Innovative Project Report

On

Revolutionizing Technology Using Quantum Computing

Submitted in complete fulfillment of the requirements for the mid-term examination evaluation

Submitted by

Lakshay Chandra

Date: April 2021

TABLE OF CONTENTS

ABSTRACT

Quantum computing is an area of computing focused on developing computer technology based on the principles of quantum theory, which explains the behaviour of energy and material on the atomic and subatomic levels.

The present-day classical computers use binary data formations to store memory i.e., the digital technology we use today can encode information in **bits** that can take the value 0 or 1. Quantum computing, on the other hand, uses quantum bits or qubits which possess a unique ability of quantum states that can exist as a combination of 0 and 1. This means in quantum computing the information has the possibility of existence in both of the states 0 and 1.

Quantum computing is based mainly on two aspects of quantum physics: Superposition and Entanglement.

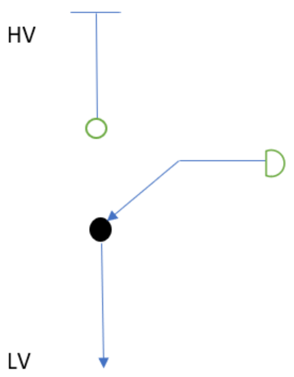
One of the properties that set a qubit apart from a classical bit is that it can be in superposition. A quantum state in superposition can be seen as a linear combination of other distinct quantum states. This quantum state in superposition forms a new valid quantum state. A quantum computer consisting of n qubits can exist in a superposition of 2^n states while n bits can store only n numbers at any specific point in time. This empowers quantum computers to handle operations at speeds exponentially higher than conventional computers and much lesser energy consumption.

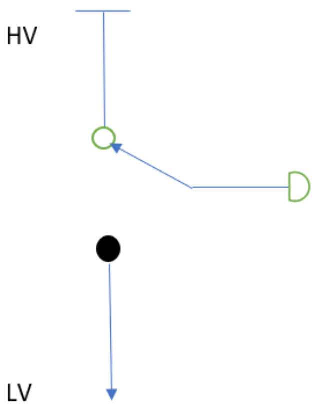
Entanglement in quantum physics, much to its literal meaning is a counter-intuitive phenomenon in quantum physics. A pair or group of particles is entangled when the quantum state of each particle cannot be described independently of the quantum state of the other particle(s) but the quantum state of the system can be described.

Quantum computing has the potency of revolutionizing the technology we use today. Quantum computers could spur the development of breakthroughs in science, medications to save lives, machine learning methods to diagnose illnesses sooner, materials to make more efficient devices and structures, financial strategies to live well in retirement, and algorithms to quickly direct resources such as ambulances.

INTRODUCTION

The classical computers we use today, work on the basis of binary logic. This means that the information in them is encoded in the form of binary numbers, which are numbers that can take one out of the two values 0 or 1. The physical object that carries this binary information is called a bit. In today’s computers, the bit is represented by the state of a transistor inside a silicon chip. 0 is represented by a Low voltage and 1 is represented by a High voltage. The transistor works as a switch that selects any one between the two possible values of voltages.





Transistor in State **0** Transistor in State **1**

Consider a system comprising of 2 bits. Then there are 4 possible combinations of values: **00, 01, 10, 11,** which are the binary representations of numbers: 0, 1, 2, and 3, respectively.

Similarly, for 3 bits, there will be 8 combinations from **000** to **111**, which represent the numbers from 0 to 7.

Hence, with N bits we will have a total of $\mathbf{2^n}$ combinations representing the numbers from 0 to 2^n-1.

A computer processes digital data by performing logical operations.

The simplest one is on a single bit. The **NOT operation** which inverts the value of the bit, i.e., 0 becomes 1 and 1 becomes 0.

The **AND operation** operates between 2 bits and return the value **1,** if both the inputs are 1, and returns the value **0** otherwise.

A **NAND Gate**, which is an **AND Gate** followed by a **NOT gate** returns the value **0** if both inputs are 1, and returns **1** otherwise.

