Quantum Supremacy – A gateway into the mysteries of the Universe

Jisha M. Chacko, Resmi Das

Assistant Professor, Airforce Technical College, Muscat
Assistant Professor, Airforce Technical College, Muscat

Abstract - *Despite the advances made in the field of science and technology there are many mysteries of this universe yet to be tackled. So for this we need to do the computing in a radically different way. Today researchers think of the next big scientific leap that could involve one of the most mysterious forces in nature,* ***Quantum Physics.*** *Entering the realm of quantum physics opens up powerful new possibilities in the shape of quantum computing with processors that could work millions of times faster than the ones we use today. Quantum computers, the new way to harness the nature based on the principles of quantum mechanics gives promising profound leaps in everything from medicine, communications and space travel to an understanding of human consciousness itself. The big tech companies like IBM, Google, and Microsoft are already in the race to build the most powerful quantum computers and Google has recently announced them attaining the Quantum Supremacy by their quantum processor the Sycamore. A brief overview of quantum computing , and the future quantum technology applications have been discussed here with a question for us to think; how this technology could be used or misused going forward.*

***Key Words*: Quantum mechanics, Superposition, quantum entanglement, Noise, quantum algorithms, Quantum Supremacy, decoherence, NISQ era.**

1. INTRODUCTION

Throughout the centuries of scientific development, humans have been driven by the conviction to uncover the mysteries of this universe. The ability to contemplate the world around us brings a constant desire to broader our horizons. This curiosity is necessary for the development of the human race.

"We make our world significant by the courage of our questions and by the depth of our answer"--- **Carl Sagan**

From the wheels to the engines, from abacus to computer, the history of mankind is a record of progress. But with each new discoveries, we were confronted with more challenges. Today we live in an age in which the possibility of crossing a new threshold of scientific knowledge is within arm's reach. This is the dream of **quantum computerization** which involves the principles of quantum mechanics. It may also play a key part in unlocking one of the greatest questions humanity has ever asked. "What is the nature of human consciousness and how does our brain work". There are theories where consciousness is someway related to quantum mechanics.

Unravelling the strange nature of quantum mechanics might even take us beyond inventing new incredible technologies. Quantum mechanics is a field of physics that studies the behavior of the most basic and smallest parts of our universe at the subatomic level. The events happening in this level is very different to the reality we experience in our daily life than even Einstein referred it as "Spooky". Scientists are just trying to understand the weird things happening in this quantum world.

2. WHAT IS QUANTUM COMPUTING?

Our conventional computers work on the basis of the laws of classical physics, specifically by utilizing the flow of electricity. A quantum computer, on the other hand, uses the principles of **quantum mechanics**, the area of physics that studies atomic and subatomic particles, to overcome the limitations of classic computing. At that minuscule scale, many laws of classical physics cease to apply, and the strange and unique laws of quantum physics come into action. Quantum machines promise to surpass even the most capable supercomputers present today. It is based on

the principles of the **superposition** of matter and quantum **entanglement** and uses a different computation method from the traditional one. In theory, they could tackle certain problems that even the most powerful classical supercomputer would take thousands of years to solve, like breaking today's cryptographic codes or simulating the structure of molecules to help discover new drugs and materials.

It was the goal of scientists for nearly four decades to develop such a computer. The idea of quantum computing was first proposed by a Russian German mathematician Yuri Manin in 1980 and a year later in 1981, the eminent physicist and a Nobel Prize winner Richard Feynman wrote:

"Trying to find a computer simulation of physics seems to me to be an excellent program to follow out… Nature isn't classical… and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."

His conviction was that it would be impossible to conduct the simulation of a quantum system with the use of a classical computer. His reasons were based on the laws of nature and he understood that the traditional engineering approach to the problems of computer development would never lead to a revolution. Feynman's lectures from his last years of scientific activities are considered by many scientists as a key moment in the development of quantum computer theory.

