THEORIZING THE BASIC FRAMEWORK OF QUANTUM COMPUTING INCLUDING THE CAPABILITIES, LIMITATIONS AND APPLICATION IN MARITIME INDUSTRY

Sudhanshu Sagar[a] and Ashutosh Ranjan[b]

[a]Tolani Maritime Institute, Pune, suddzsagar017@gmail.com

[b]Tolani Maritime Institute, Pune, ashutoshranjan.025@gmail.com

Abstract: Quantum computing can be understood by learning the quantum laws of physics by means of which great processing power can be achieved and greater capacity is developed to achieve several states and these together help in accomplishing tasks in terms of parallel attainable combinations. The advantages from the quantum physics atoms and nuclei properties are definite, as the quantum physics laws and quantum computing are permitted by these properties to work mutually as quantum bits are known as qubits, to be the processor or the memory instead of the bits in the classical computers.

KEYWORDS: Qubit, Entanglement, Superposition, Shor's Algorithm, Bloch Sphere

1. **Introduction**

It was the eccentric theories of quantum mechanics, put forward in the 20th Century, of which the quantum computing is now what it is. The concept of using quantum entities to process data and solve complex problems, much like a classical computer, can be traced back to the 1980s.

1.1. History[1]

Quantum computing is still very much in its nascent stage. It's going to take time until when we will see a quantum computer on our desks or in our palms. But advances in this new technology are occurring frequently, and no chronological record can ever be complete. Most of the concepts were put down in the 20th century.

In 1980, Paul Benioff, a US scientist, proposed an idea of a computer that would work on the principles of the quantum mechanics principles. His idea was based on Alan Turing's famous paper of 1936 "On Computable Numbers".

The next year, an American theoretical physicist, Richard Feynman proved that it was impossible to simulate quantum systems on a classical computer.

In 1985, David Deutsch, a physicist, published a paper describing the world's first quantum computer. The mathematical concepts on which a quantum Turing machine, one which could model a quantum system.

It was in the year 1994 when the race to create a quantum computer really took on. This was due to a mathematician of the Bell Labs, Peter Shor, who proposed an algorithm to factorize large integers known as Shor's algorithm. This is implied on cryptographic codes for security. A quantum computer with a sufficient number of qubits can do it in a few minutes whereas a classical computer would take the time that is longer than the age of the Universe.

Next year, Christopher Monroe and David Wineland of NIST demonstrated the first quantum logic gate, the C-NOT gate using trapped ions.

In the year 1998, Oxford researchers did an experimental demonstration of a 2-qubit Nuclear Magnetic Resonance Machine (NMR Machine) to solve computer problems twice as fast as a classical computer followed by a 3-qubit NMR quantum computer later that year. The first working quantum computer was developed by the Technical University of Munich in 2000 using a 5-qubit NMR computer.

The year 2001 is a landmark in the history of quantum computers. It was the year in which a team from IBM Almaden Research Centre in California succeeded in factorizing the integer 15 into 5 and 3. It was achieved using the 7-qubit quantum computer when pulsed with electromagnetic waves and monitored by NMR.

A 128, 512, 1152-qubit quantum computer was created in 2007, 2012 and 2015 respectively by D-Wave.
Worlds' first quantum computer was sold by D-Wave $10,000,000 in 2011 which was an adiabatic quantum computer named D-Wave One.
A Chinese team calculated factors of 143 using 7 qubits in the year 2011.
In 2012, a 512 qubit computer was bought by Google and stored at NASA's Ames Research Centre.
In 2017, D-Wave created a 2048 qubit quantum computer named D-Wave 2000Q.
And IBM made a 50 qubit quantum computer that can maintain its state for 90 microseconds.
Microsoft reveals q#, a quantum computer programming language.