NAND Gates are universal logic gates because any binary logic operation can be broken down into a sequence of NAND gates.

Modern computers contain over a billion tiny silicone transistors connected in a way that allows a programmer to decide which sequence of logic operations takes place.

Thus, all operations we perform on a computer like: web surfing, video streaming, e-mailing, programming, performing complex calculations, etc. are processed at the transistor level inside the silicon chip.

However, there are certain calculations that not even the most powerful super computer can tackle, such as:

- finding the prime factors of large numbers,
- designing molecules and materials
- finding the shortest path between many cities, and many other optimization problems.

For solving such problems which are unique in the fact that all of them involve a very large database, we need a quantum computer.

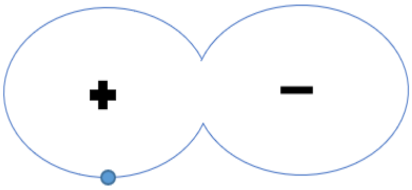
Through this case study, we would be exploring the quantum aspects of physics through a discussion on the two main principles of quantum computing: Superposition and Entanglement. We would also analyze qubits and a simple case of the quantum search algorithm which would mark the dissimilarity in how a quantum computer functions compared to a classical computer. We would conclude by studying about Quantum Supremacy and the limitations and scope of present-day Quantum computers.

QUBIT AND SUPERPOSITION OF STATES

At the microscopic level of atoms and electrons, the world obeys the laws of quantum mechanics. One of the fundamental principles of quantum mechanics is that it is possible to create super positions of different physical configurations.

The simplest analogy of superposition is observed in an H^+_2 molecule (a monoelectronic system). The molecule consists of 2 protons and 1 electron.

This electron could belong to either of the two protons. If we decide to encode binary information on the position of the electron, we can say that the electron belongs to **0** (left proton) or **1** (right proton). However, since the electron is a quantum object it can belong to both left and right protons. In other words, it exists as a superposition of the two states **0** and **1**. A simple diagram representing the H^+_2 molecule is shown below:



Qubit

A quantum system that has two basis states is called a quantum bit or qubit. Physically a qubit can be represented by the **spin of the electron** in which the two levels can be taken as spin up and spin down; or **the polarization of a single photon** in which the two states can be taken to be the vertical polarization and the horizontal polarization. In a classical system, a bit would have to be in one state or the other. However, quantum mechanics allows the qubit to be in a coherent superposition of both states simultaneously, a property which is fundamental to quantum mechanics and quantum computing.

To define the value of a qubit, we need to specify what quantum super position it's in. A pure qubit state is a superposition of 2 coherent states. In general, a qubit is represented by:

|Ψ> = a|0> + b|1>

Here **|0>** ***and*** **|1>** are called basis states (or vectors) and have matrix representations :

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ respectively.

α and **β** are probability amplitudes and can in general both be complex numbers. the probability of outcome **|0>** with value "0" is | **a** $|^2$ and the probability of outcome **|1>** with value "1" is | **b** $|^2$. Thus,

$$| a|^2 + | b |^2 = 1.$$

a qubit in this superposition state does not have a value in between "0" and "1"; rather, when measured, the qubit has a probability | ***a*** $|^2$ of the value "0" and a probability | **b** $|^2$ of the value "1".

In other words, superposition means that there is no way, even in principle, to tell which of the two possible states forming the superposition state actually pertains. Therefore, even though a qubit can exist as a superposition of 2 states, during measurement it must fall back exactly into one of the two states. And the outcome measured is completely random.

Now, if we increase the complexity by considering 2 qubits, we would be having 4 basis states namely, **00**, **01**, **10** and **11**. And the superposition of these 4 states would be represented by:

|Ψ> = a|00> + b|01> + c|10> + d|11>

where | **a** $|^2$ + | **b** $|^2$ + | **c** $|^2$ + | **d** $|^2$ = 1

Similarly, with 3 qubits we would have to specify 8 numbers: **a** to **h** to describe the superposition and so on. Every time we add a qubit, we need twice as many numbers to describe the collective state of these qubits. So, for n qubits we would require $\mathbf{2^n}$ numbers to describe the superposition of $\mathbf{2^n}$ states. Whereas in a classical bit, each state is completely specified given the value of each bit.

