HOW QUANTUM COMPUTING WILL CHANGE OUR WORLD!

Debi Prasad Mishra

Electronics and Communication Engineering, ITER, Bhubaneswar, India

E-mail: debiprasadmishra50@gmail.com

Abstract

The main purpose of this paper is to examine the quantum computation in relation with our current computers and the changes a quantum computer can bring into our civilisation. The paper is all about exploration and research details of quantum physics and the applications of qubits in modern computation and application of quantum computers in real time and change of an era to Artificial Intelligence. For the readers who are not familiar with quantum computation, a brief introduction is provided and the author hopes the paper will help many people to have more research on quantum theory and show their interest in modernising the world and to explore further and deeper in connection between AI and quantum computation and to gain knowledge.

Keywords: *quantum, computing, qubits, mechanics, superposition, entanglement, AI, bits and bytes, complex, gate*

1. Introduction

Quantum computing is a new and exciting field at the intersection of mathematics, computer science and physics. It concerns a utilization of quantum mechanics to improve the efficiency of computation. By successful creation of a quantum computer and with its computing speed and technique, current classical computers could look like an antique in front of them.

1.1. Quantum

Quantum means amount (in Latin), in modern science it means the smallest possible discrete unit of any physical property such as energy or matter. The magnitude of the physical property can take on only discrete values consisting of integer multiples of one quantum.

1.2. Quantum Mechanics

It is the theoretical basis of modern physics that explains the nature and behaviour of matter and energy on the atomic and subatomic level. The nature and behaviour of matter and energy at that level is sometimes referred to as quantum physics and quantum mechanics. It describes the wacky behaviour of photons, electrons and other particles that make up the universe.

1.3. Quantum Computing

It is the area of study focused on development of computer technology based on principles of quantum theory, which explains the nature and behaviour of energy and matter on sub-atomic level. The quantum computer follows the laws of quantum physics and it would gain enormous processing power for being in multiple states and can perform vast number of tasks using all possible permutations and combinations in shorter span of time.

2. History and Evolution of Quantum Computers

Famous physicist Dr Richard Feynman said in a 1981 conference held at MIT, “Nature isn’t classical, dammit, and if you want to make a simulation of nature, you’d better make it quantum mechanical.” That is how it all begun. Paul Benioff and Feynman continuously searched and tried different ideas and Tommaso Toffoli introduced the reversible Toffoli gate made up of NOT and XOR gate. In 1982 Benioff developed first quantum mechanical Turing machine. After the 80’s physicist Peter Shor unveiled an algorithm in 1994 that showed that a computer based on qubits could factor large numbers near-exponentially faster than the best bit-based algorithms. If scientists could invent a quantum computer advanced enough to run the algorithm, then it could crack the popular modern-day encryption systems based on the fact that it is easy for classical computers to multiply two large prime numbers together but very, very hard to factor the result back into primes. In 98 two teams published the result of first real world quantum computations, but it was not a computer at all, it was a biochemistry equipment relying on the same science as MRI (Magnetic Resonance Imaging) machine.

The prototype quantum computers in 1997 indirectly led to the success of Google and IBM as it was made in their laboratories. In 98 first experimental demonstration of quantum algorithm working with 2-qubit NMR (Nuclear Magnetic Resonance) quantum computer used to solve Deutsch’s problem and first 3-qubit NMR computer got evolved. In early 20’s 5 and 7-qubit NMR computers was demonstrated at Munich and Los Alamos laboratories respectively. In 2001 Emanuel Knill, Raymond Laflamme, and Gerard Milburn showed that optical quantum computing is possible with single photon sources, linear optical elements, and single photon detectors, launching the field of linear optical quantum computing. In 2004, first working pure state quantum computer was exhibited at Oxford University.

Since 2007 it has been a game changer for quantum computing. The development of nanotech and quantum computers rapidly grew and D-wave systems demonstrated use of 28-qubit quantum annealing computer. In 2015 D-waves' 2X Quantum Computer with more than 1000-qubits was installed at the Quantum Artificial Intelligence Lab at NASA Ames Research Centre. They have subsequently shipped systems with 2048-qubits. In 2019 D-waves announced a 5000-qubits system to be available by mid-2020 using their new Pegasus-chip with 15 connections per qubit.

