Quantum Computers : Are They The Future?

Mr. Ajay Dhananjay Dhokale[1], Mr. Atharv Abhijeet Phatak[2], Ms. Swati Yogesh Tiwari[3]
[1, 2 3]Sharad Institute of Technology Polytechnic, Yadrav, Kolhapur, Maharashtra, India

Abstract- *Quantum computing is the new field of science which uses quantum phenomena to perform operations on data. The goal of quantum computing is to find algorithms that are considerably faster than classical algorithms solving the same problem. In this paper we will talk about need of quantum computation and the advantages they offer us in compare with the classical computers. We will discuss what the elements of Quantum computing are. Along with this we will talk about the challenges to Quantum computing.*

Keywords- Quantum computing, phenomena, classical computers.

I. INTRODUCTION

As of 2016, actual quantum computers are yet to be developed, but using small number of bits several experiments are carried out. Research in the field of Quantum Computing is being funded by many military agencies and national governments to develop Quantum Computers. Theoretical and practical research is on for Quantum Computing

Problems solved by classical computers with best possible algorithms available can be solved by using Large-scale quantum computers much more quickly. Any possible probabilistic classical algorithm runs slower than Quantum algorithms like Simon's algorithm.. Any classical computer can make use of quantum algorithm as quantum computation does not violate the Church– Turing thesis.

It is clear that quantum computing has become the new 'race to the moon' pursued with national pride and tremendous investments. For instance, the European Commission is planning to launch a e1 billion flagship initiative on quantum computing starting in 2018 with substantial funding for the next 20 years. This is already a follow-up investment in addition to the 550 million that have already been spent on individual initiatives in order to put Europe at the forefront to what is considered the second quantum revolution. While the first quantum revolution started in the early 1900s with the achievements of Plank, Bohr, and Einstein leading to a theoretical understanding of the behaviour of light and matter at extremely small scales, it is now considered timely to bring the technology to the next maturity level and build real quantum computers in order to exploit their theoretical superiority over today's classical Von-Neumann computers in practical applications.

1.1 The past: Digital computer revolution

Going back in history, the world's first *programmable, electronic, digital computer,* the Colossus, was build by the research telephone engineer Tommy Flowers and used between 1943–1945 by British code breakers in Bletchley Park to decrypt and read secret messages of the German military during World War II. Another pioneer in this field, the Atanasoff-Berry computer, developed between 1937–1942 by John Vincent Antanasoff and Clifford Berry, should not go unnoticed. It deserves the credit of being the world's first electronic digital computer but is was not programmable and only designed to solve linear systems of equations. Next to Colossus, other computing machines like the U.S.-built ENIAC were designed during WWII to break decrypted messages. It took another 20 years before the first commercially available desktop personal computer, the Programma 101, was offered by Olivetti in 1964 at a regular price of $3,200 which would correspond to $20,000 today. The P101 made use of the techniques of its time, transistors, diodes, resistors and capacitors, and was used, e.g., by NASA to plan the Apollo 11 landing on the moon. It took another decade before the advent of microprocessors significantly reduced the costs of personal computers and made them a product for the masses. Further improvements in semiconductor and microprocessor technologies made it finally possible to significantly reduce the size and costs of integrated circuits and integrate all components of a computer into systems-on-a-chip bringing software-programmable computers for $20 per device.

1.2 The present: Quantum computer revolution

Over the last decades, quantum technology has been an exciting toy for scientists but it still has to demonstrate its usefulness in practice. Frankly speaking, industrial interest and long-term investment in quantum hardware and software development can only be achieved if the overall benefits outweigh the immense costs of building and operating quantum computers and their infrastructure as well as developing quantum algorithms and, finally, applications for realistic problem sizes.

It is not a coincidence that the strongest interest in building practically usable quantum computers is largely motivated by their potential to break public-key cryptography schemes such as the widely used RSA scheme. The theoretical superiority of quantum computers in this particular discipline is based on Shor's quantum algorithm for the efficient factorization of large integer numbers into prime factors in polynomial time, whereas the most efficient classical algorithms require sub-exponential time. Appendix A gives a brief overview of the different complexity classes. Variants of the Rivest-Shamir-Adleman (RSA) encryption are used everywhere, for instance, for making secure connections to the Internet, sending text messages between mobile phones and email programmes and for signing contracts and official documents digitally.

