QUANTUM COMPUTING: QUANTUM ERA WITH PHYSICS AND COMPUTER SCIENCE IN ACTION TO INNOVATE HEALTHCARE

Rohit Raj
Department of Computer Science Technology
MIT-WPU, PUNE, MAHARASTRA, INDIA
Email-rohitraj1998@gmail.com

Dr. Yogesh R. Kulkarni
Department of Computer Science Technology
MIT-WPU, PUNE, MAHARASTRA, INDIA
Email- yogesh.kulkarni@mitwpu.edu.in

Dr. Kishor R. Kolhe
Department of Computer Science Technology
MIT-WPU, PUNE, MAHARASTRA, INDIA
Email- kishor.kolhe@mitwpu.edu.in

***Abstract*--This paper presents the development of Quantum Computing and its application. It's totally a new branch and new field of Research in Computer Science. Companies like Microsoft, Google, Intel, IBM all are investing in billions for quantum development as to be Quantum Supremacy. There are several algorithms which exploit the advantage of Quantum Computing like Shor's Algorithm (efficiently factor large composite number, breaking RSA Encryption) in 1994, Grover's Algorithm (searching of an unordered list in $O(\sqrt{n})$ time) in 1996. Many believed there is exponential speedup in simulating Quantum Mechanical System that's why it is the matter of contention of 21st century. Quantum Computing can calculate problems within a moment for which the classical computer will take years.**

Keywords -Quantum Computing, Quantum Supremacy, Shor's Algorithm, Classical Computers, Grover's Algorithm.

1.1 INTRODUCTION

Quantum computing is the advance method in making parallel calculations, i.e. physics that governs subatomic particles to exchange with the most simplistic transistors in classical computers.

Quantum computers operate using qubits, computing units which can be true, false or any value between, instead of the bits in traditional computers which are either true or false, one or zero. The qubit's property to live in the in-between state is called superposition which adds a powerful capability to the computing equation, making quantum computers superior for some kinds of math.

Google achieved quantum supremacy on 23rd Oct-2019. Quantum Processor was able to perform complex mathematical calculation in 3 min 20 sec the same calculation would have taken the most powerful supercomputer nearly 10,000 years. So, it proved that Quantum speed is achievable in a real-world system and in future quantum computer will replace the so-called today's classical and supercomputers.

Google and NASA had carried many research and experiment and concluded that Quantum Computer can be at least 100 million faster than today's supercomputer also its speed on which it, got the name works with Advanced AI with ML and Deep Learning which can change the world more than the discovery of wheel, fire and electricity combined.

1.2 LITERATURE REVIEW

Existing problem

If the goal was to make 1 qbit work, it would have been done till now, but the trick is to make multiple qbit work because it triggers the creation of processing power.

Classical bits store information as a zero or one & a Quantum bit can be both zero and one at the same time.

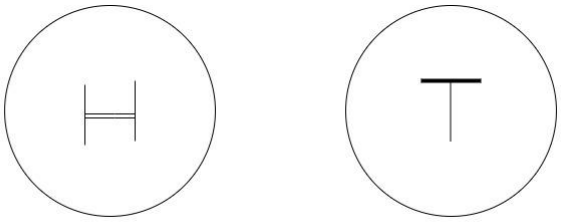


Figure 1: In classical bit it will be either of any of 2 like in tossing of coin it will be either Heads or Tails.

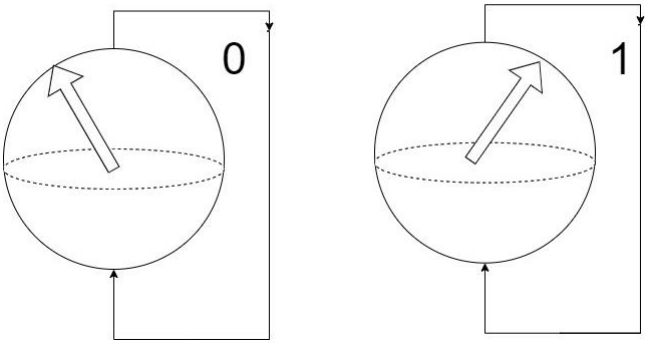


Figure 2: In Quantum bit it will be both for an example 0 and 1 at the same time. If you have 2 Quantum bits, then are four possible states that we can put in superposition states.