If we have 50 qubits, we would require $2^{50} \approx 1$ quadrillion number to describe their collective state.

This property of qubits makes them markedly different from classical bits and gives us a sense of the enormous complexity in the quantum realm. The aim of quantum computing is to harness this complexity to perform certain calculations much faster than any standard computer ever could.

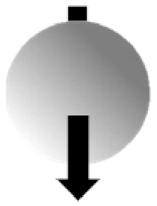
MEASUREMENT OF STATES

Quantum mechanics allows us to create super positions of different physical configurations. In quantum computers we can make super positions of quantum digital codes and the amount of information necessary to describe these super positions grows exponentially with the number of qubits. However, not all of this information is accessible to us because the process of quantum measurement poses a fundamental limit.

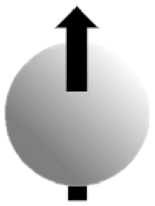
Illustration of quantum Spin

A spin is the simplest kind of quantum bit. All particles like electrons, protons and neutrons have the property of possessing an intrinsic magnetic dipole which acts like a microscopic compass needle. In reality, the spin is an intrinsic quantum property of the particle and does not actually involve any physical spinning. Just like a compass needle, the spin has the tendency to align itself along a magnetic field.

If we take an electron and place it in a magnetic field, it will have two basis quantum states - spin down and spin up. Since there is only two of them, we can also call them |0> and |1> respectively and use them to encode quantum information.



|0>

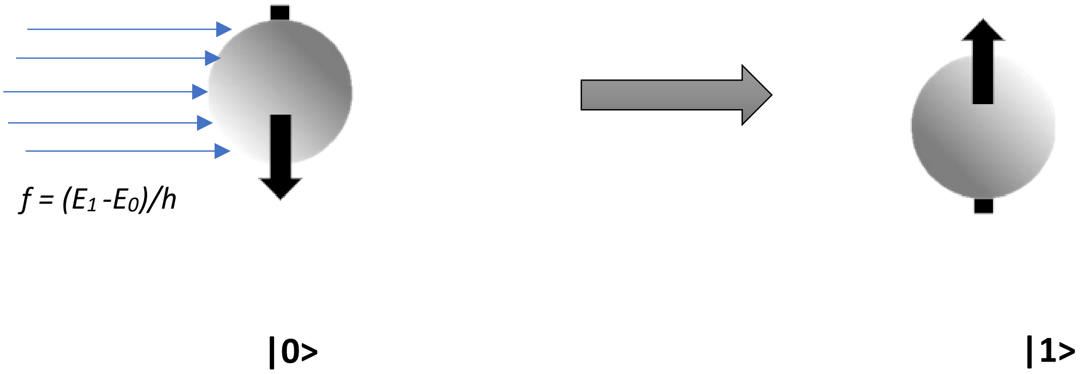


|1>

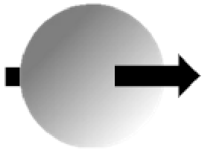
Each of these states is associated with some energy. We consider the energy of the |0> state to be lower than |1> state. Let the respective energies be E_0 and E_1.

If the spin in the |0> state is irradiated with an electromagnetic wave of frequency

$f = (E_1 - E_0)/h$, where h is the planks constant , the spin would turn around to achieve the higher spin state |1> as shown below.



Now we will create a superposition of the two spin states. The superposition should point horizontally with no vertical component.



$$1\sqrt{2}|0\rangle + 1\sqrt{2}|1\rangle$$

However, on several measurements of the spin, we observe spin up sometimes and spin down the other times. That means the measurement always converges into one of the two basis states |0> or |1> .This is known as **collapse of the wavefunction**. Hence, the process of measurement modifies the state of the spin. Moreover, the outcome of our measurement is probabilistic. i.e., we cannot tell in which measurement we will observe spin up and vice versa. But we do observe both the states. Hence, we can assign a probability to the states knowing the type of superposition we have created. For example, if prepare the following superposition:

$|\Psi> = 0.6|0> + 0.8|1>$

$P_0 = 0.6^2 = 0.36$ (or 36%)

$P_1 = 0.8^2 = 0.64$ (or 64%)

If the system is already in one of the basis states (|0> or |1>) then we have a special case in which we can tell with certainty which state it is. In other words, the outcome is well determined with 100% probability.

