IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 4, Ser. 2 (July. – August. 2023), PP 24-29
www.iosrjournals.org

Quantum Computing: Fundamentals, Core Principles & Applications

Arun Uniyal
Himalayan Garhwal University
Dept. of Computer Science & Applications
Accenture Solutions Pvt. Ltd.
Manager
Gurugram, Harayana, India

Abstract—

i) *The progression in "Quantum computing" over past many years is significant advancements in the history of quantum computers. It promises next disruptive tech, having various practical applications and implications for corporations and industries. Based on principles of "Quantum Mechanics", i.e., superposition and entanglement, to represent state of data and to perform associated operations. These two core principles enable quantum computers to solve tailored problems significantly faster compared to classical computers.*

ii) *Canada based "D-Wave" is one such quantum computer which is available since a decade. IBM has made significant leap in building an accessible quantum computer available on its cloud platform. Similarly, corporates like Microsoft, Google, Amazon, Intel, NASA etc. have been investing in developing "Quantum Computers" and their applications. "Quantum Computers" are no longer a dream of physicists or / and computer scientists but has opened avenues for information system or computer application researchers.*

iii) *This paper is an attempt to introduce the basics of quantum computing and tries to describe some known quantum applications for non-quantum physicists. It further elaborates the current developments in quantum computing with an introduction to potential application areas and few possible research areas in the field of information technology.*

Keywords *— Quantum physics, Cloud computing, Quantum computer, Quantum gates, Emerging tech, Information systems, Quantum Key Distribution, Shor's Algorithm and Grover's Algorithm*

Date of Submission: 06-08-2023 Date of Acceptance: 16-08-2023

I. INTRODUCTION

With introduction of Quantum Computing in 1980's, various attempts were made to develop quantum algorithms of which the most sought and well-known algorithm is Grover's Database Search algorithm & Shor's integer factoring algorithm. These algorithms have surpassed classical computers and were able to crack the toughest of encryption systems like AES, RSA, ECC etc. The "Quantum Computers" are making significant impact to enterprises and businesses today. Corporates & Government agencies are increasing investments in this area given the potential and promises "Quantum Computers" make to solve tailored / specific problems significantly fast when compared to classical computers.

It is one of the next big disruptions in the technology industry, with promise to impact humans in a positive way with numerous applications / implications for industries or corporations. Based on latest research and projections for the global quantum computing market, it is expected to touch one trillion USD by 2035 and most of the implementations are supposed to come in industries like "Financial Industry", "Chemicals", "Pharma", "Automotive Industry", "Tech", "Healthcare" etc. Big tech organizations like Google, Microsoft, Amazon, IBM had made significant investments at the scale of billions of dollars in R&D of "Quantum Computers" to enable access of these computers on public cloud platforms. Some Government are also making huge interest in this field example China invested 10 billion USD in National Quantum Computing Labs, US Government set aside a budget of 1 billion for the cause and Europe has kept similar scale funds of 1 billion Euros to set the foundation.

Quantum computing relies on Quantum Mechanics to exploit principles of "Superposition" and "Entanglement" to represent data and their operations which are meant for specific complex problems significantly faster compared to conventional computers. Quantum computers are designed to execute tasks in parallel than in sequence. The algorithms can be designed to solve specific problems in fewer steps than conventional computers. Quantum Computers can bring significant advantages in the areas of extreme computations, optimizations, AI, simulations etc.

This paper is an attempt to introduce Quantum Computers for Information systems with its layered architecture. The potential benefits this can bring is by provoking queries in this emerging filed to (i) business models, (ii) process innovations, (iii) solving IT challenges etc.