2.1 How do Quantum computers work?

We know that our ordinary classical computers use transistors to process information in the form of sequences of various combinations of zeroes and ones. These are known as *bits*, which are like tiny switches that can be either in the ON position, represented by a one or in the OFF position represented by a zero. Every app you use, the website you visit and photograph you take is ultimately made up of millions of these bits in some combinations of zeros and ones. All this does great for certain things but it doesn't reflect the way the universe actually works. In nature, things aren't just ON or OFF. They are uncertain. Even the existing powerful supercomputers are unable to handle these uncertainties. This is where quantum computers comes in, and **qubits** are used instead of bits. These qubits rather than being in the ON (1) /OFF (0) position can also be in a state called Superposition, where they can be both an ON and OFF simultaneously or somewhere on a spectrum between the two. So whereas two traditional bits holds only two values a pair of these so called qubits can hold 4 values .And as the number of qubits increases, a quantum computer becomes exponentially more powerful. ie, 3 qubits hold 8 values, 4 qubits hold 16 and so on. So while a classical computer runs one calculation at a time a computer that uses the quantum effects is possible of multitasking.

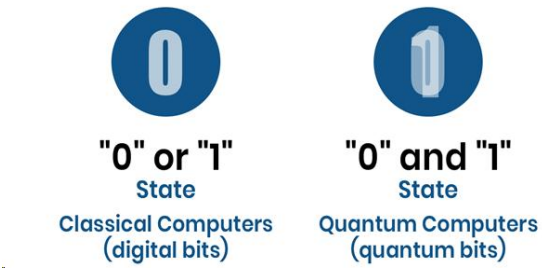

Fig -1: Bits and Qubits

Quantum physicists also explain it in this way. They say that quantum mechanics is based on numbers called amplitudes. Amplitudes can be positive or negative, infact they can be even complex numbers involving the square root -1. So qubit is a bit that has an amplitude for being zero and another amplitude for being one. The goal for

quantum computers is to make sure the amplitudes leading to wrong answers cancel each other leaving the amplitudes to the right answer of whatever problems they are trying to solve.

2.2 The power of qubits

Quantum affords us three superpowers that are exhibited in the qubits. They are:

a) Superposition

Let's understand this with a small example. Take a coin and flip it .When it falls on the ground and stops spinning there can be a chance it is a head or tail, just like zero or one. But what is the state while it is spinning. Superposition is this spinning of a coin and it is one of the things that makes a quantum computer powerful. A qubit can allow for uncertainty.

b) Interference

This is a principle in quantum mechanics where a particle in its superposition state can interfere with the direction of its path. This has been proved by the double slit experiment. But this is not an operation which can be performed in a classical bit world whereas it is possible in a quantum computer. Also the beautiful thing of quantum is that an exponential number of states (2^n) can be created.

c) Entanglement

This is a powerful and unique phenomenon in quantum mechanics. Particles get entangled when they interact with each other which means that when we measure the state of one particle its entangled pair will have an opposite state no matter what the distances between them are. It sounds weird and physicists haven't yet found out how or why it works. Einstein called this "*spooky action at a distance*". Once we can access these entangled quantum states it will help us in exploiting the exponentially large computational power of quantum systems.

In short existence in multiple states is called superposition and the relationship among these states is called entanglement.

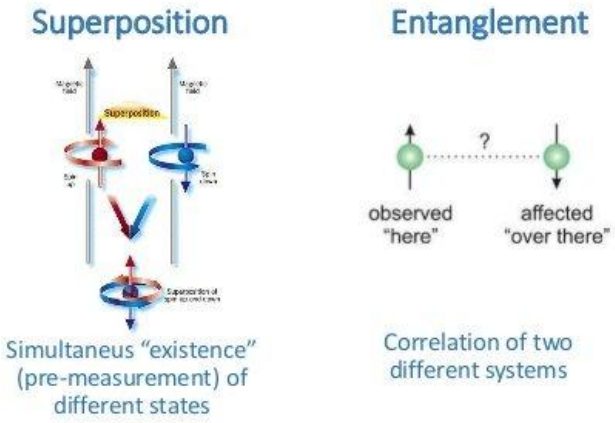

Fig -2 Superposition and

Let's put all these together and see how an algorithm works in a quantum computer. Suppose we have 5 qubit quantum computer .We prepare the computer to be in a superposition of states. That is 2^5 states which is equal to 32 states. After that we have to encode the problem by injecting data into the quantum machine through *quantum gates*. That encoding is done in all 2^5 states through entanglement. The gates re orient the qubits into new