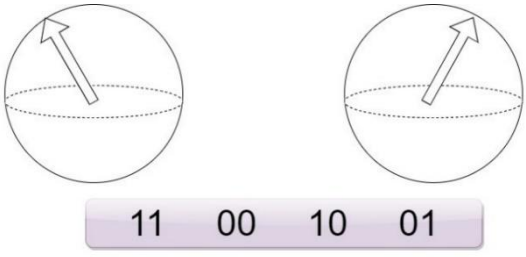


Figure 3: Four possible outcomes

If you have 3 Quantum bits, then are eight possible states that we can put in superposition states.

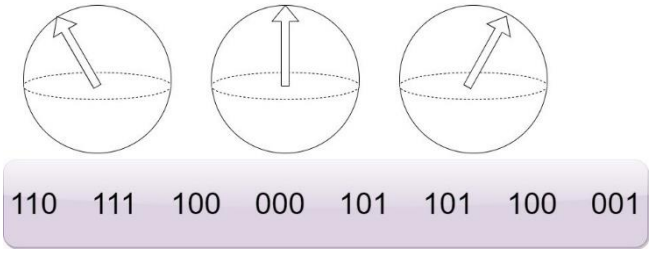


Figure 4: Eight possible outcomes

If you have four quantum qbits there are 16 possible outcomes.

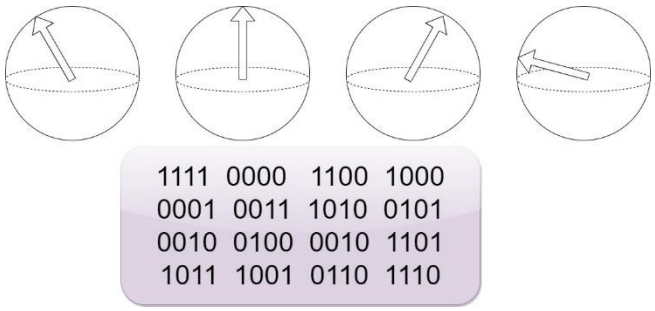


Figure 5: Sixteen possible outcomes

It grows exponentially with more qbits processing power growth exponentially as with only decay because only with 300 cubic quantum computer we could perform more calculation at once then there are atoms in the observable universe and it's all due to another quantum phenomena called Quantum Entanglement. Two separate particles can be at the opposite ends of our galaxy and still be entangled meaning that changing one of them would immediately change the other without any physical connection. Einstein has called this phenomenon "Outright Spooky", and it truly is but it's how quantum computer will be able to work the trick is to entangle qbits to make them work together and beat them we can exponentially grow computing power with every added qbit.

Right now, people don't even have the language to fully describe how a quantum computer works. But it's easy to understand that superior speed and processing capabilities above quantum computer have the possibility to change literally every aspect of our life but how close are we to make it a reality.

Proposed solution

One of the famous drug manufacturers company Turbine AI have used a simulation platform which would help them lower the astonishing 96% of failure rate in clinical trials. They believe that the major scientific leap enabled by Quantum Computing in their field would be the accurate simulation of protein folding because the working of these little nanomachines behaviour is crucially important for understanding for working of cells and many more mystery in Biology which is still in development stages would be essentially unlocked by having an ability using the power of quantum computers to simulate these tiny systems that is these nanomachines living in ourselves.

We all can tell we're still far away from it but Google achieving quantum supremacy was a major turning point in the development in reaching Quantum Supremacy. In future they will look back at this moment as we look at Wright Brothers first flight but for now even Google says that first Quantum Application could be a decade away and quantum computing in healthcare could be an even more further if we consider how healthcare systems are not obviously slow adopters of innovative technologies and even if there will be ready for destruction, Quantum Computer won't exactly drive the cost down which is the major problem for most healthcare system around the world, but Google demonstration gave us the hope that quantum computing is in fact possible and eventually it will revolutionise medicine.

1.3 AIM AND OBJECTIVES

Today's computer so called classical or supercomputer works on classical 'bits' which is 0 or 1 at the particular time, whereas 'Quantum bit' is both 0 and 1 at the same time.

Classical computers are based on mechanical structure designed by the language of mathematics while quantum computers leverage the strange rules of the quantum world. They are dependent on two phenomena which happened beyond the atomic level (1) Superposition and (2) Quantum Entanglement.