II. QUANTUM COMPUTERS: LAYERED SYSTEM FRAMEWORK REPRESTATION

Computer manufacturers are trying to create systems which can help in massive processing powers, but all the efforts to create such a system is still under experimentation. The systems created so far are not able to meet the basic parametric requirements viz. computing power, processing speed etc. According to **Howard Aiken** (an American engineer) United States compute requirements will be met by just six electronic digital computers. Similarly, Moore's Law stated that the microprocessor transistors will double in every 18 months resulting in atomic scale microprocessor by year 2020 / 2030. This is represented in the following extrapolation:

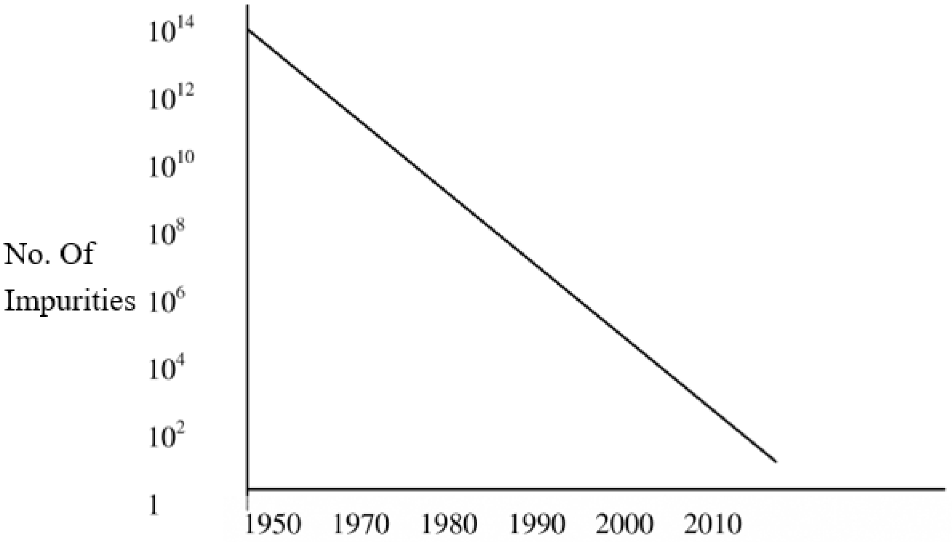


Fig 1: number of electrons required to store a single bit of information.

Quantum computer leverages underlying power molecules and atoms to perform tasks related to processing and memory. Quantum computers are designed to perform certain specific calculations significantly faster than any silicon-based computer or conventional computer. There are several enterprises, which are trying to simultaneously work on an architecture that is scalable. Figure 1: Layered control framework of quantum computer architecture

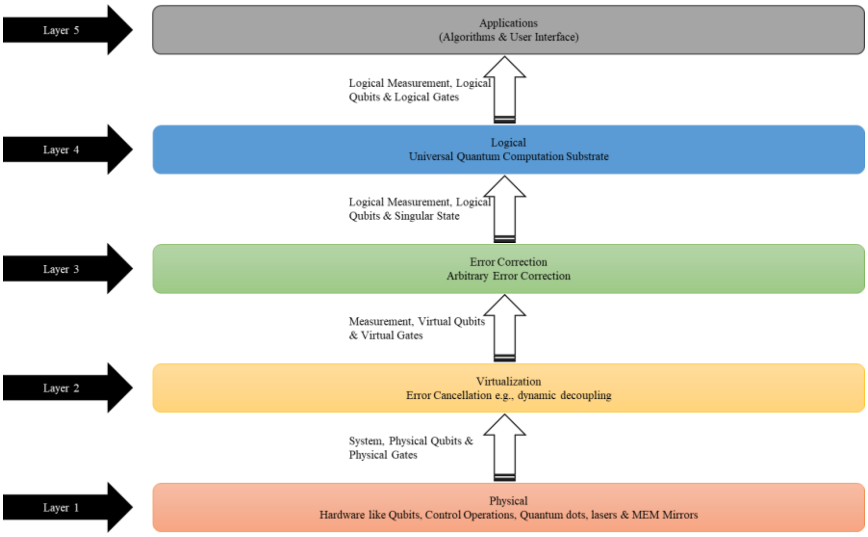

Layer 5
Applications
(Algorithms & User Interface)
Logical Measurement, Logical Qubits & Logical Gates
Layer 4
Logical
Universal Quantum Computation Substrate
Logical Measurement, Logical Qubits & Singular State
Layer 3
Error Correction
Arbitrary Error Correction
Measurement, Virtual Qubits & Virtual Gates
Layer 2
Virtualization
Error Cancellation e.g., dynamic decoupling
System, Physical Qubits & Physical Gates
Layer 1
Physical
Hardware like Qubits, Control Operations, Quantum dots, lasers & MEM Mirrors

Fig 2: quantum-computer framework architecture

The Quantum hardware platform is realized on a specific platform known as QuDOS (quantum dots with optically controlled spins). It is based on electronic spin of qubits within quantum dots which are arranges in a two-dimensional array. This promises a large-scale extension of Quantum systems.

