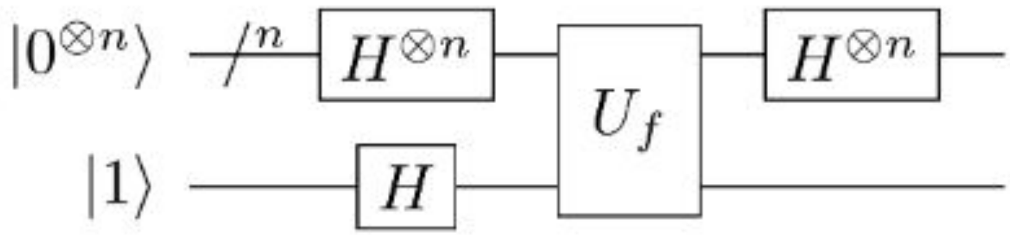
Deutsch Algorithm

- The evolution of the states is as follows:

$$
\begin{aligned}
|0\rangle|1\rangle &\xrightarrow{H\otimes H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|-\rangle \\
&\xrightarrow{U_f} \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)\,|-\rangle \\
&\xrightarrow{H\otimes I} \frac{1}{2}\Big[\Big((-1)^{f(0)} + (-1)^{f(1)}\Big)|0\rangle + \Big((-1)^{f(0)} - (-1)^{f(1)}\Big)|1\rangle\Big]\,|-\rangle
\end{aligned}
$$

Deutsch-Jozsa Algorithm

Deutsch Jozsa algorithm is a generalization of Deutsch algorithm. The circuit of DJ algorithm is as follows



Deutsch-Jozsa Algorithm

The evolution of the state of the system is as below:

$$
\begin{aligned}
|0\rangle|1\rangle &\xrightarrow{H\otimes H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle \\
&\xrightarrow{U_f} \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)|-\rangle \\
&\xrightarrow{H\otimes I} \frac{1}{2}\left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right]|-\rangle
\end{aligned}
$$

Grover’s Algorithm

- Grover’s algorithm is one of the most popular quantum algorithms that is the backbone of many other quantum algorithms.
- It is a method that offers polynomial speed up over best known classical algorithms for solving a wide class of important problems.
- One such problem is the unordered search where a classical algorithm needs O(N) queries while Grover’s search requires only O(sqrt(N)).

Simon’s Algorithm

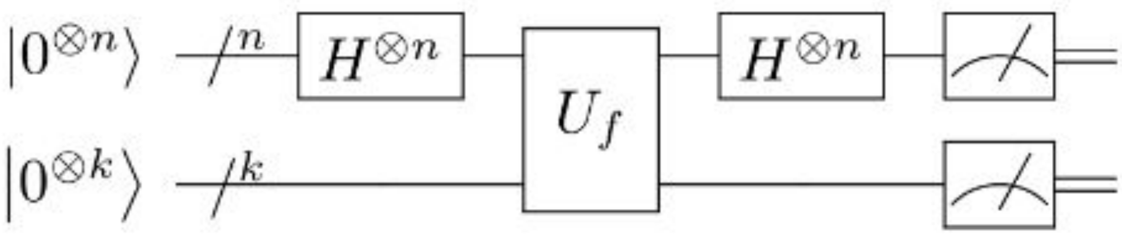
<u>Simon’s Problem:</u>

Given a function such that the output values of the function is identical iff the inputs differ by a fixes shift s, our goal is to find the s.

Simon’s algorithm efficiently uses the exclusively quantum concepts of constructive and destructive interference to solve the period-finding problem.

Simon's Algorithm

- While a classical algorithm uses atleast $O(2^{n/2})$ queries, Simons's algorithm solves the same in O(n) queries. The circuit for Simon's algorithm is as follows:



Refer to handouts for detailed explanations