On the Study of Quantum Computing

Myo Myo Aung[#1], Kay Thwe Kywe Aye[#2], Tun Myat Aung[#3]

Natural Science Department, Myanmar Institute of Information Technology, Mandalay, Myanmar

[1]myomyoaung@miit.edu.mm, [2]kaythwekyweaye@miit.edu.mm, [3]tma.mephi@gmail.com

Abstract – **Quantum computing is the new field of science which uses quantum phenomena to perform operations on data at the intersection of mathematics, computer science and physics. This paper is to guide computer scientists through the barriers that separate quantum computing from conventional computing. We introduce basic principles of quantum mechanics to explain where the power of quantum computers comes from and why it is difficult to harness. We describe the differences between classical and quantum computers, bit and quantum bit and quantum operation.**

Keywords: **classical computer, quantum bit, quantum computer**

I. INTRODUCTION

Computers are getting smaller and faster day by day because electronic components are getting smaller and smaller. But this process is about to meet its physical limit. Electricity is flow of electrons. Since size of transistors is shrinking to size of few atoms, transistors cannot be used as switch because electron may transfer themselves to the other side of blocked passage by the process called quantum tunnelling.

The field of quantum computing is actually a sub-field of quantum information science, which includes quantum cryptography and quantum communication. Quantum Computing was started in the early 1980s when Richard Feynman and Yuri Manin expressed the idea that a quantum computer had the potential to simulate things that a classical computer could not. In 1994, Peter Shor published an algorithm that is able to efficiently solve some problems that are used in asymmetric cryptography that are considered hard for classical computers.

Qubits are fundamental to quantum computing and are somewhat analogous to bits in a classical computer. Qubits can be in a 1 or 0 quantum state. But they can also be in a superposition of the 1 and 0 states. However, when qubits are measured the result is always either a 0 or a 1; the probabilities of the two outcomes depends on the quantum state they were in.

Today's physical quantum computers are very noisy and quantum error correction is a burgeoning field of research. Unfortunately, existing hardware is so noisy the fault-tolerant quantum computing is still a rather distant dream. As of April 2019, no large scalable quantum hardware has been demonstrated, nor have commercially useful algorithms been published for today's small, noisy quantum computers. We will describe development of classical computer, quantum states, and how they are represented mathematically and then possible operations on these states are discussed.

II. AIM

There is an increasing amount of investment in quantum computing by governments, established companies, and start-ups. Both applications of near-term intermediate-scale device and the demonstration of quantum supremacy are actively pursued in academic industrial research. The object is to help us understand this new age technology and its benefits.

III. CLASSICAL COMPUTER

Intensive research of classical computers began during World War II, when there was a need to calculate with large numbers and difficult problems in the Manhattan project. Many scientists were brought together to face this problem. The first computers they built were so big that they filled up a whole room, which restricted their wider application. Fortunately, in the late 1940s transistors were invented by William Shockley, John Bardeen and Walter Brattain, which lead to massive development of classical computers. In the next decades the computational power has risen fast. This increase was examined by Gordon E. Moore who observed that the number of transistors doubles roughly every two years. The capabilities of many electronic devices are strongly related to this law: memory capacity, processing speed or sensors. This exponential increase has a huge impact in every segment of the world economy. The increase of computational power and decrease of size of smartphones, tablets or laptops is astonishing. The dependence of the number of transistors on time is shown in Fig1.

However, this exponential increase has its boundaries which will show according to experts at the end of 2015. The increase in performance is due to the fact that we lay more transistors on a same size chip. That is why large processor manufacturers such as Intel or AMD try to produce smaller and smaller transistors. However, when the distance between two transistors will get smaller then 10^{-9}m disturbing quantum mechanical effects will take place and the transistors will no longer work properly. The second factor that speaks against smaller transistors is protection from overheating. At these small distances it is almost impossible to cool the transistors by air. Liquid cooling would be expensive for commercial use.

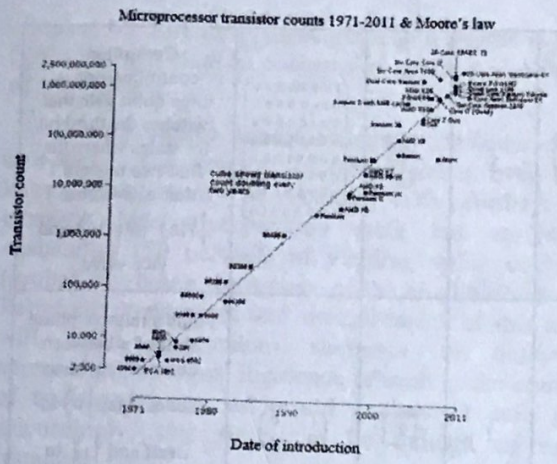

Fig.1 CPU transistor counts against dates of introduction

IV. BASIC CONCEPT OF QUANTUM COMPUTER

A. *Quantum Bit*

A quantum computer also represents information as a series of bits, called quantum bits, or qubits. Like a normal bit, a qubit can be either 0 or 1, but unlike a normal bit, which can only be 0 or 1, a qubit can also be in a state where it is both at the same time. When extended to systems of many qubits, this ability to be in all possible binary states at the same time gives rise to the potential computational power of quantum computing. A qubit is represented as 2-by-1 matrix with a complex number, as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