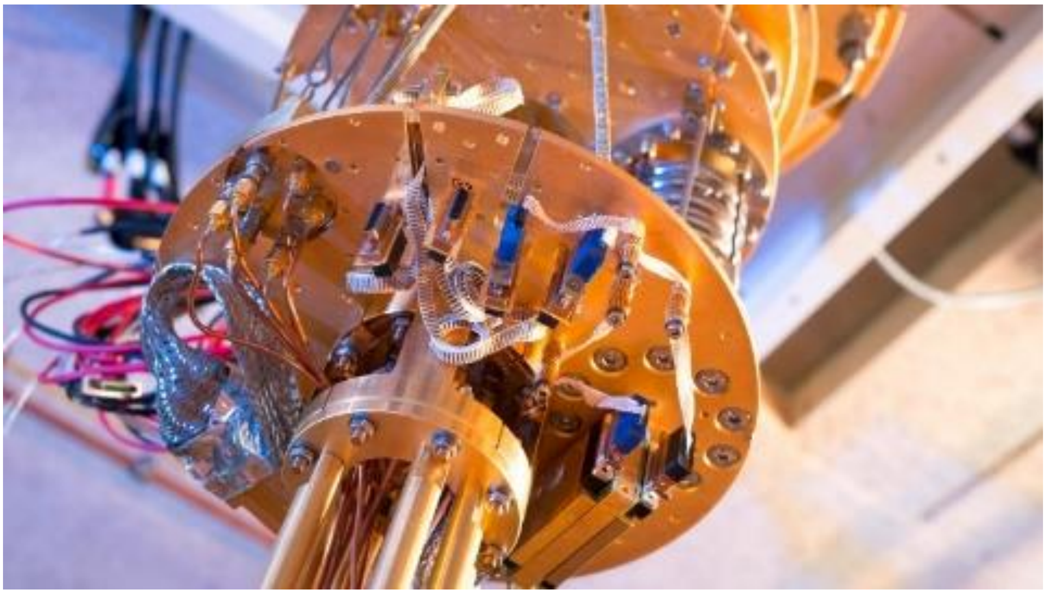

Fig. 1: A Quantum Computer at Microsoft [5]

2. Main Body

2.1 Principle

Quantum computing is a big paradigm shift. It's a new and big form of computing that goes exponentially beyond the best and the most powerful supercomputers today. Its grounded in the principles of quantum mechanics which underlies the fundamental theories of nature at atomic and subatomic scale. So with a quantum computer, it's quantum mechanics that govern how we store the information and how we process it. Today computers are based on transistors which are like a switch which support only two states like a light switch and with two positions either on or off that translates to binary 1'and 0's that we ultimately program in. As we need more information with a transistor based machine and more compute power one needs to add more 1's and 0's and more transistors in. And of course, we are striving to fit as many transistors as we can.

In quantum computer we deal with very small subatomic particles which are governed by laws of quantum mechanics, so we need a totally different approach to computing and programming. We actually have to learn how to program and develop these new applications and algorithms.

2.2. Qubit

One has to have qubits that have to work in such a way that has to have quantum mechanics. Artificial atoms are made which behave quantum mechanically. It's made out of superconducting Josephson Junction coupled to a microwave resonator. Its cooled to 0.015 K. qubits are controlled via microwaves.

A pure qubit state is a linear superposition of the basis states. This means that the qubit can be represented as a linear combination of $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \theta|0\rangle + \varphi|1\rangle,$$

where θ and φ are the probability amplitudes and can, in general, be both complex numbers.

When we measure this qubit in the standard basis, the probability of outcome $|0\rangle$ is $|\theta|^2$ and the probability of outcome $|1\rangle$ is $|\varphi|^2$. Since the absolute squares of the amplitude equate to probabilities, it follows that θ and φ must be constrained by the equation:

$$|\theta|^2 + |\varphi|^2 = 1$$

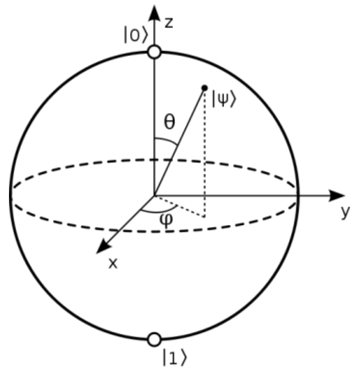

Fig.2: A Bloch Sphere (representation of a qubit) [6]

2.3. Working

We're operating on a small scale in terms of information but ultimately the quantum computer is going to fit in a large dilutional refrigerator. Indeed the way we hold and process information operates differently. In the transistor model, we have this on-off switch but a quantum computer is more like a dimmer switch. One can take on both zero and one states simultaneously which is called superposition.