It is clear that the ability to read and possibly modify encrypted data and communication is most tempting for intelligence services and hackers alike, thus justifying research on quantum computers and algorithms for this purpose alone. It is, however, not completely unthinkable that quantum computers, like personal computers since the 1980s, will become available for the masses once the technologies for manufacturing and operating quantum hardware has matured and the total cost of ownership have reached an economically acceptable level. That said, we believe that the most probable scenario will be quantum computing as a service as it is already offered by IBM through its "Quantum Experience" servive.

1.3 The possible future: Quantum-accelerated computing as a service

A common challenge of most of today's quantum devices is the need for extremely low operating temperatures near absolute zero, which suggests quantum computing as a cloud service as most promising business model to bring this technology to the endusers. However, this immediately raises the question about the reliability of results received from a quantum computer in the cloud when the communication takes place over an Internet connection that can be decrypted by other quantum computers.

Technology breakthroughs like the Transmon cryogenic 5-qubit devices have heralded the era of practical quantum computers. Researchers worldwide are now focussing on maturing the mass production of multi-qubit devices so as to enable the construction of large-scale quantum computers with millions and billions of qubits, which will be necessary to solve real-world problems. It is, however, equally important to create a quantum ecosystem consisting of a standardized quantum programming language, compilers and debuggers , and a quantum hardware abstraction layer that allows to compile a single quantum program for different target quantum hardware platforms as it is common practice for classical computers. Furthermore, quantum computers need extra effort to detect and correct errors since all qubit technologies available today are very fragile and prone to errors.

In this article we describe possible scenarios of how the advent of practical largescale quantum computers *can* revolutionize scientific computing in the next decades. We thereby leave aspects of quantum hardware and the manual realization of quantum algorithms out of consideration and focus on quantum computers as softwareprogrammable computing devices that enable the development, simulation, testing and analysis of device-independent quantum algorithms. It is our strong belief that quantum computers will not exist as stand-alone machines but need to find their niche in the global computing landscape. The future of scientific computing and quantum computing is, of course, not predictable. We therefore sketch a thinkable scenario that would maximise the impact of quantum computing on scientific computing, namely, quantum-accelerated computing brought to the end-user as a cloud service.

The remainder of this article is structured as follows: In Section 2 we briefly outline the current state of the art in scientific computing and continue with describing the challenges faced by future computing hardware in Section 3. Section 4 gives a very brief introduction into the principles of quantum computing to prepare the reader for the discussion of known quantum algorithms in Section 5. The potential impact of quantum computing on computational sciences is sketched in Section 6 followed by a short outline of possible long-term quantum-enabled applications in Section 7.

II. ELEMENTS OF QUANTUM COMPUTING

A classical computer has worst performance than quantum computer only in few thing so it makes sense to do the bulk of the processing on the classical machine. In general we'll modify a classical computer to design a quantum computer which will have some kind of quantum circuit attached to it and some kind of interface between conventional and quantum logic.

2.1 Bits and Qubits:

These are the building blocks of quantum computing. It gives the description of qubits, gates, and circuits. Quantum computers perform operations on qubits which can be in superposition of state which is an additional property and are same as bits used by classical or digital computer.

In comparison with classical computer a quantum register with 2 qubits can store 4 numbers in superposition simultaneously where classical register with 2 bits stores only 2 numbers and 300 qubit register holds more numbers than the total number of atoms in the universe. This leads to storage of infinite information at the time of computation but we can't get at it. The problem occurs at the time of reading out an output in a superposition state holding so many different values.

Superposition state collapses and we get only one value. This tantalizes us but sometimes it can work as computational advantage for us.

2.2 The Ket | >:

Part of Dirac's notation is the ket (|>). The ket is just a notation for a vector. The state of a single qubit is a unit vector in C2. So,

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

is a vector, and is written as:

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

With

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

And

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

2.3 Entangled States:

Subatomic particles are in entangled state which means that regardless of distance between them they are connected to each other. They show instantaneous effect on measurement with each other. This effect is useful for computational purposes.

Consider the following state (which is not entangled):

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$

it can be expanded to:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle + 0|11\rangle$$

Upon measuring the first qubit (a partial measurement) we get 0 100% of the time and the state of the second qubit becomes:

giving us equal probability for a 0 or a 1.