The two basis state can be superposed,

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

with the condition that,

$$|\alpha|^2 + |\beta|^2 = 1$$

The $|\alpha|^2$ is the probability that the measurement of state will result in state 0, and the $|\beta|^2$ is the probability that the measurement of state will result in state 1 . Keep in mind that the general qubit cannot be seen: whenever the qubit is measured or observed, it spontaneously become a bit. Next, a representation of a qubit is introduced.

The general state of one qubit system can be represented in the form,

$$\psi = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers. It might seem there are four parameters. However, the equation holds the condition that,

$$|\alpha|^2 + |\beta|^2 = 1$$

So, the equation can be reformed in terms of two parameters,

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{0}{2}|1\rangle$$

With natural ranges $0 \le \theta \le \pi$ and $0 \le \psi \le 2\pi$. As only two real numbers are required to represent a qubit, it can be mapped into a three-dimensional coordinate system. The mapping looks like a unit sphere known as Bloch Sphere. It is a representation of qubit, the fundamental building block of quantum computer in Fig.2.

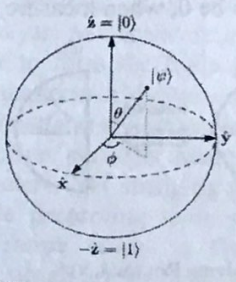

Fig. 2 The Bloch Sphere

B. *Quantum Operation*

1. The measure command measures the quantum register and returns the measured value. The measure operation is not reversible.
2. Unitary Gates:

   (i) Hadamard Gate: The Hadamard Gate is defined by the transformation matrix,

$$H = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The usage is to map n qubits initialized with 0 to a superposition of all 2^n orthogonal states in the $|0\rangle$, $|1\rangle$ basis with equal weight. This means, if observed, the state will collapse to be a 0 or 1 with equal probability.

(ii) Qubit Rotation: The rotation of a single qubit is defined by the transformation matrix,

$$U(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

The theta parameter used in this paper has range from $\frac{\pi}{2}$ to $-\frac{\pi}{2}$.

(iii) Using Hadamard gate and Qubit Rotation: Hadamard gate is used for transforming into an even superposition state of quantum register. According to Bloch's sphere, a qubit can be visualized as Fig.3-left. When a qubit rotation is applied, for example pi/4, the state will be Fig.2-right. This means the qubit is more likely to be 0, when measure, than 1.

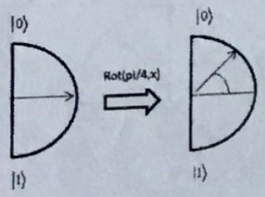

Fig.3 Applying Rot (pi/4, x)

Table 1. Commonly used 1-, 2-, and 3-qubit quantum gates, along with their corresponding unitary matrices, circuit symbols, and a description of their effects. The T, Hadamard, and CNOT gates are known to form a universal quantum gate set.

Gate	Qubits	Circuit Symbol	Unitary Matrix	Description
Hadamard	1		$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	Transforms a basis state into an even superposition of the two basis states.
T	1		$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$	Adds a relative phase shift of $\pi/4$ between contributing basis states. Sometime called a $\pi/8$ gate, because diagonal elements can be written as $e^{-i\pi/8}$ and $e^{i\pi/8}$.
CNOT	2		$\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$	Controlled-not; reversible analogue to classical XOR gate. In put connected to the solid dot is passed through to make the operation reversible.
Toffoli(CCNOT)	3		$\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{pmatrix}$	Controlled-controlled-not; a three qubit gate that switches the third bit for states where the first two bits are 1 (that is, switches) $\|110\rangle$ to $\|110\rangle$ and vice versa.
Pauli-Z	1		$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Adds a relative phase shift of π between contributing basis states. Map $\|0\rangle$ to itself and $\|1\rangle$ to $\|-1\rangle$. Sometimes called a "phase flip"
Z-Rotation	1		$\begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$	Adds a relative phase shift of (or rotates state vector about z-axis by) θ
NOT	1		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	Analogous to classical NOT gate; switches $\|0\rangle$ to $\|1\rangle$ and vice versa.