In binary today, we take 4 light switches and work through all zeroes and ones all the possible string combinations we can get 16 values that are 2^4 possible states but that combination of zeroes and ones can be operated in one string at a time. In quantum state let's take 4 qubits instead of 4 bits. Now, these 4 qubits, in fact, store all of those 16 states at once in 4 bits. It's obvious why the number of qubits matter. If one has 1 qubit, one can be in 2 states in the moment and when one has more qubits one can be in a superposition of 2^n states.

Another important factor is an error rate. It is to be controlled what is going on in the qubits. Getting high error rates won't really solve the problem. So, a new method called quantum volume is used. Higher computational power is acquired but not if one has really high error rates. So, to be really efficient it must have both, i.e., really low error rates and high computation.

2.4 Superposition

Superposition is when two waves overlap and interact. Sometimes they have to form bigger waves, and sometimes they cancel out each other, and often it's the combination of the both.

Confusingly, in the quantum world superposition can mean something entirely different. At the quantum scale, particles can also be thought of as waves. Particles can exist in different states, for example, they can be in different positions, have different energies or be moving at different speeds. But instead of thinking about a particle being in one state or changing between a variety of states, particles are thought of as existing across all possible states at the same time. It's like lots of waves overlapping each other. This situation is known as a superposition of states. In brief, it means that a particle can be in two states at once. Superposition is like a limbo between basic states. When we observe the computation and look at it from the perspective of these basic states it must choose one collapsing the wave function and reveal a single state.

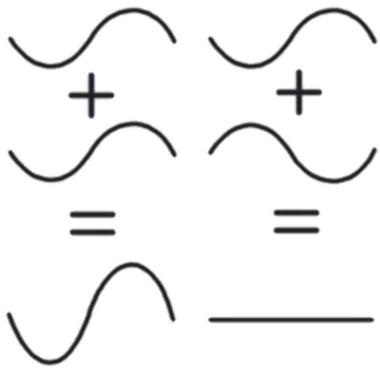

Fig. 1: Superposition of Waves

2.5 Spooky Action

In quantum physics, entangled particles are as the name defines connected, in such a way that actions performed on one affect the other. This phenomenon is what Albert Einstein called "spooky action at a distance". The quantum physics rules for a photon says that an unobserved photon exists in all states simultaneously but, when observed or measured, exhibits the only state. Entanglement occurs when a pair of particles interact physically. A laser beam fired through a certain type of crystal can cause individual photons to split up into entangled photons. The photons can be separated by no matter what distance, the transfer of state is observed instantaneously.

2.6 Topological Qubit [2]

A topological quantum computer is a theoretical quantum computer that employs two-dimensional quasiparticles called anyons, whose world lines pass around one another to form knots in a three-dimensional spacetime (i.e., one temporal plus two spatial dimensions). These knots form the logic gates that make up the computer. Other qubits store information in a volatile state like a painting made of sand. Topological qubits store information in a more stable state like the knot on the string. Whatever happens to the string, the knot remains. The advantage of a quantum computer based on quantum knots over using trapped quantum particles is that the former is much more stable. Small, cumulative perturbations can cause quantum states to decohere and introduce errors in the computation, but such small perturbations do not change the knots' topological properties. This is like the effort required to cut a string and reattach the ends to form a different knot, as opposed to a ball (representing an ordinary quantum particle in four-dimensional spacetime) bumping into a wall. Alexi Kitaev proposed topological quantum computation in 1997. To do so, it is necessary to learn to manipulate the qubit using fundamentally different branch of physics.

2.7 Mathematical Representation

Quantum computation with 2 qubits. It has 4 basic states 00, 10, 01, 11. These are the states that two classical computers can be in but also in infinitely many states formed by superpositions or combinations of these basic states. Each operation of quantum computation is performed by a quantum gate which like a classical gate changes the states that the qubits are in. Let's start a quantum computation in state 00 and then apply a quantum gate. Now the qubits are in a superposition. There is a one-half probability or 50% chance of being 01 and one-half probability of being 10. The particular superposition it is in a result of the quantum gate we chose to apply. Here's one more quantum gate changing the state of the computation. At the end of the quantum computation, we observe or measure the system. We can't see these superpositions. Superposition is like a limbo between basic states. When we observe the computation and look at it from the perspective of these basic states it must choose one collapsing the wave function and reveal a single state. In this case, it collapses to state 01. If the same computation is run repeatedly, the final result will be half the time, 10 one-sixth of the time and 11 one-third of the time.