superposition for all the 2^5 states by altering their phase and amplitude. Then the principle of interference comes from the fact that we can now take these states and combine them and interfere them with one another in such a way that we get to cancel things out and maximize the correct answer. Or in other words they magnify the amplitudes of the most probable answers and shrink the improbable answers. Some recursive problems will require running through the steps again So many things fall away and finally we perform a measurement and get the end result. Here we can see how different the working of quantum machine compared to classical bit operations is. Moreover there is an important relationship between these entangled states and the amount of data which can be processed. This relationship is exponential. The table below shows the number of classical bits (0 and 1) required to represent that complex entangled state described above. Here we can see that by the time we have 100 perfect qubits that are entangled to each other it would require every atom of planet earth to store those zeroes and ones, which is impossible.

Table -1

Qubits	Bits required to represent an entangled state
2	512 bits
3	1024 bits
10	16 kilobytes
16	1 megabyte
30	17 gigabyte
100	More than all atoms of planet earth
280	More than all atoms in the universe

2.3 Impact of quantum computing

Why does the hype over quantum computers matter these days. It is because despite how powerful our present day supercomputers are, there are a vast number of problems like factoring, problems in optimization which they cannot tackle. In fact there is an infinite number of problems in the world of mathematics and these problems are deeply important for businesses worldwide. Quantum computers will find use anywhere there is a complicated system that needs to be simulated. That could be anything from predicting the financial market, to improving weather forecasting, to modelling the behavior of individual electrons. They even have the potential to rapidly accelerate the development of Artificial Intelligence. They are expected to have a significant impact on the future of pharmaceutical, manufacturing and banking industries

Fig (3)

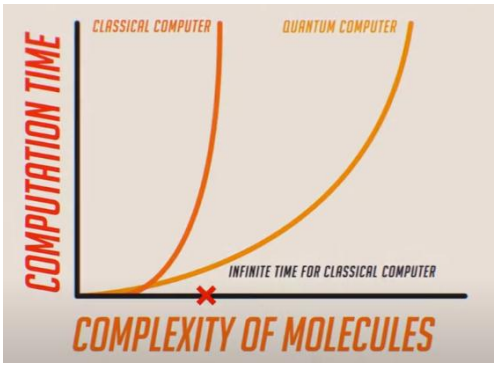

Fig -3 Computation time between a classical computer and Quantum Computer

3. SOME POSSIBLE KEY APPLICATIONS

a. Security

In terms of security there is a belief that quantum computers are going to be able to break all encryptions which would mean that banks, governments and cryptocurrency networks which use encryption algorithms for security would become hackable. At present there is difficulty in breaking down large numbers into prime numbers. This is called **factoring** and for a classical computer it is slow, expensive and impractical. There are rumors that intelligence agencies around the world are stock piling vast amounts of encrypted data in the hope that they will soon have quantum computer that can crack it. The only way to fight back is with **quantum encryption**. Quantum encryption keys could not be copied or hacked. They would be completely unbreakable. But inorder to that be a reality we require more technical advances in quantum computing especially more qubits and robust **quantum error correction**. Error correction ensures we get useful results