Table 2. Measurement Outcomes and Probabilities for a Single Qubit Given Its Initial State for Several Examples

Premeasurement State (Wave function) of Qubit	Measurement Outcome	Probability of Outcome	Post measurement State of Qubit
$\|\psi\rangle = \|0\rangle$	0	100%	$\|\psi\rangle = \|0\rangle$
$\|\psi\rangle = \|1\rangle$	1	100%	$\|\psi\rangle = \|1\rangle$
$\|\psi\rangle = \frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle$	0	50%	$\|\psi\rangle = \|0\rangle$
	1	50%	$\|\psi\rangle = \|1\rangle$
$\|\psi\rangle = \frac{1}{2}\|0\rangle + \frac{\sqrt{3}}{2}\|1\rangle$	0	25%	$\|\psi\rangle = \|0\rangle$
	1	75%	$\|\psi\rangle = \|1\rangle$
$\|\psi\rangle = \frac{1}{\sqrt{2}}\|0\rangle + \frac{\sqrt{3}}{2}e^{-i\pi/4}\|1\rangle$	0	25%	$\|\psi\rangle = \|0\rangle$
	1	75%	$\|\psi\rangle = \|1\rangle$

When a qubit is in the state $|\psi\rangle = |0\rangle$, the result of measurement will be 0 with a probability of 100 percent, which is not unlike what happens with a

classical bit. Similarly, measurement of a qubit in state $|\psi\rangle = |1\rangle$ will yield an outcome of 1 with a probability of 100 percent.

For a qubit in a superposition state, the outcome is less simple the outcome of measurement, even of a known state, cannot be predicted with certainty. For example, the superposition state has an equal probability (50 percent) of yielding either outcome (probability being the square of the amplitude, or ½). Repeated preparation and measurement of this state will yield a random sequence of outcomes approaching an equal incidence of each as the number of trials increases, as would a classical coin flip. Accordingly, this state can be thought of as a "quantum coin."

After measuring a certain value, the qubit is left in the state corresponding to that value. For example, if the outcome of measurement is 1, the post measurement qubit is in the state $|\psi\rangle = |1\rangle$, regardless of the state it was in prior to measurement.

C. *Structure of Quantum Computer*

A quantum computer looks like this, taking n input qubits, the register V, and producing n output qubits, the register W:

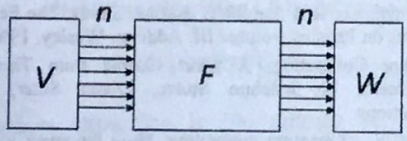

Fig. 4 Basic Structure of Quantum Computer

The input register can be prepared as a superposition of states, e.g. superposition of all integers from 0 to 2^n can be stored in input register. The computer then calculates in parallel the function applied to all 2^n integers simultaneously. From QMP (Quantum Measurement Postulate), when we measure W, according to resulting wave of qubits which is in entangled state a Boolean value for every bit from the output register is chosen. To maximize the probability that the answer we want and output we measure is same we have to design F.

Quantum computer hardware must satisfy fundamental constraints: (i) the qubits must interact very weakly with the environment to preserve their superposition, (ii) the qubits must interact very *strongly* with one another to make logic gates and transfer information, and (iii) the states of the qubits must be able to be initialized and read-out with high efficiency.

D. *Difference between Classical and Quantum Computing*

The most important difference between Classical Computers and Quantum Computers is the data representation. The qubit plays the same role in quantum computing as the bit does in classical computing: it is the fundamental unit of information. However, compared to a qubit, a bit is downright boring. Although both bits and qubits generate one of two states (a 0 or a 1) as the outcome of a computation, a qubit can simultaneously be in both 0 and 1 states prior to that outcome. If this sounds like quantum superposition, it is. Qubits are quantum systems par excellence.

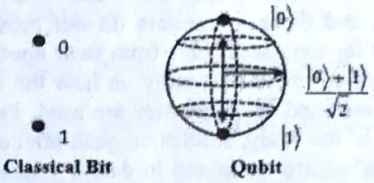

Fig.5 A Qubit is a Quantum bit

Classical conventional computers are built bit by bit with transistors that are either On or Off, quantum computers are built qubit by qubit with electrons in spin-states that are either Up or Down (once measured, of course). And just as transistors in On/Off states are strung together to form the logic gates that perform classical computations in digital computers, electrons in Up/Down spin-states are strung together to form the quantum gates that perform quantum calculations in quantum computers. Yet stringing together individual electrons (while preserving their spin states) is far. This unique feature allows a Quantum Computer achieve speeds which are multiple million folds faster than the Classical Computers of today.