3. Quantum Computing

Computers are getting smaller and faster eventually because electronic components are getting smaller and smaller but this process is about to meet its physical limit. It is the use of quantum mechanical phenomenon such as super-position and entanglement to perform computation at sub-atomic level. A quantum computer is used to perform complex computations, which can be implemented theoretically and physically but in much faster rate.

Quantum computers are different from other computers such as DNA computers and traditional computers based on transistors. Some computing architectures such as optical computers may use classical superposition of electromagnetic waves, but without some specifically quantum mechanical resources such as entanglement, they have less potential for computational speed-up than quantum computers. The power of quantum computers Integer factorization is believed to be computationally infeasible with an ordinary computer for large integers that are the product of only a few prime numbers (e.g., products of two 300-digit primes). By comparison, a quantum computer could solve this problem more efficiently than a classical computer using Shor's algorithm to find its factors. This ability would allow a quantum computer to "break" many of the cryptographic systems in use today, in the sense that there would be a polynomial time (in the number of bits of the integer) algorithm for solving the problem.

3.1. Qubit or Quantum bit

Until now, most silicon-based qubits have been made from the electron or the nucleus of a single phosphorous atom. A qubit design uses both the nucleus and electron of a phosphorous atom to create a single qubit inside a layer of silicon.

3.1.1 Features of Qubits

They operate on completely different principles on existing computers, which makes them really well suited to solve particular mathematical problems like finding very large prime number.

Researchers are also excited about the prospect of using quantum computing to model complicated chemical reactions. In July 2016, Google engineers used a quantum device to simulate a hydrogen In classical computing for example there are 4 bytes. The molecule for the first time and since then IBM has managed to model the behaviour of even more complex molecules.

A bit is either in state 0 or in state 1. That was sufficient for the classical world but that is not sufficient for the quantum world. In that world we have situations where we are in one state and in the other state simultaneously. In the quantum world, we have systems where a switch is in a superposition of states on and off. So we define a "quantum bit" or a "qubit" as a way of describing a quantum system of dimension two. We shall represent any such qubit as a two by one matrix with complex numbers:

$$\begin{bmatrix} c0 \\ c1 \end{bmatrix}$$

A quantum computer uses qubits to supply information and communicate through the system. Its encoded with quantum information in both states of **0 and 1** instead of classical bits which can only be **0 or 1**. This means a qubit can be in multiple places at once due to superposition.

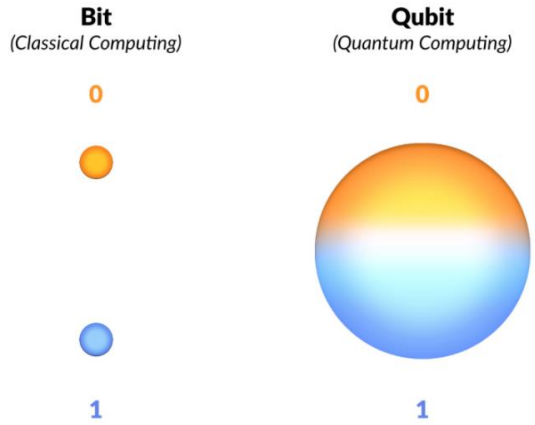

Figure 1. Difference between a bit and a quantum bit

3.2. Superposition

In classical computing bits has two possible states **either zero or one**. In quantum computing, a qubit (short for "quantum bit") is a unit of quantum information—the quantum analogue to a classical bit. Qubits have special properties that help them solve complex problems much faster than classical bits. One of these properties is **superposition**, which states that instead of holding one binary value ("0" or "1") like a classical bit, a qubit can hold a combination of "0" and "1" simultaneously. Qubits have two possible outcomes zero or one but those states are superposition of zero and one. In quantum world qubits don't have to be in one of those states. It can be in any proportion of those states. As soon as we measure its value, it has to decide whether it is zero or one. This is called superposition. It is the ability of the quantum system to be in multiple states at same time.

combination of 4 bytes can represent 2^4=16 values in total and one value a given instant. However, in a combination 4 qubits all 16 combination are possible at once.