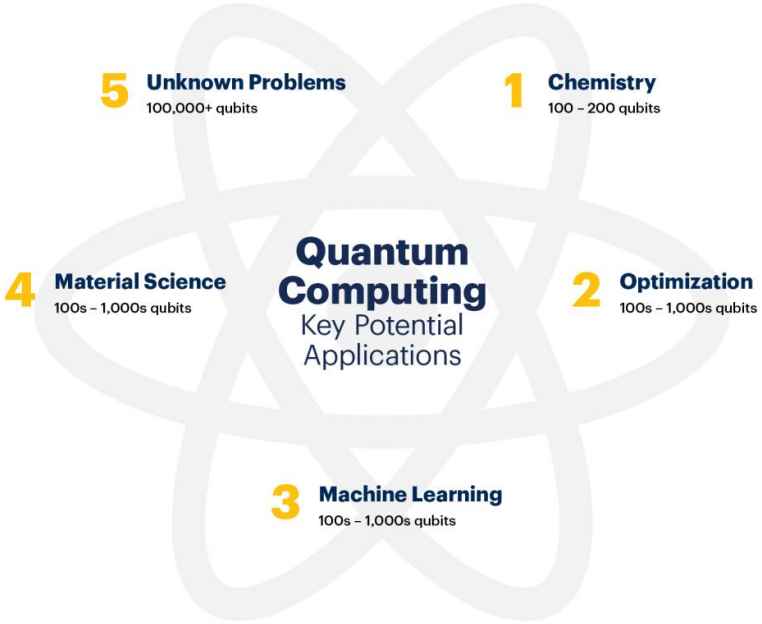

Fig -4 Major Applications of Quantum Computing

b. Medicine

Quantum technologies can also transform healthcare and medicine. The design analysis of molecules for drug development is a challenging problem today because we have to calculate the quantum properties of atoms in such molecules. If we can simulate a chemical reaction we can predict the outcome digitally. That would allow us to design new cures for diseases faster and help us understand the human body including brain at a much deeper level. But to do this even with the existing powerful supercomputer is a computationally difficult task. While as a quantum computer can do it easily because it functions under the same quantum properties a molecule is trying to simulate.

c. Finance

Billions of dollars are being invested in quantum technology hoping to find new ways to model financial data that ultimately help to understand key global risk factors. The global market is very computationally expensive to simulate and financial modelling teams use every tricks they can to do so at some level. This helps mitigate risks which allows them to invest smarter. Quantum computing has huge potential here.

d. Optimization problems

These problems deal with finding the lowest price ticket across a number of cities or the shortest route. Machine learning training of a big neural network is always formulated as an optimization problem and quantum algorithms can solve optimization problems than classical computers.

In about ten years from now quantum processors would turn out to be an indispensable co- processor for AI systems. The word co- processor which means that we have a processor that is good in certain specialized tasks but certainly not good in other things, the right way to think about quantum processors. Quantum computers will never fully replace "classical". They won't run browsers, help you with taxes or stream the latest video from Netflix. What they will do is offer a fundamentally different way of performing certain calculations faster than conventional computers.

4. WHAT IS QUANTUM ALGORITHM

An algorithm is a step by step procedure to perform or calculate a set of instructions to solve a particular problem. Each of these steps is performed in a classical computer. These algorithms can be called as quantum algorithms when it can be performed in a quantum computer, where atleast one step is quantum that uses the properties of quantum mechanics. We can also say that a quantum computer is a programmable machine that obeys the laws of physics and an algorithm is a recipe for solving the problem. When you design an algorithm you have to make sure that the machine you plan to run it on can execute each of those steps. Generally this is not a big problem in classical computers because one of the central principles of theoretical computer science is that if you use the right basic instruction set then any real world machine you could build can run that algorithm on it. But there is an exception in this rule in the case of quantum computers. Quantum computers use a fundamentally different instruction set than classical computers. As a result they can run different algorithms, algorithms which cannot run in classical computers. Those algorithms make use of quantum effects like the Superposition, Entanglement and Interference which we have already discussed above. Some of the best known algorithms are Shor's algorithm and Grover's algorithm.

Shor's algorithm is a quantum algorithm developed by Peter Shor in 1994 for integer factorization. It suggests that quantum mechanics allows factorization in polynomial time instead of the exponential time and this can have a dramatic impact in the field of data security.

Grover's algorithm or search algorithm can search an unstructured database faster than a classical computer to find a specific information.

5. THE ARCHITECTURE OF A QUANTUM COMPUTER

The quantum computers developed by companies like Google, IBM and Rigetti were all made by a process called *superconductivity.* You have a chip which is the size of an ordinary computer chip and you have little coils of wire in the chip which are quite enormous by the standards of qubits but quite difficult to see with naked eye.