Whenever people heard the word 'Quantum Computing' they mostly think of 'Superposition' and classical computer work with bits which can be a 0 or 1 but a Q-bit or Quantum bit can we both zero and one at the same time and observing a qubit make it overlapping into a fixed position no one knows why that occurs but to solution of this mystery will be solved by the Quantum Computers itself.

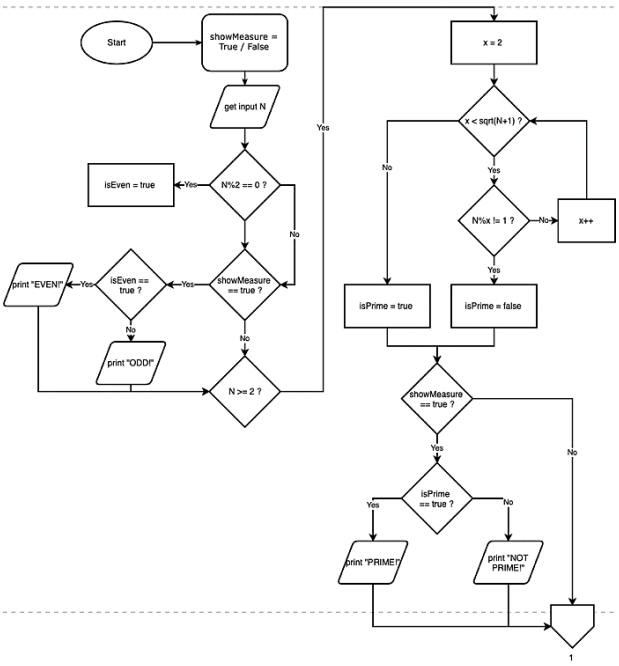
Problem Statement

For example, A bit having a defined value as 0 or 1, a Q-bit has the probability of being either. By flipping a coin enough times as zero or one is an example of bit, but Q-bit has the probability of being either. Flip the coin enough times and the probability of heads and tails will become clear in the same way and continuous measuring a Q-bit will reveal the probability which is the position because the universe works that way too. We can easily relate nature as a quantum. We have been searching for work in probabilities which they can only be accurately simulated on the quantum computers. Quantum computer working in with synergy with quantum mechanics of universe and they leverage its capabilities. Richard Feynman one of the biggest physicists known for his work in the path of integral formulation of quantum mechanics stated the idea as- "Nature isn't classical, dammit and if you want to make a simulation of nature, you will better make it, Quantum Mechanical".

1.4 METHODOLOGY

Till now there are 2 famous equations which have come forward (1) Shor's Algorithm and (2) Grover's Algorithm so here is a bit of summary of both the equation.

A. Shor's Algorithm Flowchart



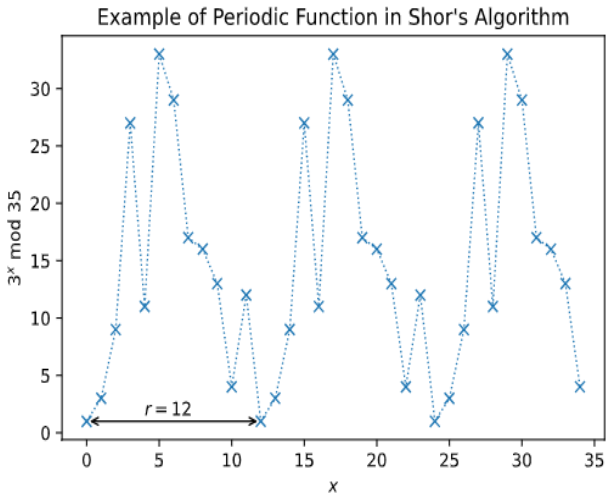
Shor's algorithm is famous for factoring integers in polynomial time. Since the best-known classical algorithm requires super polynomial time to factor the product of two primes, the widely used cryptosystem, RSA, relies on factoring being impossible for large enough integers.