2.4 Quantum Gates:

Single Qubit Gates:-Just as a single qubit can be represented by a column vector, gate acting on the qubit can be represented by a 2 x 2 matrix. The quantum equivalent of a NOT gate, for example, has the following form:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The only constraint these gates have to satisfy (as required by quantum mechanics) is that they have to be unitary, where a unitary matrix is one that satisfies the condition underneath. This allows for a lot of potential gates.

$$U^\dagger U = I.$$

Multi Qubit Gates :-A true quantum gate must be reversible, this requires that multi qubit gates use a control line, where the control line is unaffected by the unitary transformation. In the case of the CNOT gate, the classical XOR with the input on the b line and the control line a. Because it is a two qubit gate it is represented by a 4 x 4 matrix:

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

2.5 Quantum Circuits:

Quantum circuit is a quantum state which represents one or more qubits on which unitary operators i.e. quantum gates are applied is sequence. We now take a register and let gates act on qubits, in analogy to a conventional Circuit

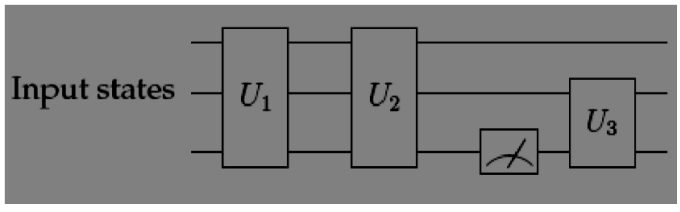

Fig 1: Generalized Quantum Circuit

This gives us a simple form of quantum circuit (above) which is a series of operations and measurements on the state of n-qubits. Each operation is unitary and can be n described by a 2X2 matrix. Each of the lines is an abstract wire, the boxes containing unitary quantum logic gates or it can be a series of gates. Meter symbol is a measurement. Quantum algorithms implementation is all together this gates, wires, input, and output mechanisms.

It is always possible to rearrange quantum circuits so that all the measurements are done at the end of the circuit. Quantum circuits are one way circuits that just run once from left to right, whereas traditional classical circuits contains loops.

2.6 Quantum Computer:

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

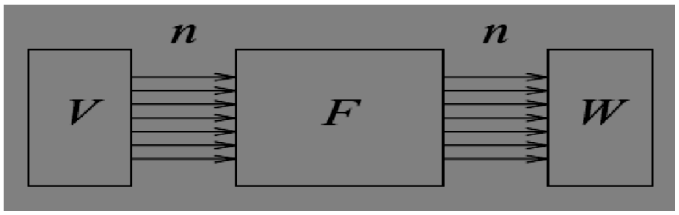

Fig. Basic Structure of Quantum Computer

The input register can be prepared as a superposition of n states, e.g. superposition of all integers from 0 to 2 can be stored in input register. The computer then calculates n in parallel the function applied to all 2 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.

III. QUANTUM COMPUTER ARCHITECTURE

This is similar to the architecture of a building: what type of rooms does it have, how big is each room, where are they located, how are they connected together? To a certain extent, the architecture of a computer depends on the technology you're going to use to build it, just as in with a building, the architecture varies depending on whether it is brick, wood, concrete or steel. And just like the architecture of a building, the architecture of a computer is judged by how useful it is for your purpose.

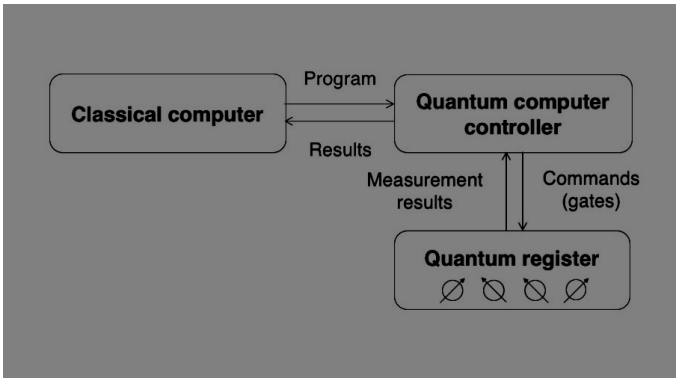

Fig. The basic model of quantum computer architecture

A quantum computer has both classical and quantum parts. The program is (at least for the moment) entirely classical, stored in a classical controller. A quantum algorithm uses both classical and quantum data.