Table 3. Comparative Overview of Classical Computers and Quantum Computers

Data Representation	Bit: 0/1	Qubit: 0/1/Any superposition of 0 and 1		
Data Carriers	Transistor: Open / close	Photon:Polarizat-ion	Electron :Spin	Atom/Ion: Energy level
Encoding	0: close 1: open	0: horizontal 1: vertical S:other directions	0: up 1. down S: other spin	0:ground state 1:excited state S:other states
Data processing	Gates: AND/OR/ NOT/...	Quantum gates: Hardmard/NOT/CNOT/...		

The memory of a classical computer is a string of 0s and 1s, and it can perform calculations on only set of numbers simultaneously. The memory of a quantum computer is a quantum state that can be a superposition of different numbers. A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously. Performing a computation on many different numbers at the same time and then interfering all the results to

get a single answer, makes a quantum computer much powerful than a classical one.

E. *Use of Quantum Computers*

Quantum computer technology is very new and still under development. In this process, different properties can be added to quantum computers according to different usage areas. Quantum computers are not substitutes for conventional computers, and these computers do not provide any advantages for the users apart from their specific use. There is not any extensive study on how the quantum computers are used or where they are used. Therefore; in this part of the study, studies on quantum computers and approaches are examined in detail. The summary of the finding is presented and revealed the following usage areas:

Quantum computers have both positive and negative effects for security mechanisms. These effects can be classified as making the public key cryptosystems used in today's security protocols insecure (SSL, SSH, IPsec), the need for creating reliable cryptosystems instead of classical public key cryptosystems, and designing reliable protocols that can work on quantum computer infrastructure.

Quantum computers are regarded as a solution for such issues as search problems in engineering fields, integer factorization problem, discrete logarithm problem and so on. This solution directly affects the security of the RSA cryptosystem. In addition, new approaches are needed to classify difficult problems. In today's classification, integer factorization problem and discrete logarithm problem are in the NP class and those fall into the P class when quantum computers are considered.

It is thought that quantum approaches can make a difference in all kinds of data processing and security mechanisms that will be applied in application fields such as big data and cloud computing which are related to data processing.

By simulating quantum systems at the atomic level, near realistic results are obtained in the fields, particularly in medicine and the pharmaceutical industry, and information that cannot yet be accessed can be accessed in these fields.

V. CONCLUSIONS

In this work we introduced the basic principles of quantum computers. Our first goal was to introduce the fundamentals of quantum computing. These gates are an essential part of building more complicated quantum circuits performing different calculations. It is important that making a practical quantum computing is still far in the future. One of the main promises of quantum computers has been that they can solve complex problems much faster than classical computers can. We will show that parallel quantum algorithms running in a constant time period are strictly more powerful than their classical counterparts; they are probably better at solving certain linear algebra problems associated with binary quadratic forms. Scientists already think about a quantum computer, as a next generation of classical computers.

ACKNOWLEDGEMENT

The author would like to thank, Dr. Tun Myat Aung who has introduced her to field of computer science. She appreciates his guidance and support, and author value the interesting discussions on various subjects we had. He also has taught her many practical aspects of research.

REFERENCES

[1] Phillip R. Kaye, Raymond Laflamme and Michele Mosca, 'An Introduction to Quantum Computing'2007.

[2] R.P. Feynman, R.B. Leighton, and M. Sands. The Feynman Lectures on Physics, volume III. Addison-Wesley, 1965b.

[3] Quantum Computing: A Short Course from Theory to Experiment, by Joachim Stolze, Dieter Suter, Wiley publications.

[4] Bertels, K., 'Quantum computing: How far away is it?' in High Performance Computing &Simulation (HPCS), 2015 International Conference on, vol., no., pp.557-558, 20-24 July 2015.

[5] Barila, A., 'From classical computing to quantum computing,' in Development and Application Systems (DAS), 2014 International Conference on, vol., no., pp.198-203, 15-17 May 2014.

[6] Kaizer Vizzotto, J., 'Quantum Computing: State-of-Art and Challenges,' in Theoretical Computer Science (WEIT), 2013 2nd Workshop-School on, vol., no., pp.9-13, 15-17 Oct. 2013.

[7] Ying. M., Yuan Feng, 'An Algebraic Language for Distributed Quantum Computing,' in Computers, IEEE Transactions on, vol.58, no.6, pp.728-743, June 2009 doi: 10.1109/TC.2009.13.

[8] Michael A. Nielsen and Isaac L. Chuang, 'Quantum Computation and Quantum Information', 10th Anniversary Edition, Cambridge University Press, 2000.

[9] Yanofsky, Noson S. and Mannucci, Mirco A. Quantum Computing for Computer Scientists. Cambridge: Cambridge University Press, 2008. 978-0-521-879965.

[10] Song Y.Yan, Quantum Computational Number Theory, Springer, 2015.