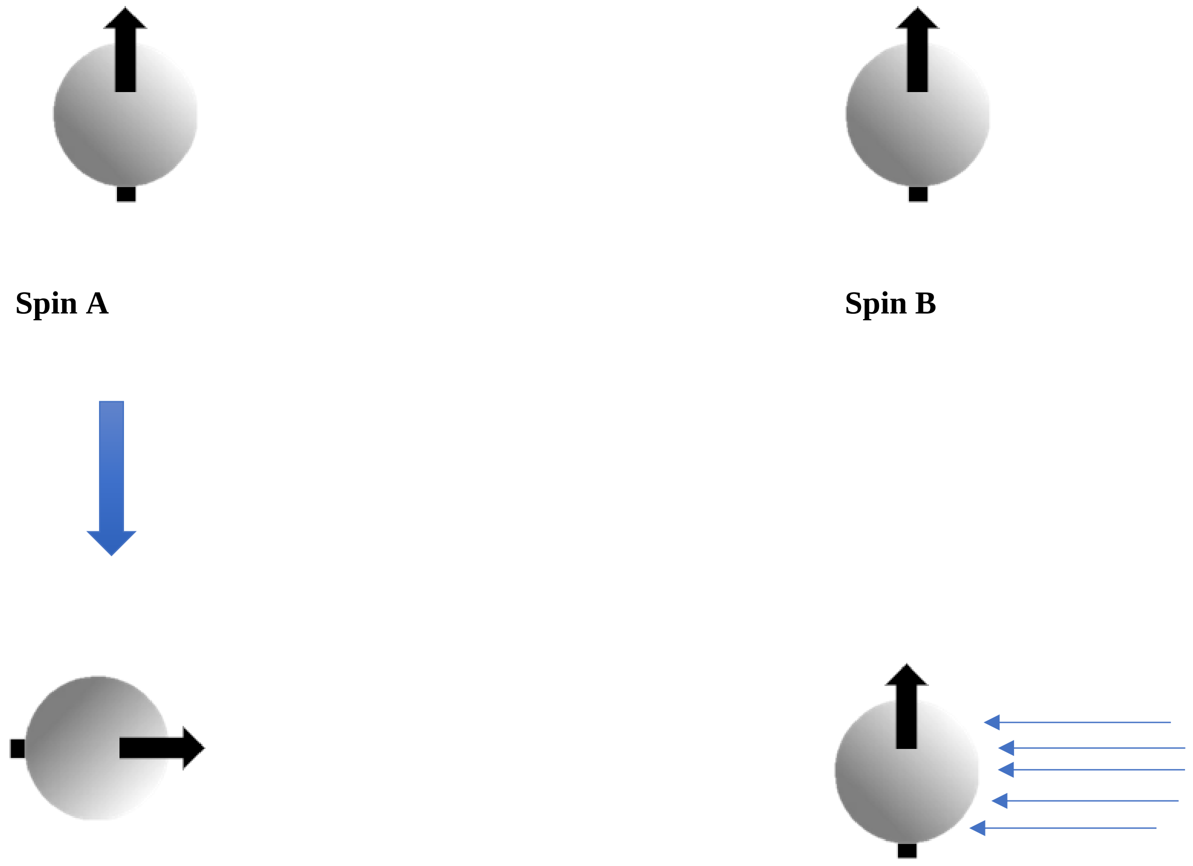
This phenomenon has important implications for quantum computing.

We know that with n qubits, we need 2^n numbers to fully describe the quantum state. But that information is not really accessible because the measurement would disrupt the quantum superposition. So, to use the power of quantum information, we need to design quantum algorithms which explore the existence of huge amounts of information stored in the quantum superposition, but at the end of the calculation, leave the system in one of the basis states which we are always able to measure with certainty.