III. QUANTUM GATES & ALGORITHMS

Unlike conventional classical logic gates which operates on a classical bit, quantum gates operate on qubits also known as quantum bits. They are fundamentally based on two key concepts of quantum mechanics viz. ***superposition and entanglement***. Perhaps there is inherent hidden concept which governs the implementation of qubits and that is ***reversibility***. In simple terms all quantum logic gates are ***reversible*** in nature. This implies that all quantum logic gates can be reversed which enables them with one of the core principles of "***never lose information***." Simply put, a qubit retains its position during transition.
Let us now delve into quantum logic gates:

Pauli Gate: named after Wolfgang Pauli, who managed to immortalize two of the best-known principles of modern physics: **the celebrated Pauli exclusion principle** and the dreaded **Pauli effect**. Pauli gates act on only one, qubit at a time which translates to a simple 2 x 2 matrices. The Pauli gates are based on Pauli matrices (i.e., Pauli spin matrices) which are useful for calculating changes to the spin of a electron. Electron spin is the favored property for a qubit in quantum gates. In any event, there's one Pauli gate/matrix for each axis in space (X, Y and Z).

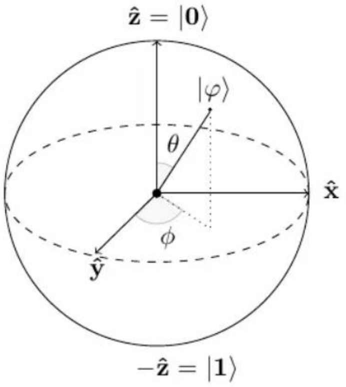
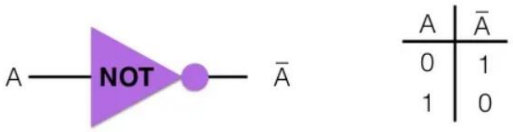

$\hat{\mathbf{z}} = |\mathbf{0}\rangle$
$|\varphi\rangle$
θ
$\hat{\mathbf{x}}$
ϕ
$\hat{\mathbf{y}}$
$-\hat{\mathbf{z}} = |\mathbf{1}\rangle$

Fig 3a: representational plane for a pauli plane

Pauli X Gate*:* This is equivalent to a classical NOT gate which is based on one single operation i.e., negation. This is often known as Quantum Not gate. The X-gate generally reverses the state of a spin-up from |0> of an electron into spin-down state |1> or vice-versa.

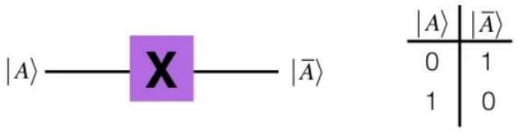
Classical NOT Gate:



A	$\bar{A}$
0	1
1	0

Fig 3b: classical not gate

Pauli X Gate:



$\|A\rangle$	$\|\bar{A}\rangle$
0	1
1	0

Fig 3c: representational plane for a pauli X gate

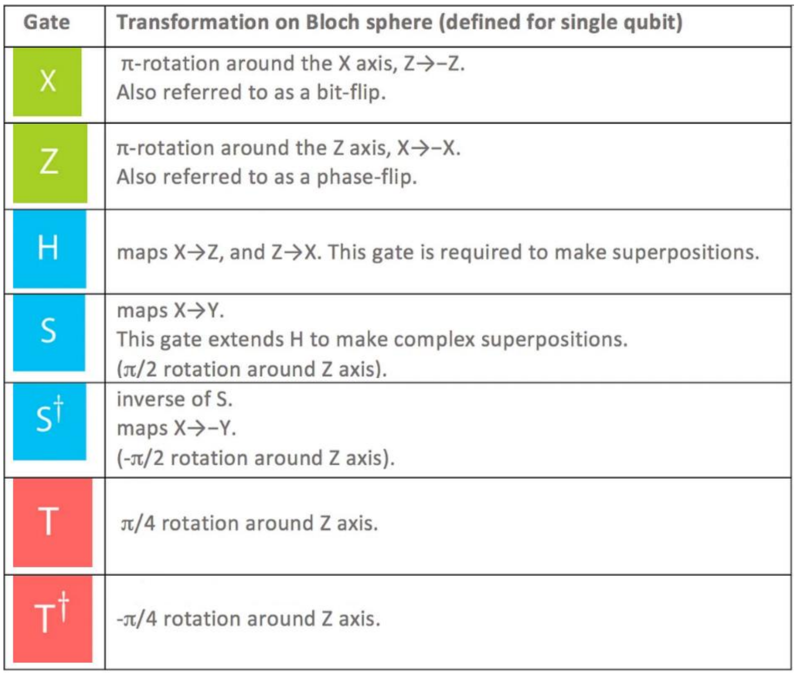
Pauli Y & Z Gates:

a) *Pauli Y gate:* The Pauli Y gate is a multiple of X gate with an I (square root of -1)
b) *Pauli Z gate:* It flips the sign of second entangled state.

The Hadamard or H gate*:* It acts on a single qubit which creates an equal superposition state if given a cimputational basis state. It is represented by Hadamard matrix

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

Most of the quantum functions are performed with basic quantum gates which are represented by the notations listed below:



Gate	Transformation on Bloch sphere (defined for single qubit)
X	π-rotation around the X axis, Z→–Z. Also referred to as a bit-flip.
Z	π-rotation around the Z axis, X→–X. Also referred to as a phase-flip.
H	maps X→Z, and Z→X. This gate is required to make superpositions.
S	maps X→Y. This gate extends H to make complex superpositions. (π/2 rotation around Z axis).
$S^\dagger$	inverse of S. maps X→–Y. (-π/2 rotation around Z axis).
T	π/4 rotation around Z axis.
$T^\dagger$	-π/4 rotation around Z axis.

Fig 4: main quantum logic gates

To find an algorithm which should be useful for quantum computers relies on framing it in such a way that the likelihood of determining the anticipated results is exploited. Though the outcome from a quantum computer may be exponentially large number of explanations, we are generally interested in a minor subdivision of these explanations. To find such a subset without running the entire algorithm many a times is the art of constructing a quantum algorithm. The most important quantum algorithms are highlighted below:

- **Shor's algorithm**: This is commonly known as integer factorization algorithm. Using this algorithm, we can factorize the integers at a lightning-fast speed which is exponentially faster than any known conventional algorithm used in classical computers.
- **Grover's algorithm**: This is generally known as quantum search algorithm. It is used to find an unstructured dataset or an unordered list of objects. To find an item in a database of a particular size Y, it takes an average of Y/2 objects to find it. With use of this algorithm, the same objective can be achieved within an average√N steps. If the dataset is comparatively large this is a comparatively fast and is called a quadratic speedup.
- **HHL (Harrow Hassidim Llyod)**: It is a quantum computing algorithm for linear system of equations. On average this algorithm is capable of estimating the results of any function of a solution z of a linear system (Sz = k), where S corresponds to a matrix and k to a vector.

IV. APPLICATIONS OF QUANTUM COMPUTING

The innovation in technology has taken quantum computing to reality which has created a plethora of opportunities across industries. It is the latest innovation which has open avenues in the field of technology trending towards extreme computations and accelerated outcomes for high volume data. The feasibility to realize a quantum computer will allow industries to implement use cases which were not possible with classical conventional computers. Some of the potential applications of quantum computers are highlighted below with an endless list for possibilities for use of this technology beyond the suggested use cases.