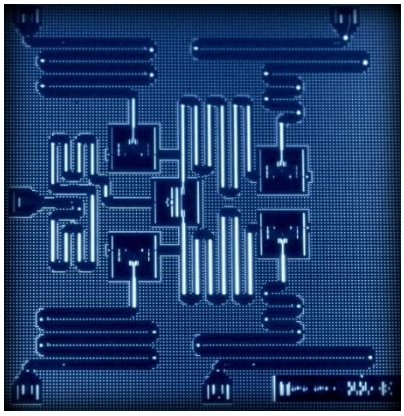

Fig -5 The Quantum Chip

You have two different quantum states of current that are flowing through these coils that correspond to a zero or a one and you can also have superpositions of the two. The coils can interact with each other via Josephan's junction which are coupled to a microwave resonator. The squares marked in *Fig (5)* are the qubits and the squiggly lines are the microwave resonator and inside the qubits are the superconducting Josephan's junction. They are laid out in roughly rectangular array and the nearby qubits can talk to each other and there by generate these very complicated states, what we call entangled states. This is one of the essentials of quantum computing and the way that the qubits interact with each other is fully programmable. So you can send electric signals to the chip to say which qubit should interact with each other ones at which time. Also these qubits are incredibly sensitive to any kind of external interference which can knock it out from the delicate position of superposition. And so they should be kept isolated from all forms of electrical interference. For this to work the whole chip is placed in the **dilution refrigerator**. That is the size of a closet roughly and the chip is kept at absolute zero.This is significantly colder than outer space. This is when you get the superconductivity that allows these bits to behave as qubits. Now the whole structure looks like a golden Chandelier *fig(6)* and we have the quantum processor at the bottom of this cryostat. So this makes it clear that building a reliable quantum hardware is challenging. And adding more and more qubits to increase the computational power is an even more difficult and expensive task.

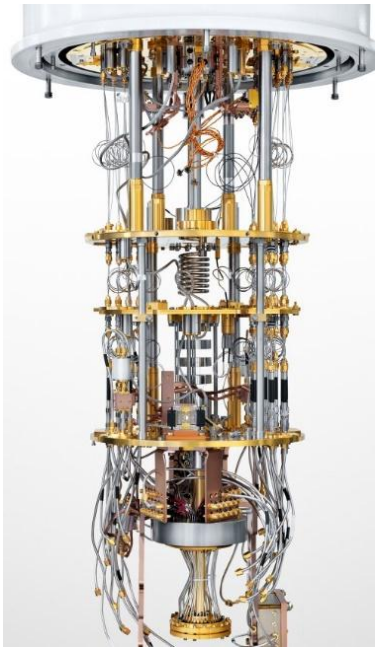

Fig -6 The inside of a Quantum Computer

Google quantum processor , the **"Sycamore"** have recently unveiled processors of 54 qubits there by claiming to attain ***Quantum Supremacy***.

6. QUANTUM SUPREMACY

It is a term proposed by John Preskill in 2012. It is the point where quantum computers can do things that classical computers cannot. Reaching that point is significant as an entirely new computer could be created that would allow an entirely different way of dealing data. That could revolutionize the world. Recently in October 2019 Google claimed to attain this supremacy. According to them their computer with 54 qubits which did a calculation in just more than 3 min which a supercomputer would have taken 10000 years. Not everyone agrees that the announcement represents true quantum supremacy. IBM claims that its most powerful supercomputer *"Summit"* can do the same task in 2.5 days rather than 10000 years. Still Google's success is noteworthy as Preskill says. He also said that "It won't change anything overnight but it is significant that quantum computers are now at the stage that atleast in some arena they can outperform the best computers on earth. Google accepts that the task performed isn't super important for this milestone, it's much more about the fact that the milestone happened in the first place.

They also cited the wright brothers as an analogy." For them to demonstrate that aviation is possible, it didn't matter so much where the plane was headed, where it took off and landed, but that it was able to fly it all".

Preskill also forewarned that this is entirely new technology with a whole lot of unknowns. The real journey is much longer and there is so much left to do for the upcoming scientists and researchers.