QUANTUM ENTANGLEMENT

Quantum entanglement is a physical phenomenon that occurs when a pair or group of particles interact in a way such that the quantum state of each particle of the pair or group cannot be described independently of the state of the other, no matter whatever be the distance between them.

To illustrate the concept of quantum entanglement, we consider 2 electrons each **having spin (spin A and spin B) in the |1> state. Then we create a superposition of |0> and |1> spin states for the first electron so that its spin becomes, 1√2|0> + 1√2|1> in the superimposed state.**



1√2|0> + 1√2|1>

Now, if we irradiate the second electron with light having frequency it would respond to if spin A was in |1 > state, we observe that spin B flips and does not flip simultaneously. This occurs because Spin A is not in |1> state rather in superposition of |0> and |1> state.

The resulting state of the two electron spins is represented by:

$$|\Psi> \;=\; 1\sqrt{2}\;|10> \;+\; 1\sqrt{2}\;|01>$$

This state is referred to as **Entangled state** which is a peculiar state in which we do not have knowledge about the direction of spin of either of the electrons, but both these spins are so related that if we isolate the two spins, they always point in opposite directions. (no matter how far apart we keep them.)

This property of entanglement is unique to quantum systems which differentiates them from their classical counterparts.

Thus, we can generate entangled states in a quantum computer and with the increasing number of qubits, the more of these entangled states the quantum computer becomes capable of coding. Gaining access to these entangled quantum states is the key to exploiting the exponentially large computational power of quantum computers.

QUANTUM LOGIC AND QUANTUM ALGORITHMS

Quantum Logic Gates

In classical computers we implement logic operations by using a sequence of NAND Gates on pairs of bits and NOT operations on individual bits.

However, there is a significant difference between quantum logic operations and classical logic operations. Unlike a classical logic circuit, Quantum logic circuits must have a one-to-one relationship between the input and output. What this means is that given the output, we can deduce a unique input. Quantum circuits maintain the rules of reversible logic, but are different from reversible logic of classical systems owing to their unique property of superposition.

This happens because quantum mechanics imposes very strict requirements. A quantum system can never lose information over time and it must always be possible to reconstruct the past. Hence all classical operations are not allowed in quantum systems.

The C-NOT Operator

In quantum mechanics C-NOT or Controlled- NOT operator, is an operator which operates on a quantum register consisting of 2 qubits. The CNOT gate flips the second qubit (target qubit, here B) if and only if the first qubit (control qubit, here A) is |1>. The CNOT gate is capable of implementing any logic function on a quantum computer.

BEFORE		AFTER	
A	B	A	A ⊕ B
|0>	|0>	|0>	|0>
|0>	|1>	|0>	|1>
|1>	|0>	|1>	|1>
|1>	|1>	|1>	|0>

More generally, the inputs are allowed to be a linear superposition of |0> and |1>.

The CNOT gate transforms the quantum state:

|Ψ> = a|00> + b|01> + c|10> + d|11> into:

|Ψ> = a|00> + b|01> + c|11> + d|10>

Apart from C-NOT, there are many other logic gates like: Pauli -X- Gate, Pauli - Y- Gate, Phase-shift Gate, Square root of Swap Gate, etc. which are used in creating interactions among qubits and in the development of quantum algorithms.

Quantum Algorithm

The power of quantum computers arises from quantum parallelism which comes from the ability of a quantum memory register to exist in a superposition of basis states. This means that instead of processing each input one by one, quantum mechanics allows us to perform operations on a super position of all the possible simultaneously.