A vector is a list of numbers and the dimension of that vector is the number of numbers in the list. Actual qubits use negative or even complex numbers. One qubit is represented as a two-dimensional number.

State 0 and 1are represented by:

$$\mathbf{0} = \begin{vmatrix} 1 \\ 0 \end{vmatrix} \qquad \mathbf{1} = \begin{vmatrix} 0 \\ 1 \end{vmatrix}$$

For a two-qubit quantum computer, states can be are represented as:

$$\mathbf{00} = \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \end{vmatrix} \qquad \mathbf{01} = \begin{vmatrix} 0 \\ 1 \\ 0 \\ 0 \end{vmatrix} \qquad \mathbf{10} = \begin{vmatrix} 0 \\ 0 \\ 1 \\ 0 \end{vmatrix} \qquad \mathbf{11} = \begin{vmatrix} 0 \\ 0 \\ 0 \\ 1 \end{vmatrix}$$

A 2-dimensional vector, i.e., a quantum computer with 1 qubit would point to a spot in a 2-dimensional space (in a circle). When we consider a 4 qubit computer, it would point to a spot in 4-dimensional space.

2.8 Quantum Communication [3]

Quantum communication makes use of the property of photon polarization (i.e., the orientation of photon's oscillation). A specific spin can be considered as 0 and opposite spin as 1. Rectilinear and diagonal oscillations are most commonly used.

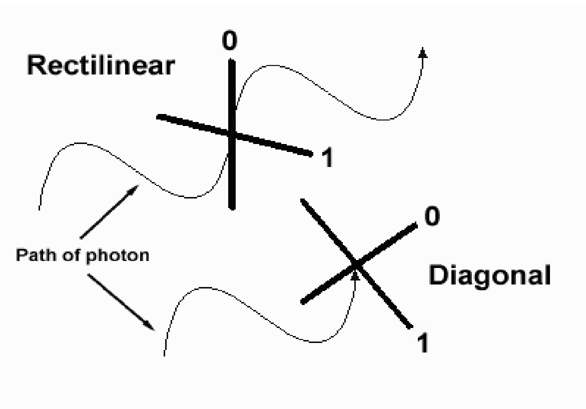

Fig. 2: Rectilinear and Diagonal oscillations are most common polarization [7]

The quantum computer uses the correct filter polarizations i.e., the receiver would use the same polarisation that the information was transmitted in. If rectilinear polarization is used, and if the diagonal polarization was used by the transmitter, completely different result would be received. This method is used to detect the presence of an eavesdropper. If an eavesdropper has intercepted and forwarded the information, level of error would be more. The information would have to be sent again and the algorithm used to transmit the information is sent at last so that receiver would decode it correctly.

2.9 Heating Over Lost Information

According to studies, it is believed that quantum theory does not place any absolute limits on swiftness, consistency or memory capacity of computing machines. For a computer to run extensively fast, its operation must be reversible (i.e., the outputs can be used to deduce the inputs). This is because of the fact that the irreversible computation involves information dropout which is resultant to heat loss, and thus the ability of the system to dissipate heat as it will cause edgy performance of the system. So, it is necessary for the availability of an operation that could deduce the input by judging the output. One can basically understand. The help was available in 1976 by Charles Bennett proved that it is possible to build a universal computer completely with reversible gates, and expressing a program in terms of primitive reversible operations that would not show a significant slowdown. Toffoli gate (invented by Tommaso Toffoli) is subjected to be used.

2.10 Augmentation of Artificial Intelligence

The quantum computer theories have exciting insinuations in the field of artificial intelligence. The thoughts of the artificial intelligence are yet philosophical if it would be able to artificial. People against the topic think that the way of human processing cannot be performed on the Turing's machine, which is the base of the quantum computing.