6.1 Demonstrating quantum supremacy

To demonstrate quantum supremacy there are basically three steps:

First is to pick a circuit. Second, is to run it in a quantum computer. And finally, simulate what the quantum computer is doing, on a classical computer. Then we gradually increase the complexity of that circuit. At some point it becomes completely impossible for the classical computer to keep up this pace. Then we say we achieved quantum supremacy. This was what Google did. They constructed a device consisting of 54 qubits made of tiny loops of superconducting wire and capable of representing 10 quadrillion states. With it they created a quantum random generator and generated 1,000,000 numbers in just 200 seconds. And after running some tests in the world's most powerful supercomputer they concluded that the machine would take about 10,000 years to do the same thing. Even though it was a slight exaggeration we can conclude that quantum computers are getting better. Technologies are born this way. Let's say the space age started with a satellite orbiting earth and it was not doing much rather than just beeping. So now after Google attaining the quantum supremacy the quest for galactic conquest can begin in earnest.

7. THE NOISE (ERRORS) IN QUANTUM COMPUTING

Why do we say that quantum computing is very hard? It is because of **Noise**. What is this Noise .It is not loud sound which makes us difficult to concentrate. Here we mean something else. Noise describes all things that can cause a quantum computer to malfunction. A quantum computer is susceptible to noise from all sorts of sources like electromagnetic signals coming from Wifi or disturbances in the earth's magnetic field. When qubits in a quantum computer are exposed to such noise the information in them gets degraded just the way sound quality is degraded by interference in a phone call. This is known as **Decoherence**. When a qubit is staying idle, not being used in a computation its states can be affected in a decoherence and when we are performing a quantum logic operation like a bit flip we can also suffer from errors that causes to rotate by the wrong amount. In either case the quantum state doesn't end up in the way you expect and overtime it can be randomized or totally erased. That's not good thing because that quantum state was actually representing an information. Compared to standard computers, quantum computers are extremely sensitive to such noises. A typical transistor in a microprocessor can run for about a billion years without ever suffering from a hardware fault. But in contrast the quantum bits gets randomized very fast. Now in the case of a quantum algorithm, executing many operations requires a large no of qubits. Now noise can make the qubits to be randomized which can lead to errors in our algorithm. The greater the influence of the noise the shorter the algorithm we can run. As a result we can run only a dozens of operations instead of trillions before noise causes a fatal error. Right now even the best quantum computer with 54 qubits is not reliable as their error rates are high. That means that for now, claims of quantum supremacy have to be taken with a pinch of salt.

7.1 NISQ (Noise intermediate scale quantum) era.

We now know that noise and decoherance are the major problems for quantum computers. Even leveraging the power of quantum hardware, errors will limit the scale of the machines we can build. We have to move to lower error rates and higher computational values. The good news is that clever algorithm designers have started to discover new problems which can potentially be solved with *Noisy Intermediate Scale Quantum computers or NISQ computers.* This is the new era in computer science which has already started. Eventually this will be superseded by an area when we have fault tolerance or error corrected quantum computers.

8. WILL CLASSICAL COMPUTERS BE REPLACED BY QUANTUM COMPUTERS.

One can simulate a quantum computer on a classical computer by just numerically solving the equations of quantum mechanics. If you do that then the computational burden on the classical computer increases exponentially with the number of qubits that you try to simulate. You can do 2-4 qubits on a personal computer but to about 50 qubits you need a cluster of supercomputers. Anything beyond 50 -55 qubits cannot presently be calculated at least not in any reasonable amount of time. Even with these advantages we cannot say that quantum computers will replace classical ones. They are not universally faster. They are faster only for special types of calculations where you can use the fact that you have different superpositions available to you at the same time to do some computational calculations. Like if you just want to watch a movie in HD or browse the internet they are not going to give you any particular improvement. We should not think of a quantum computer something that every operation is going to be faster rather it is the number of operations required to arrive at a particular result is exponentially small. In short it is not in the speed but in the number of steps to reach the result. Actually the term 'quantum Supremacy' leads to misunderstandings, because quantum computers will never reign supreme over classical computers but will rather work together with them ,since they have their unique strengths. So that is why it is not universal or a replacement to classical computers.