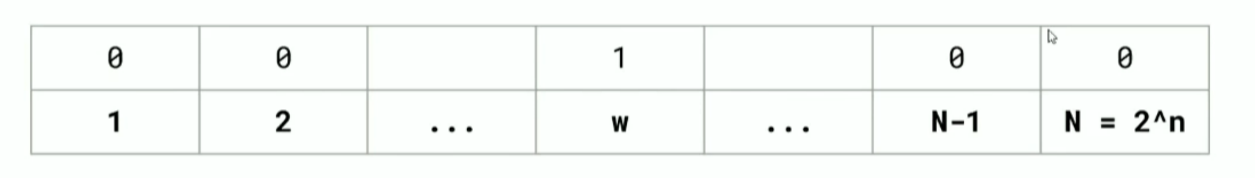
In quantum computing, a quantum algorithm is an algorithm which runs on a realistic model of quantum computation. Although classical algorithms can also be performed on a quantum computer, the term quantum algorithm is usually used for those algorithms which use some essential feature of quantum computation such as quantum superposition or quantum entanglement.

A Simple Illustration using Grover’s Search Algorithm.

The Grover algorithm uses qubits in superposition in parallel universes to make its computation. It can find with high probability the unique input to a particular output. It can perform searches on a quantum computer with significant reduction in the number of steps required to achieve the output compared to a classical computer.

We consider a problem, where we have N inputs and we wish to find the output corresponding to a particular input. If we do an unstructured search using a classical computer, it would take N steps(in the worst case) to solve the problem. This would turn time consuming when N is very large.

We use an Oracle function to assign a value 1 to our desired input w, and assign a value 0 to all other inputs.



0	0		1		0	0
1	2	...	w	...	N-1	N = 2^n

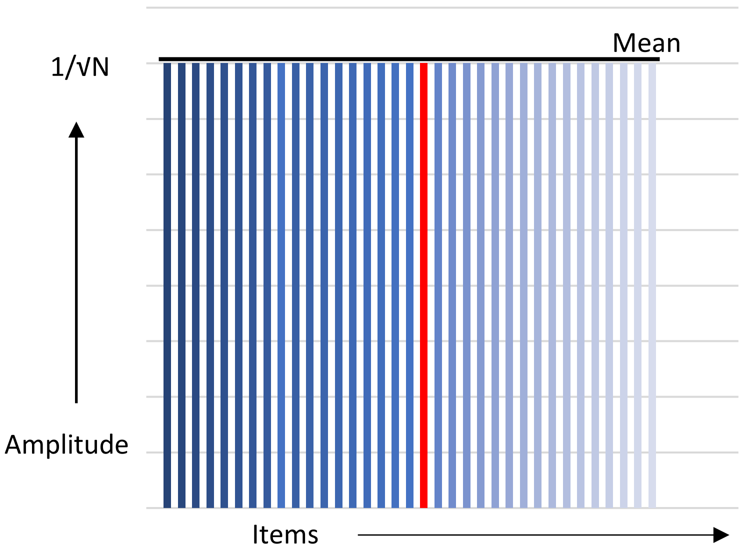
A Grover’s search begins with superposition of the n qubits.

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

Where |s> denotes the uniform superposition over all states.

This pictorially results into a curve having inputs along the x axis, and the amplitude of output corresponding to each input along the y axis.

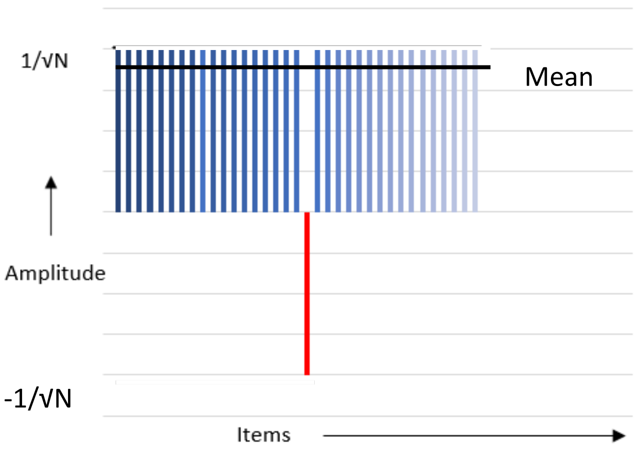
By symmetry, at t=0, all amplitudes will be equal to A, such that the sum of N times the square of A is 1. i.e., A= 1/√N