Think of a qubit as an electron in a magnetic field. The electron's spin may be either in alignment with the field, which is known as a spin-up state, or opposite to the field, which is known as a spin-down state. Changing the electron's spin from one state to another is achieved by using a pulse of energy, such as from a laser - let's say that we use 1 unit of laser energy. But what if we only use half a unit of laser energy and completely isolate the particle from all external influences? According to quantum law, the particle then enters a superposition of states, in which it behaves as if it were in both states simultaneously. Each qubit utilized could take a superposition of both 0 and 1. Thus, the number of computations that a quantum computer could undertake is 2^n, where n is the number of qubits used. A quantum computer comprised of 500 qubits would have a potential to do 2^500 calculations in a single step. This is an awesome number - 2^500 is infinitely more atoms than there are in the known universe (this is true parallel processing - classical computers today, even so called parallel processors, still only truly do one thing at a time: there are just two or more of them doing it). But how will these particles interact with each other? They would do so via quantum entanglement.

3.3. Entanglement

Entanglement is an extremely strong correlation that exists between quantum particles — so strong, in fact, that two or more quantum particles can be linked in perfect unison, even if separated by great distances. The particles remain perfectly correlated even if separated by great distances. Two qubits are entangled through the action of laser. Once they have entangled, they are in an indeterminate state. The qubits can then be separated by any distance, they will remain linked. When one of the qubits is manipulated, the manipulation happens instantly to its entangled twin as well.

Entanglement Particles (such as photons, electrons, or qubits) that have interacted at some point retain a type of connection and can be entangled with each other in pairs, in a process known as correlation . Knowing the spin state of one entangled particle - up or down - allows one to know that the spin of its mate is in the opposite direction. Even more amazing is the knowledge that, due to the phenomenon of superposition, the measured particle has no single spin direction before being measured, but is simultaneously in both a spin-up and spin-down state. The spin state of the particle being measured is decided at the time of measurement and communicated to the correlated particle, which simultaneously assumes the opposite spin direction to that of the measured particle. This is a real phenomenon (Einstein called it "spooky action at a distance"), the mechanism of which cannot, as yet, be explained by any theory - it simply must be taken as given. Quantum entanglement allows qubits that are separated by incredible distances to interact with each other instantaneously (not limited to the speed of light). No matter how great the distance between the correlated particles, they will remain entangled as long as they are isolated. Taken together quantum superposition and entanglement create an enormously enhanced computing power. Where a 2-bit register in an ordinary computer can store only one of four binary configurations (00, 01, 10, or 11) at any given time, a 2-qubit register in a quantum computer can store all four numbers simultaneously, because each qubit represents two values. If more qubits are added, the increased capacity is expanded exponentially.

3.4. What Quantum computers can do!

Quantum computers can easily crack the encryption algorithms used today in very less time whereas it takes billions of years to best supercomputer available today. Even though quantum computers would be able to crack many of today's encryption techniques, predictions are that they would create hack-proof replacements. Quantum computers are great for solving optimization problems.

Quantum computers are in their early stage of development much like the classical computers back in the 50's. No doubt with the classical computers came revolutionary technology such as the internet so imagine the applications of quantum computers for the future.

3.4.1. Applications of Quantum Computer

A quantum computer can helps us in better online security with development in quantum encryption, significantly improvement in AI technology, drug research and discovery, more accurate weather predictions, optimizing traffic control and many more.

3.5 Classical computing vs Quantum computing

3.5.1. Classical computing

The conventional method of computing is the most popular method for solving the desired problem with the estimated time complexities. Algorithms of searching, sorting and many others are there to tackle daily life problems and are efficiently controlled over time and space with respect to different approaches. For example, Linear Search has time complexity of O(n), Binary Search have (nlog2n). These all give a boom to software industries and other IT sectors to work for the welfare of the world.