1. **Real time Traffic flow management**: Today we are facing a lot of challenges to travel over road. The real time management of traffic is a nightmare with the use of conventional computers. A part of the problem is solved using some latest technology developments around AR/VR where real time violators get a ticket, but to resolve the entire process need a massive computational effort. This can be resolved once the quantum computers are commonly available for use.
2. **Drug Design & Development**: Drug development is a lengthy and long process which is based on the process of trial and errors. Based on various research, it is believed that the process of drug discovery can be run through quantum computers which can better understand these drugs and correlation to humans in terms of its impact, thus saving enormous time and money.
3. **Cybersecurity**: With digitization, the number of cyberattacks are increasing every day. Quantum computing is a blessing in disguise, which will help to deploy large machine learning models to identify the threats and address this issue.
4. **Quantum Cryptography**: The process to encrypt and protect data in a way that only parties having correct secret code or key can use the message is called **Cryptography**. Quantum Cryptography uses Quantum Mechanics to secure and transmit data which can never be hacked due to inherent qubit properties where it can’t be copied or measured.
5. **Weather Forecasting**: The challenges with traditional computers in the field of weather forecasting is change in weather itself by the time the system is able to forecast or predict outcomes. Given Quantum Computers are capable of handling large volumes of data by cutting down the processing time, it will help to benefit this field.
6. **Financial Models**: The financial problems take a lot of time to generate outcomes in any conventional classical computer. Simulations using Monte Carlo methods consumed a lot of time and complex calculations which can be accelerated with use of quantum computers with ease.
7. Some other areas where Quantum Computers can help are:

a. Discovery of New Materials
b. Development of Clean Fertilizers
c. Task optimizations
d. Extreme data processing or computational requirements
e. Search & Optimizations
f. Complex network architecture in Algebra
g. Large scale simulations etc.

V. QUANTUM COMPUTERS AND THE FIELD OF INFORMATION TECHNOLOGY

The latest research, development, and progression in the field of photon-based data storage and calculations has opened multiple avenues for information systems. The field of Quantum Computing is now seeming a reality where large enterprises were able to simulate upto 500 qubits and the advancement is looking promising where IBM may release a 1000 qubit quantum computer by end of 2023. While the filed is still emerging, the infrastructure is made available to end consumers over various cloud platform. Anyone, with little to no investment can experiment with these quantum computers over a cloud channel through available services from these vendors. Some of the cloud quantum computing vendors are:

1) ***IBM****:* enabled through IBMs Quantum Cloud (IBM Q)
2) ***Google****:* The Quantum AI lab from Google is providing access to NISQ (Noisy Intermediate-Scale Quantum) processors and simulators for researchers.
3) ***XANADU:*** The canada based Quantum Cloud provider enables access to three fully programmable photonic computers.
4) ***Rigetti***: The QCS (Quantum Cloud Services) offered by Rigetti is enabled via Forest SDK which is capable of simulating the code by QCS through programs in Quil.
5) ***AWS****:*Amazon Braket is a fully managed cloud service offered by AWS that helps users to get started with Quantum Computing. It enables end users to cloud environment which help them to develop, experiement and design quantum algorithms. This can be tested on simulated quantum computers and then can be executed on quantum system hardware of user’s choice.
6) ***Microsoft****:* Azure Quantum service from Microsoft that brings together most innovative quantum computing and optimization solutions into a single service.
7) ***Qutech****:* Quantum Inspire from Qutech is being the first platform in Europe to provide cloud based quantum computing to two hardware chips.
8) ***QC Ware****:* The FORGE cloud platfrom provides access to D-Wave hardware alongside simulators from Google & IBM and is flexible for users to deploy their own quatum algorithms.

9) ***D-Wave****:* Leap Quantum Cloud Service delivers realtime immediate access to underlying quatum computer and associated services for performance and scalability.
10) ***AQT:*** Working on general-purpose quantum information processors.
11) ***Oxford Quantum Circuit****:*offered on a private cloud, it is the first company to offer Quantum Computing as a service to enterprises.
12) ***Alibaba Group****:* Available via Quantum Computing Cloud Platform, the Aliyun service is under experimentation to offer Quantum Computing.
13) ***Collaboration between Honeywell & Cambridge****:* Quantinuum is a quantum cloud computing supplier offering, hardware-diverse software development platform, an operating system, real-world applications, and high-performing quantum systems.