Now we apply a global operation which negates the amplitude corresponding to our desired input while keeping the remaining amplitudes unchanged. Mathematically,

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$

So graphically we have:

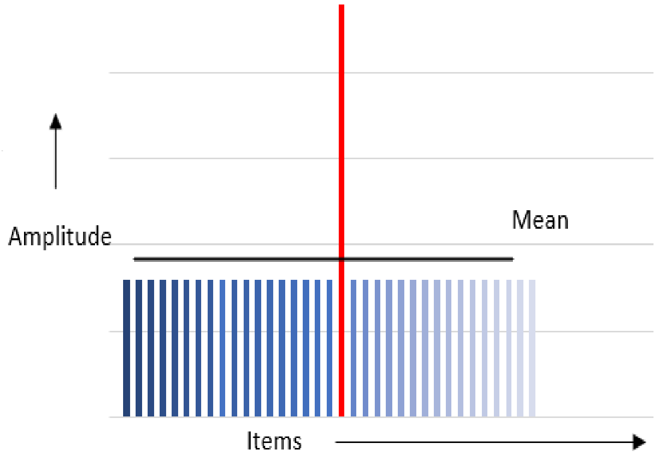


Next, we apply a phase change to the above system about the new mean. Mathematically,

$$U_s = 2|s\rangle\langle s| - 1$$

$$|\psi_{t+1}\rangle = U_s U_f |\psi_t\rangle$$

So, our graph looks like:



As we can see, the amplitude corresponding to desired value has been amplified.

On iterating through the above 2 steps again and again for a total of √N times we will very high probability (around 95%) of the amplitude corresponding to the desired input.

Thus, the quantum computer can extract a solution to such a problem in √N steps, while a classical computer would take a total of N steps (in the worst case) to achieve the same output.

QUANTUM SUPREMACY AND CHALLENGES TO QUANTUM COMPUTING

Quantum supremacy refers to quantum computers being able to solve a problem that a classical computer cannot. It tries to show that experimental quantum computers can surpass the best supercomputers in the world.

To do this a circuit is chosen and run on a quantum computer. The output is simulated on a classical computer. The complexity of the circuit is increased gradually till a state is attained when the classical computer fails to keep up with the quantum computer.

On September 20, 2019, the Financial Times reported that "Google claims to have reached quantum supremacy with an array of 54 qubits out of which 53 were functional, which were used to perform a series of operations in 200 seconds that would take a supercomputer about 10,000 years to complete"

Quantum supremacy gives an idea about the exponential power of a quantum computer over a classical computer. However, this does not been the quantum computer is universally faster. This is because the quantum computers are way ahead of classical computers only in tasks that require a very large database, like solving optimization problems at various levels. Classical computers are still better at some tasks than quantum computers (like email, spreadsheets and desktop publishing to name a few). The intent of quantum computers is to be a different tool to solve different problems, not to replace classical computers. Moreover, a quantum computer is a fragile system. Any kind of vibration impacts the atoms and causes decoherence. Quantum computers are exceedingly difficult to engineer, build and program. As a result, they are crippled by errors in the form of noise, faults and loss of quantum coherence Many of the quantum computing technologies around the world operate at around 0.1 Kelvin. Which requires special cryogenic refrigeration techniques. Hence right now there is no scope for commercialization of quantum computers at large scale. Active research on dedicated quantum hardware, and algorithms is in its way. As a technology, quantum computing is still in early stages. We have a long way to go to revolutionize present technologies with quantum computing and the world is hopeful.

REFERENCES

- UNSW YouTube Videos on Computing
  https://www.youtube.com/playlist?list=PLHSIfioizVW2uC27IFkHlSc-NgvZjBliZ
- IBM Research on Quantum Computing
  https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/
- Wikipedia -
  https://en.wikipedia.org/wiki/Quantum_computing#:~:text=Quantum%20computing%20is%20the%20use,are%20known%20as%20quantum%20computers.
- Quantum Computing for Everyone – Chris Bernhardt
- Quantum Computation and Quantum Information – Textbook by Isaac Chuang and Michael Nielsen