Classical computing relies, at its ultimate level, on principles expressed by Boolean algebra, operating with a (usually) 7-mode logic gate principle, though it is possible to exist with only three modes (which are AND, NOT, and COPY). Data must be processed in an exclusive binary state at any point in time - that is, either 0 (off / false) or 1 (on / true). These values are binary digits, or bits. The millions of transistors and capacitors at the heart of computers can only be in one state at any point. While the time that the each transistor or capacitor need be either in 0 or 1 before switching states is now measurable in billionths of a

second, there is still a limit as to how quickly these devices can be made to switch state. As we progress to smaller and faster circuits, we begin to reach the physical limits of materials and the threshold for classical laws of physics to apply. Beyond this, the quantum world takes over, which opens a potential as great as the challenges that are presented.

Certainly, we use bits (either 0 or 1) for storing the information and with the help of these 2 bits, we calculate Giga to Tera to Petabytes of data and even much more with quite unparalleled efficiency. Now let's go deep into it, Four classical Bits can be transformed in 2^4 combinations i.e. 16 combinations as follows-

```
0000    0001    0010    0011
0100    0101    0110    0111
1000    1001    1010    1011
1100    1101    1110    1111
```

That's 16 possible combinations, out of which we can use only one at a time. Our CPU calculates at average 2.4GHz, apparently, it looks like that all combinations are calculated simultaneously but of course they are distinct from each other and CPU calculate one at a time each combination. Although simultaneous calculation can be done by having more than 1 CPU in the machine and that's is called as Multiprocessing but that's a different thing. The fact is that our CPU calculates each combination one at a time. Here arises a big and advanced research question – can all of them be used simultaneously at once without having any multiprocessors?

3.5.2. Quantum Computing

To answer this crazy question, Quantum Computing came into the picture. The Quantum computer, by contrast, can work with a two-mode logic gate: XOR and a mode we'll call QO1 (the ability to change 0 into a superposition of 0 and 1, a logic gate which cannot exist in classical computing). In a quantum computer, a number of elemental particles such as electrons or photons can be used (in practice, success has also been achieved with ions), with either their charge or polarization acting as a representation of 0 and 1. Each of these particles is known as a quantum bit, or qubit, the nature and behaviour of these particles form the basis of quantum computing. The two most relevant aspects of quantum physics are the principles of superposition and entanglement .This computing technique makes direct use of distinctively quantum mechanical phenomena such as superposition and entanglement to perform the operation on the data. The basic and extraordinary idea for quantum computing is that in normal classical computers, bits are the basic smallest unit of information.
Quantum computers use qubits (Quantum bits) which can also be set up as 0 or 1 likewise the classical bits but the container of these bits are changed from transistors to photons. A Qubit can be among any 2 level quantum system, such as spin and a magnetic field, or a single photon. The possible states can be entitled as 0 or 1 as per the horizontal or vertical polarisation. Consequently, of Quantum World theory, qubit doesn't have to be just one of those. it can be in any ratio of both the states at once. That merely called as Superposition.
This can lead to a severe and ground-breaking foundation in the field of computer science. This helps to solve many unsolved or virtually solvable problems with the unified space and time complexities.

3.6 How does a quantum computer work!

At 100-qubits a single quantum computer processor would theoretically be more powerful than all the super computers on the planet combined. They do not follow the normal rules of physics, instead of bits like the classical computers, they use qubits to store information. Building a functional computer requires holding an object in a superposition state long enough to carry out various process on them. Unfortunately once a superposition meets with materials that are part of a measured system, it loses its in-between state in what's known as de-coherence and becomes a boring old classical bit. Devices need to be able to shield quantum states from de-coherence while still making them easy to read.

4. How quantum computing will change our world?

Quantum computers will disrupt every industry. They will change the way we do business and the security we have in place to safeguard data, how we fight disease and invent new materials, and solve health and climate problems. As the race to be the first to create a commercially viable quantum computer accelerates, here are just a few ways quantum computing will change our world.

4.1. Online Security

There will be good and bad for online security once there is widespread adoption of quantum computers. Our current data encryption tactics will become obsolete. Currently, most online security methods count on the fact that it takes an extraordinary amount of time to "crack the code" as computers crunch large numbers. However, quantum computers will be able to process this information quickly leaving our computers, financial institutions and private information vulnerable. The good news is that significant work has been done to develop quantum encryption methods such as quantum key distribution, an ultra-secure communication method that requires a key to decipher a message. Thanks to the peculiar properties of quantum mechanics, if the message gets intercepted, no one else can read it.