$$f(x) = a^x \bmod N$$

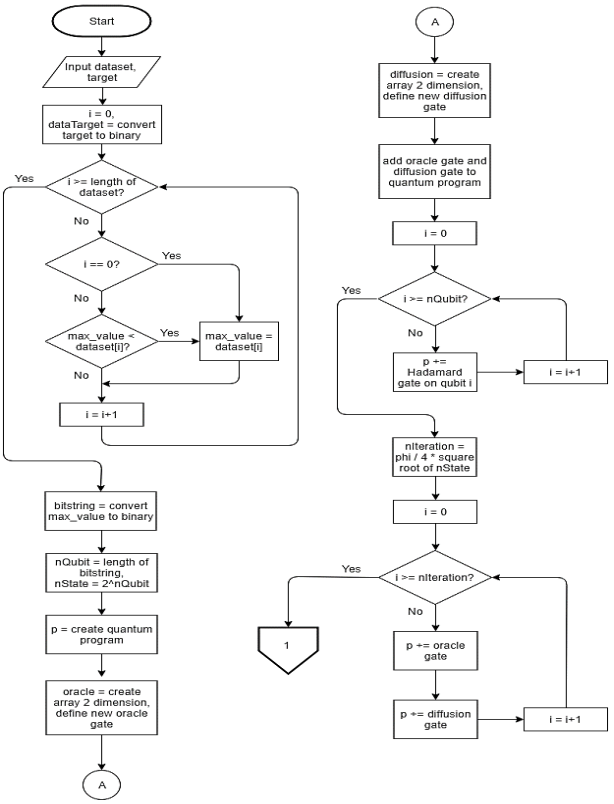
where a and N are positive integers, a is less than N, and they have no common factors. The period, or order (r), is the smallest (non-zero) integer such that:

$$a^r \bmod N = 1$$

We can see an example of this function plotted on the graph below. Note that the lines between points are to help see the periodicity and do not represent the intermediate values between the x-markers.

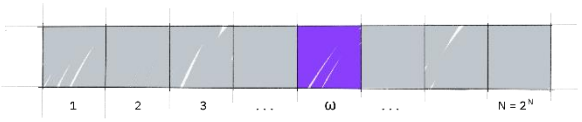


B. Grover's Algorithm Flowchart



This algorithm can speed up an unstructured search problem quadratically, but its uses extend beyond that; it can serve as a general trick or subroutine to obtain quadratic run time improvements for a variety of other algorithms. This is called the amplitude amplification trick.

Unstructured Search: Suppose you are given a large list of N items. Among these items there is one item with a unique property that we wish to locate; we will call this one the winner ω. Think of each item in the list as a box of a particular colour. Say all items in the list are Gray except the winner ω, which is purple.



To find the purple box -- the marked item -- using classical computation, one would have to check on average N/2 of these boxes, and in the worst case, all N of them. On a quantum computer, however, we can find the marked item in roughly $\sqrt{N}$steps with Grover's amplitude amplification trick. A quadratic speedup is indeed a substantial time-saver for finding marked items in long lists. Additionally, the algorithm does not use the list's internal structure, which makes it generic; therefore, it immediately provides a quadratic quantum speed-up for many classical problems.

For the examples database is comprised of all the possible computational basis states our qubits can be in. For example, if we have 3 qubits, our list is the states $|000\rangle$, $|001\rangle$, $|111\rangle|000\rangle$, $|001\rangle\ldots|111\rangle$ (i.e., the states $|0\rangle\rightarrow|7\rangle|0\rangle\rightarrow|7\rangle$). Grover's algorithm solves oracles that add a negative phase to the solution states. I.e., for any state $|x\rangle|x\rangle$ in the computational basis:

$$U\omega|x\rangle=\begin{cases} |x\rangle \; if \; x = w \\ -|x\rangle \; if \; x = w \end{cases}$$

This oracle will be a diagonal matrix, where the entry that correspond to the marked item will have a negative phase. For example, if we have three qubits and ω=101, our oracle will have the matrix:

$$\begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

What makes Grover's algorithm so powerful is how easy it is to convert a problem to an oracle of this form. There are many computational problems in which it's difficult to *find* a solution, but relatively easy to *verify* a solution. For example, we can easily verify a solution to a sudoku by checking all the rules are satisfied. For these problems, we can create a function f that takes a proposed solution xx and returns f(x)=0 if x is not a solution ($x \neq \omega$) and f(x)=1 for a valid solution (x=w)

1.5 RESULTANDANALYSIS

Let's see how a Quantum Computer can help in a Patient's Medical Journey:

1) **Sequencing DNA**:

Sequencing DNA at full speed even through today it's possible to afford the complete Genome Sequencing and its cost are down to an affordable level but in future genome sequencing will be like blood or urine test and Quantum Computers able to analyse the vast amount of data & Quantum Computing can ensure faster sequencing & more comprehensive analysis comparing patients result with millions of other patients with similar lifestyle and health parameters and it will be able to make a reliable predictions about what might go wrong with the patient later and how to tackle that in present to prevent it. Quantum computer can finally help on crack the human genome its impact on health and disease and take out guesswork from personalise medicine for ensuring better healthcare for everyone.

