Deutch's algorithm

Assume the Oracle is a "black box" that encodes an unknown function \(f(x)\)

\[
\begin{align*}
|0\rangle & \rightarrow |0\rangle |0\rangle \\
|1\rangle & \rightarrow |1\rangle |f(0)\rangle
\end{align*}
\]

• How many times do we need to query the Oracle in order to determine whether \(f(0)\) is constant or balanced? (i.e. whether \(f(0)\) is \(0\) or \(1\)?)

\[
|0\rangle |f(0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle |0\rangle + |1\rangle |1\rangle)
\]

Deutch's algorithm for \(|0,1\rangle\rightarrow|0,1\rangle\)

\[
|0\rangle |f(0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle |0\rangle + |1\rangle |1\rangle)
\]

\[
= \frac{1}{2} \left[ (|0\rangle + |1\rangle)(|f(0)\rangle + |\bar{f}(0)\rangle) - (|0\rangle - |1\rangle)(|f(0)\rangle - |\bar{f}(0)\rangle) \right]
\]

Remark about Deutch's algorithm

• It took advantage of "quantum parallelism"

\[
|f(0)\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}
\]

• No info whatsoever would be gained by measuring output register \(y\). Also, the quantum procedure yielded information on the actual value of \(f(0)\) or \(\bar{f}(0)\) Note the trade-off here. We gave up the knowledge of \(f(0)\) in order to obtain "behavioral" or "logical" information on \(f(x)\) for all \(x\)

Circuit derivation: Let's "open the hood" of the Oracle

• Recall from last class:

\[
\begin{align*}
|0\rangle & \rightarrow |0\rangle \\
|1\rangle & \rightarrow |1\rangle
\end{align*}
\]

• Note how the "H" flipped the OR gate of the balanced \(f(x)\) only. Circuit we get the same result with a classical reversible computer? The answer is no, it is not reversible. And we can flip the output bits with an XOR gate. So, we say the circuit would be \(|f(x)\rangle\) or \(|\bar{f}(x)\rangle\) for either if \(|f(x)\rangle\) is constant or balanced.

Action of Hadamard on qubits

• To generalize Deutch to many qubits, we need this:

\[
|\psi\rangle = \frac{1}{2} \sum_{i=0}^{2^n-1} (-1)^i |i\rangle
\]

• "Blaise module 2 inner product"

\[
\langle \psi | \phi \rangle = \sum_{i=0}^{2^n-1} (-1)^i \langle i | \psi \rangle \langle \psi | i \rangle
\]

• Example:

\[
|\psi\rangle = \frac{1}{2} \sum_{i=0}^{2^n-1} (-1)^i |i\rangle
\]

Generalizing Deutch to \(|0,1\rangle\rightarrow|0,1\rangle\)

• Now there are 2 inputs \(x\):

Support you know a priori that \(f(x)\) is either constant or balanced. How many queries do you need to assert that \(f(x)\) is either constant or balanced? (This is called "quantum parallelism"

Summary

• Before an algorithm inputs a superposition state containing all computational basis states into the Oracle:

\[
\begin{align*}
|\psi\rangle & = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle
\end{align*}
\]

• Due to linearity, when the Oracle acts on this state, it evaluates \(f(x)\) for all \(x\) simultaneously. This is called "quantum parallelism"

• The resulting state can now be "engineered" with additional units in order to yield useful information where read out. For example, applying \(|\psi\rangle = |0,1\rangle\).

This was an exercise to show that Deutch's algorithm is more than just a "quantum" algorithm. It is a valid algorithm that performs much better than classical but only if you have access to the Oracle.