4.2. Artificial Intelligence

The information processing that it critical to improve machine learning is ideally suited to quantum computing. Quantum computers can analyse

large quantities of data to provide artificial intelligence machines the feedback required to improve performance. Quantum computers are able to analyse the data to provide feedback much more efficiently than traditional computers and therefore the learning curve for artificial intelligence machines is shortened. Just like humans, artificial intelligence machines powered by the insights from quantum computers can learn from experience and self-correct. Quantum computers will help artificial intelligence expand to more industries and help technology become much more intuitive very quickly.

4.3. Drug development

In order to develop an effective drug, chemists need to evaluate the interactions between molecules, proteins and chemicals to see if medicines will improve certain conditions or cure diseases. Due to the extraordinary amount of combinations that are analyzed, this is time and labor intensive. Since quantum computers can review multiple molecules, proteins and chemicals simultaneously, they make it possible for chemists to determine viable drug options quicker. Additionally, some drugs are being cancelled in the trial stage even when they might work for a subset of the population. Quantum computing would allow for a person's genes to be sequenced and analyzed much more rapidly than the methods we use today and would allow for personalized drug development.

4.4. Improve weather forecasting and climate change predictions

Even with sophisticated tools, weather forecasting remains a bit of a guessing game. Just ask anyone who has been caught in a storm with no warning or prepared for a blizzard but ultimately only saw flurries. Since quantum computers can analyse all the data at once, meteorologists will have a much better idea of when bad weather will strike to alert people to ultimately save lives, anguish and money. The UK Met Office, the national weather service of the United Kingdom, has already invested in quantum computing technology to help improve forecasting. We can also gain more insight into how we are influencing our climate because quantum computers will help us build better climate models. The sooner we know how things are expected to shift, the better we will be able to prepare and respond to climate change and its impact.

4.5. Traffic Control

Whether in the air or on the ground, quantum computers will help to streamline traffic control. They will be able to quickly calculate the optimal routes concurrently which allows for efficient scheduling and would reduce traffic congestion. For similar reasons, quantum computers are also powerful for optimizing supply chains, air traffic control, fleet operations and deliveries.

4.6. Tackling the whole problem

Instead of troubleshooting issues bit by bit as we do now with classical computers, quantum computers tackle the entire problem at once. This opens the door for amazing developments in every field from financial services to our national security.
Perhaps Eric Ladizinsky, co-founder of quantum computing company D-Wave, explained the differences between a regular computer and a quantum computer best when he spoke at WIRED 2014 conference. He said to imagine that you only have five minutes to find an X written on a page of a book among the 50 million books in the Library of Congress. In this scenario, you would be a regular computer and you would never find the X. But, if you had 50 million parallel realities and you could look at a different book in each of those realities (just like a quantum computer), you would find the X. A quantum computer splits you into 50 million versions of yourself to make the work quick and easy.

Quantum computers give us the ability to solve complex problems that are beyond the capabilities of classical computers.

5. Disadvantages of a Quantum computer

The main disadvantage of computing is the technology required to implement a quantum computer is not available at present. The reason for this is the consistent electron is damaged as soon as it is affected by its environment and that electron is very much essential for the functioning of quantum computers. The research for this problem is still continuing the effort applied to identify a solution for this problem has no positive progress. It is not cost effective, Even IBM recent show case their first commercial Quantum Computing solution, it is make viable sense to offer as "subscription" basis base on the use case on demand only. For the Quantum Computing to be really achieve critical mass adoption, it take a long time for all the cost variable become reasonable, then we can see how Quantum Computing revolution the current mass technology. So, it make sense to be aware that is coming, but may or may not necessary to heavy invest on it yet.

References

[1] Prasant, Universite de Montreal, Montreal, Canada: A study on the basis of Quantum Computing

[2] Mingsheng Ying,Center of Quantum computations and Intelligent Systems, University of Technology, Sydney, Australia: Quantum Computation, quantum theory and AI, 18 November 2009

[3] Noson S. Yanofsky, An introduction to Quantum computing, 2 Aug 2007.

[4] Tanissa Bassan, A brief Introduction to quantum computing, jan 23rd 2018