One way to look at the overall system is to treat the quantum part as a *coprocessor* to a classical system. Like the GPU (graphics processing unit) in your desktop or laptop computer, a quantum computer is used to perform specific tasks in the context of a larger program.

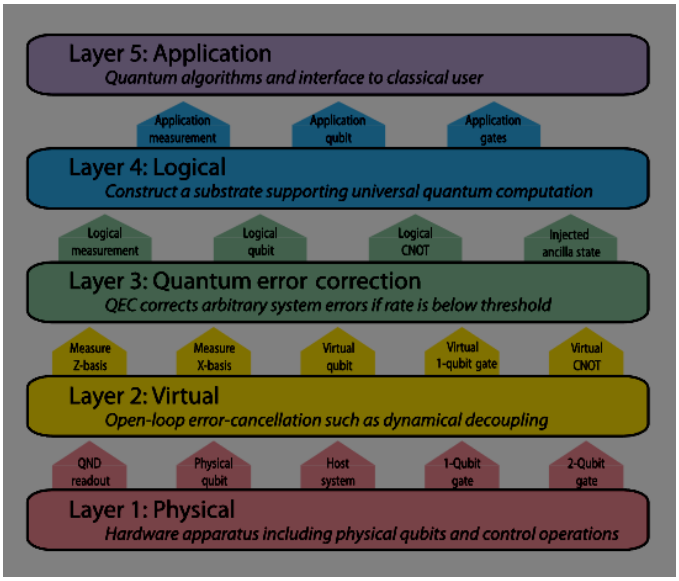

Fig. layered Architecture of Quantum Computer

IV. CHALLENGES TO QUANTUM COMPUTER

The challenges to build a quantum computer are enormous and can be separated in physics and engineering challenges.

The physics challenges are mainly- coherence time of output bit in superposition state and qubits in entangled state and on defining ways to increase the exactness of the qubit and to compensate for the errors that occur during the quantum operations. The engineering challenge can be summarized by the word 'scalability'. Several articles emphasis that due to the above mentioned physical challenges, we will need a very large number of qubits in order to perform any meaningful quantum operation. For instance, in order to apply the famous factorization algorithm developed by Shor, it is expected that for the factorization of 2000 bit number in sufficiently lesser time we require around 5 billion physical qubits. But we know that on today's date we can create and control maximum of 10 physical qubits, it immediately becomes clear that several breakthroughs are needed to achieve the goal of building a quantum computer. This is further illustrated by the speed at which qubit technology needs to evolve to reach the goal of billions of qubits in 30 years from now.

The engineering challenges are thus focused on the scalability by preservation of exponential computing power of qubits which means qubits are needed to be corrected and controlled. Sometimes we need to manipulate the qubit.

The quantum state of the qubit is very fragile because a qubit is in entangled. Any small interaction with the environment causes a superposition state to decohere lead by phase shift error. In addition, the superposition state gets destroyed while measuring the quantum state. This destructive reading as well as the duration and breaking of the superposition state i.e. decoherence time are the vulnerabilities of quantum computing. This qubit behaviour disturbs the correct operation which is a main challenge for any quantum computer.

V. CONCLUSION

Quantum computation promises the ability to compute solutions to problems that, for all practical purposes, are insoluble by classical computers. However, the quantum promise is still a long way from achieving practical realization. The some properties of quantum mechanics that enable quantum computers superior performance also make the design of quantum algorithms and the construction of functional hardware extremely difficult.

We need to imply some solutions to improve the quality of qubit technology by increasing the coherence time of qubits and the speed of quantum operations. We also need to correct the state of the qubit for quantum error correction.

REFERENCE

[1] Quantum computers online available: https://www.sciencedaily.com/terms/quantum_computer.htm

[2] Quantum Computers Wikipedia: https://en.wikipedia.org/wiki/Quantum_computing

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

[4] Paler, A.; Devitt, S.J., "An introduction into faulttolerant quantum computing," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE , vol., no., pp.1-6, 8-12 June 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-ofArt and Challenges," in Theoretical Computer Science (WEIT), 2013 2nd Workshop-School on , vol., no., pp.9-13, 15-17 Oct. 2013

[7] How Does Quantum Computers Work? : **https://www.youtube.com/watch?v=PzL-oXxNGVM**