Quantum Computing: An Introduction

by Amit Behera - Saturday, June 30, 2018

http://gonitsora.com/quantum-computing-an-introduction/

Over the years, the methods and techniques of computations have undergone havoc advancements regarding efficiency and feasibility. Till now in modern day "classical" computers, the primary source or representations of information are bits which can be 0 or 1 signifying on and off respectively.

Now consider a machine where one unit represents much more information than this. It can hold not only 0 or 1 but also any possible superpositions of the classical zeros and ones. No classical machine can do that. Isn't it evident that such a machine will be far more superior to the classical computers in terms of efficiency?

Well, in theory, quantum mechanics allow us to do so in the form of qubits. A single qubit, in general, can represent any vector of a two dimensional Hilbert space so fixing elements of any orthonormal basis as a representation of 0 and 1 we get any possible combination or superposition of 0 and 1.

An n-bit classical bit string can take only one of the $latex 2^n$ possible values but we cannot create any superposition of these states whereas an n qubit quantum state can represent any vector of $latex 2^n$ dimensional Hilbert space. Hence it can represent any possible superposition of the $latex 2^n$ basis elements Each of the individual basis states can be represented by an n-bit classical string, but we can never have any superposition of these states using n classical bits. So to do some computation on all of these $latex 2^n$ states, we can just compute on the superpositions instead of applying the computation individually on each of the $latex 2^n$ states.

To illustrate with an example we can look at the Deutsch Problem.

To begin with, let's define the term oracle. An oracle is a sub-routine or a sub-algorithm which is usually expensive and can be queried multiple times during the algorithm.

Now, coming back to the problem, if we are given a function $latex f : \{0,1\}^n \rightarrow \{0,1\}$

with oracle access and has the property that it is either constant or balanced, and we need to figure out whether it is balanced or constant. By balanced we mean the function gives 0 output on half the inputs and 1 output on the rest half of inputs, whereas constant means it gives the same output on all the inputs.

Classically, we need to query the function oracle on at least $latex (2^{n-1} + 1)$ possible strings and check whether it is constant or not. But we can do this very efficiently only by one query using quantum computing, thanks to the superposition property that we mentioned.

Basically, we need to prepare an n qubit quantum state which is a suitable superposition of all the $latex 2^n$ basis states (each representing each of the $latex 2^n$ n-bit classical strings) and call the quantum analogue of that function oracle on an n+1 qubit state comprising of an ancillary qubit and the prepared n qubit state. The ancillary qubit helps to check the behaviour of the function on the superposition and measuring the n-qubits at the end; we can accurately tell whether it is constant or balanced.

Here also, the critical factor is that since the quantum state is a superposition of all the $latex 2^n$ basis states, by only one query to the quantum oracle, we manage to get hold of the "$latex f$" value of each of the $latex 2^n$ basis states or in other words, the image of all possible inputs under $latex f$. Hence, in some sense, in the quantum setting, one oracle call does the work of $latex 2^n$ oracle queries in the classical context. This algorithm quite cleverly exploits this fact, the complete technicalities of which can be found here: Deutsch Jozsa algorithm.

Another interesting property that qubits posses is the No-cloning theorem. It states that if you are given an unknown quantum state, there is no way you can tell of your own, what state it is in, with certainty, hence cannot copy or clone it. This is again a striking difference, between classical bit-strings and qubits. Classically, you can always tell the state as soon as I give you the classical bit-string and can copy it easily. Hence, qubits appear to be a better candidate as information-carriers than classical bit-strings since unlike the classical bit-strings, qubits are irreproducible and hence are more secured by the fundamental principles of Quantum mechanics. Due to the same reasons, the No-cloning theorem is at the very core of Quantum Cryptology and Quantum Information.

This was a brief introduction to the fascinating world of quantum computing.

In Deutsch’s words:

> Quantum Computation is…...a distinctively new way of harnessing nature….it will be the first technology that allows useful tasks to be performed in collaboration with parallel universe.