8.1 A personal Quantum Computer

We will probably never have quantum chip in our laptop or smartphone. The reason is as discussed above they are incredibly sensitive to interference .Almost anything can knock this qubit out of its delicate state of superposition. So these computers has to be kept isolated from all sorts of electrical interference and also chilled to absolute zero. That is colder than interstellar space. Currently the cost of creating a quantum computer and maintaining it runs in the hundreds of thousands of dollars if not millions. In future they might be used by academics' and businesses who can access them remotely. For example now we can access IBM's quantum computer in the cloud and it is called *IBM quantum experience*. All can access it for free and we can even play a card game in it.

9. CONCLUSIONS

So quantum computers however have a long way to go. They need exponentially more qubits before they can start doing anything useful as promised. Infact they need bigger advances than what occurred during the timeline of classical computing and Moore's law. Moore's law is doubling every 2 years but for quantum computers we may need doubling every year and occasionally some bigger jumps. However as the technology advances we will reach the point where we are doing things that we think go beyond what we can do with current or foreseeable classical computers. It could take decades. As John Preskill says there are a lot of ideas and researches going on and with a breakthrough the technology could take off. So let's patiently await the quantum future.

REFERENCES

[1] J. Eisert, M. Wilkens, "Quantum games and quantum strategies," Phys. Rev. Lett., vol. 83, pp. 3027–3088, 1999.

[2] M. Freedman, and C. Nayak, Majorana zero modes and topological quantum computation, npj Quantum Information 1, 15001 (2015), arXiv:1501.02813

[3] Steane, A. M. Error correcting codes in quantum theory. *Phys. Rev. Lett.*

[4] Montanaro and S. Pallister, Quantum algorithms and the finite element method, Phys. Rev. A 93, 032324 (2016), arXiv:1512.05903

[5] D. A. Spielman and S.-H. Teng, Smoothed analysis of algorithms: why the simplex algorithm usually takes polynomial time, Journal of the ACM 51, 385-463 (2004), arXiv:cs/0111050

[6] R. Barends, J. Kelly, A. Megrant, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A.. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, Superconducting quantum circuits at the surface code threshold for fault tolerance, Nature 508, 500-503 (2014), arXiv:1402.4848,

[7] Bang, J.; Ryu, J.; Kaszlikowski, D. (2018): Fidelity deviation in quantum teleportation. Journal of Physics A: Mathematical and Theoretical, vol. 51, no. 13, pp. 135302-135311

[8] R. Penrose, The Emperor's New Mind: Concerning Computers, Minds, and the Laws of Physics, [80] A. Petersen, M. Oskin, A new algebraic foundation for quantum programming languages, in: Proceedings of the 2nd Workshop on Non-Silicon Computing, 2003

[9]M.S. Ying, Y. Feng, R.Y. Duan, Z.F. Ji, An algebra of quantum processes, ACM Transactions on Computational Logic 10 (2009), art. no. 19. [113] S.Y. Zhang, Y. Feng, X.M. Sun, M.S. Ying, Upper bound for the success probability of unambiguous discrimination among quantum states, Physical Review A 64 (2001), art. no. 062103.

[10] Preskill, J. Reliable quantum computers. Proc. R. Soc. Lond. A 454, 385–410 (1998)

[11]Knill, E., Laflamme, R. & Zurek, W. H. Resilient quantum computation. Science 279, 342–345 (1998)

[12] Feynman, R. P. Simulating physics with computers. Int. J. Theor. Phys. 21, 467–488 (1982)

[13] Steane, A. M. Quantum computing. Rep. Prog. Phys. 61, 117–173 (1998).

[14] T. o. Lanting, "Entanglement in a quantum annealing processor," Phys. Rev. X, vol. 4, p. 021041, May 2014. [Online]. Available: S. Debnath, N. Linke, C. Figgatt, K. Landsman, K. Wright, and C. Monroe,

[15] "Demonstration of a small programmable quantum computer with atomic qubits," Nature, vol. 536, no. 7614, pp. 63–66, 2016. [9] T. Monz et al., "Realization of a scalable shor algorithm," Science, vol. 351, no. 6277, pp. 1068–1070, 2016.

[16] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. Ieee, 1994, pp. 124–134.

[17] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell et al., "Superconducting quantum circuits at the surface code threshold for fault tolerance," Nature, vol. 508, no. 7497, pp. 500–503, 2014.