2) Making patient's truly the point of care:

Quantum Computer can make another promise for digital health or in reality we already have massive amount of health data at the disposal we had smartphone and health sensor and portable diagnostic devices which keeps us informed about our own health and disease management but Quantum Computing will be able to make sense of astronical data sets and tracking patient help on the go connected sensor system might even render physical hospital useless and truly make patients the point of care they would get diagnosis and treatment wherever they are.

3) Arriving at the perfect Decision Support System:

We have almost passed those eras when the accumulated knowledge of medical professionals could reside in one head and it's just too much when there are almost 31,000,000 medical studies with half million more coming out every year. IBM tried to overcome this problem when they created the first supercomputer and its algorithm from IBM Watson to shift through millions of studied in second, but quantum computer could take that to whole new level and even add some more extra skills. These computers could not just use our entire lexical empirical knowledge in real time, but they could provide the ultimate decision support for doctor. They could skim through all the studies, clinical trials and textbook at once. They could find correlations and causation that the human eye would never find, and they could find diagnosis or treatment options that humans could have never figured out by themselves.

4) **Drug Design:**

This is where the Quantum Computers capabilities are best used for. The Road Design would not just leverage the speed in processing power of a quantum computer but the very nature of Quantum Computing because the way how electron of the molecules of drugs interacts with the human body, it works by the same principle as Quantum Mechanics, simulating Quantum Phenomena on Quantum computers can lead to much faster and much more precise results as by doing all those classical computers seems primitive compared to that number.

5) Clinical Trials:

Quantum Computing could lead to an era of and in silico clinical trial as well as in silico trials means that no humans, animals or not even a single cell is required for testing a particular therapy of drugs. It's human way and theoretically could be the fastest and more effective path in any viable trials. Today completely simulated clinical trials are not feasible with current technologies and understanding of biology yet but with quantum computing virtual humans can undergo trials and have new drugs reaching market within week from their discovery.

6) Creating The Safest Medical Data System:

Even one of the biggest concern about quantum computer is safety even the dumbest Quantum Computer could easily crack the safest encryptions on classical computer qubits could simply overpower any security, so our medical records could easily be exposed to, right... not exactly, what many people forget that while Quantum Computing could easily crack traditional encryption but they will also be used for to leverage quantum uncertainty to create encryptions and quantum security is literally unbreakable. Hackers would have to break the laws of quantum physics to gain access to our health record. The biggest challenge that lies ahead is not whether being health care it will be able to understand how quantum computer work because no offence 99% of us never will but rather we will stop caring about our health when we will be taken care by Quantum Computer, what if we must prepare for word where our well-being is neither healthy or diseased, but it has a probability of being either or both.

1.6 CONCLUSION

Quantum computing will revolutionize the Computing technique in every domain because it will have potential to create and analyse the data with advance AI and ML technique but still everything is theoretical. However, we must wait till next decade which can be used in real life, so this is rather a science fiction till now. Also, another question arises with quantum computing is that the resources

are limited to very few people who can understand its workings completely because one with the knowledge of Quantum Mechanics can only operate it.

1.7 REFERENCES

1) Quantum Computing History and Background

https://docs.microsoft.com/en-us/azure/quantum/concepts-overview

2) ScienceDaily: Quantum Computer

https://www.sciencedaily.com/terms/quantum_computer.htm

3) Born M. The Born-Einstein Letters. London: Walker; 1971.

4) Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2018 Symposium.

https://www.ncbi.nlm.nih.gov/books/NBK538701/

5) Feynman RP. Simulating physics with computers. International Journal of Theoretical Physics. 1982;21(6-7):467–488.

6) Ladd TD, Jelezko F, Laflamme R, Nakamura Y, Monroe C, O'Brien JL. Quantum computers. Nature. 2010;464(7285):45–53.

7) Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science; 1994. pp. 124–134

8) What Can Quantum Computing Do to Healthcare?

https://medicalfuturist.com/quantum-computing-in-healthcare/

9) Shor's Algorithm

https://qiskit.org/textbook/ch-algorithms/shor.html