VI. FUTURE WITH QUANTUM COMPUTERS

The advancement in computing have promised a big leap in the field of quantum computing. With services offered by some big enterprises enabling use of initial quantum computing setup over cloud, the avenues are enormous. Over the past couple of years, the quantum computing infrastructure has promised significant development moving from a preliminary 2-digit qubit computer to a setup of over a 1000 qubit by end of 2023. It is a rapidly developing field, and future is full of breathtaking possibilities. There are enormous potentials for quantum computing in the future:

1) Improved Quantum Hardware
2) Applications in various industries
3) Hybrid Classical-Quantum Computing infrastructure
4) Quantum Networks
5) Extreme Computational capabilities offered by Quantum Computing
6) Talent gap and change

VII. CONCLUSION

This paper is an attempt to extend the theory of "***extreme data processing capabilities in real time***" through the world of quantum computing. While this is just an introduction to this new field with potential use cases or applications in various industries, the possibilities are enormous. As we advance the development in this field, this filed will further grow and expand possibilities beyond the current simulations or initial research into few. As more enterprise or government start investing into filed of quantum, it will be accessible to majority of the population at an optimal cost. The field also offers an interlock through cross communication between Quantum & Conventional systems offering possibilities beyond thoughts.

REFERENCES

[1] Sujeti Das, Top Applications Of Quantum Computing Everyone Should Know About At Https://Analyticsindiamag.Com/Top-Applications-Of-Quantum-Computing-Everyone-Should-Know-About/

[2] James Dargan, 5 Crucial Quantum Computing Applications & Examples, Https://Thequantuminsider.Com/2023/05/24/Quantum-Computing-Applications/#:~:Text=3.-,Quantum%20Computing%20Application%20in%20Machine%20Learning%20(ML),Advantage%20in%20Learning%20from%20Experiments%E2%80%9D

[3] Sahil Pawar, Top Applications Of Quantum Computing, Https://Analyticsdrift.Com/Top-Applications-Of-Quantum-Computing/

[4] Apporva Bellapu, Top 10 Unexpected Applications Of Quantum Computing In 2023, Https://Www.Analyticsinsight.Net/Top-10-Unexpected-Applications-Of-Quantum-Computing-In-2023/

[5] Cody Jones Et Al, Layered Architecture For Quantum Computing, Https://Journals.Aps.Org/Prx/Pdf/10.1103/Physrevx.2.031007

[6] Https://Quantumcomputing.Stackexchange.Com/Questions/9067/How-Is-A-Quantum-Computer-Programmed

[7] IBM, What's Next In Quantum Is Quantum-Centric Supercomputing, Https://Research.Ibm.Com/Quantum-Computing

[8] Sergey Bravyi Et Al, IBM Study Charts Future Of Superconducting-Based Quantum Computing, Https://Www.Hpcwire.Com/2022/10/19/Ibm-Study-Charts-Future-Of-Superconducting-Based-Quantum-Computing/

[9] IBM, The Era Of Quantum Utility, Https://Www.Ibm.Com/Quantum

[10] Dinesh C Verma Et Al, Software Architecture For Operation And Use Of Quantum Communications Networks, Https://Arxiv.Org/Ftp/Arxiv/Papers/2305/2305.20013.Pdf

[11] Matt Lourens Et Al, Hierarchical Quantum Circuit Representations For Neural Architecture Search, Https://Www.Nature.Com/Articles/S41534-023-00747-Z

[12] Bacciagaluppi Et Al, The Uncertainty Principle, Https://Plato.Stanford.Edu/Entries/Qt-Uncertainty/

[13] Jason Roell, The Need, Promise, And Reality Of Quantum Computing, Https://Jasonroell.Com/2018/02/01/The-Need-Promise-And-Reality-Of-Quantum-Computing/,

[14] Jason Roell, Demystifying Quantum Gates — One Qubit At A Time, Https://Towardsdatascience.Com/Demystifying-Quantum-Gates-One-Qubit-At-A-Time-54404ed80640#:~:Text=Classical%20gates%20operate%20on%20classical,Classical%20gates%3A%20superposition%20and%20entanglement

[15] Https://En.Wikipedia.Org/Wiki/Qiskit

[16] Https://En.Wikipedia.Org/Wiki/Quantum_Logic_Gate#:~:Text=Unlike%20many%20classical%20logic%20gates,Having%20to%20use%20ancilla%20bits.