2.11 Applications Of Quantum Computers In Maritime Sector

Classical computers have allowed us to do amazing things. The internet, our smartphones, space exploration, and another million plus things. But just like the age of typewriters has doomed so will be of the classical computers. This is because of the fact that there are many things the classical computers are really bad at. Sure they can solve small versions of such problems but when the problem starts to get exciting we run out of computing horsepower.

1) Optimization: Quantum computers could be used to hyper-optimize logistics operations across modes of transportation, creating a more seamless flow of goods between maritime, rail, air and ground shipping. They could enable real-time, adaptive mass transit that responds to demand rather than following predetermined routes.
2) Chemistry: With enhancement of processing speed and high computational power quantum computers can be used to analyse instantaneous ship loads and tweak governors to achieve a better fuel combustion efficiency resulting in cleaner emissions. This not only helps with lowering the running costs but also aids the shipping companies to comply with the upcoming more stringent emission regulations.
3) Material Science: Faster simulation and development of advanced material to be used in zones that experience and sustain higher wear and tear with higher time between overhaul. Conventional computers require long duration for simulation which may not always be successful and is required to do the same repeatedly.
4) Navigational advancements: They could be used to optimize marine traffic routes on a national scale and eliminate marine traffic control-based delays. One day, a single quantum computer might even be capable of managing every aspect of a maritime activities at a global and centralised scale. This level of integration would create invaluable efficiencies and usher in an era of highly responsive transportation.
5) Accelerate the development of artificial intelligence: Artificial intelligence is intelligence displayed by machines, in contrast with the natural intelligence displayed by human and other living beings. The traditional problems (or goals) of AI research include reasoning, knowledge, planning, learning, natural language processing, perception and the ability to move and manipulate objects.

It must be noted that a quantum computer cannot always outperform a classical computer but in those in which quantum parallelism is required; examples of which being Shor's algorithm that allows quick factorization of huge numbers.

2.12 Limitations Of Quantum Computers

A Schrodinger's Cat Thought Experiment is what haunts the world of quantum computing, as of now. Consider a cat in the box without the information of if it is dead or alive. Prior to looking in the box, the state of the cat can be either dead or alive. But once the peeked into a solution is to be considered if it is dead or alive. Similarly, a qubit once captured and seen takes its base state, either 0 or 1. So the solution from a quantum computer is basically probability based. The same calculation is done quite a few times until the maximum probability of the solution is observed. The process is called decoherence and the qubit is said to decohere in one of the classical states. This problem is compounded by the fact that even looking at a qubit can cause it to decohere, making the process of obtaining a solution from a quantum computer just as difficult as performing the calculation itself.

3. Conclusion

Quantum computers are still in the early development stage with all the big names working hard and fast on it. Google recently reached quantum supremacy, i.e., out do the classical computers. However, it will take a while before quantum computing becomes a reality in business and personal places, but when it does, the impact is guaranteed be huge. Faster, smarter and better is what it's reliability shall be. Maritime sector is sure to take full advantage of this new era of super computers in secure and greener shipping.

4. Acknowledgement

We would like to thank Tolani Maritime Institute for providing us the opportunity to present a technical paper on such a strong topic that is of great importance and is still scarcely treaded upon . We are glad we are able to grab this opportunity and take full advantage of it.

5. References

Timeline of quantum computing

http://www.wikiwand.com/en/Timeline_of_quantum_computing

Topological Quantum Computer

https://en.wikipedia.org/wiki/Topological_quantum_computer

A Brief History of Quantum Computer

https://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/#7

Quantum Computing Can Reshape Our Physical Infrastructure If We Let It
https://www.forbes.com/sites/ellistalton/2018/11/26/quantum-computing-can-reshape-our-physical-infrastructure-if-we-let-it/#2bf245a99b46

The Microsoft approach to quantum computing
https://cloudblogs.microsoft.com/quantum/2018/06/06/the-microsoft-approach-to-quantum-computing/

Bloch sphere

https://en.wikipedia.org/wiki/Bloch_sphere

Quantum communication will carry the burden of the information security strategy of big powers

http://doc.xueqiu.com/149235cdc46db3fe709d040c.pdf