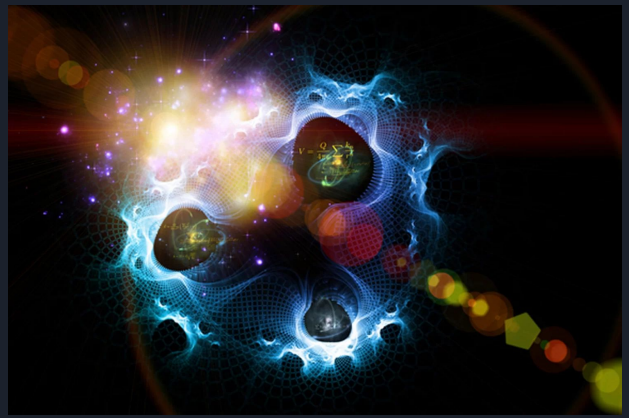
Quantum Gates & Future of QUANTUM COMPUTING

Made by Ajitesh Nair
Eshwar A R
Yash Raj

What do we Understand by the word QUANTUM?

QUANTUM is a LATIN word meaning *AMOUNT* and in the modern understanding, means the SMALLEST POSSIBLE DISCRETE UNIT of any physical property such as energy & matter.



What is QUANTUM COMPUTING?

Quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. A quantum computer is used to perform such computation, which can be implemented theoretically or physically.

The field of quantum computing is actually a sub-field of quantum information science, which includes quantum cryptography and quantum communication.

QUANTUM COMPUTING fundamentals

All computing systems rely on a fundamental ability to store and manipulate information. Current computers manipulate individual bits, which store information as binary 0 and 1 states. Quantum computers leverage quantum mechanical phenomena to manipulate information. To do this, they rely on quantum bits, or qubits.

TIMELINE of QUANTUM COMPUTING

-> Birth of QUANTUM COMPUTING dates back to 1960s. When STEPHEN WEISNER introduces "**Conjugate Coding**"

What is CONJUGATE CODING?

Conjugate Coding is the Cryptographic tool. It has two application as stephen described one for QUANTUM CODING along with a method for creating fraud-proof banking notes.

The application where the concept was based from was a method of transmitting multiple messages in such a way that reading one destroys the others. This is called **“quantum multiplexing”** and it uses photons polarized in conjugate bases as "qubits" to pass information. Conjugate coding also is a simple extension of a random number generator.

1970s

1973

Alexander Holevo publishes a paper showing that n qubits cannot carry more than n classical bits of information (a result known as "Holevo's theorem" or "Holevo's bound").

Charles H. Bennett shows that computation can be done reversibly.

1975

R. P. Poplavskii publishes "Thermodynamical models of information processing" which showed the computational infeasibility of simulating quantum systems on classical computers, due to the superposition principle.

1976

Polish mathematical physicist Roman Stanisław Ingarden made the first attempts at creating a quantum information theory

1980s

Paul Benioff describes quantum mechanical Hamiltonian models of computer and application to TURING MACHIINES and proposes first recognisable theoretical framework for a quantum computer

Richard Feynman observes that it is impossible in general to simulate an evolution of a quantum system on a classical computer in an efficient way & proposes a basic model for a quantum computer that would be capable of such simulations

Tommaso Toffoli introduces the reversible Toffoli gate which provides a universal set for reversible classical computation.

William Wootters and Wojciech Zurek and independently Dennis Dieks prove the no-cloning theorem.

Charles Bennett and Gilles Brassard employ Wiesner's conjugate coding for distribution of cryptographic keys.

1990s

Artur Ekert at the University of Oxford, invents entanglement-based secure communication.

Dan Simon invents an oracle problem for which a quantum computer would be exponentially faster than a conventional computer. This algorithm introduces the main ideas which were then developed in Peter Shor's factorization algorithm.

“**Peter Shor**”, at AT&T's Bell Labs in New Jersey, discovers an important algorithm. It allows a quantum computer to factor large integers quickly. It solves both the factoring problem and the discrete log problem. Shor's algorithm can theoretically break many of the CRYPTOSYSTEM in use Today

Limitations of CLASSICAL COMPUTATION

There are several physical and practical limits to the amount of computation or data storage that can be performed with a given amount of mass, volume, or energy.

1. There's an upper bound on how much information you can fit in a given physical space.

2. There's a lower bound on how much energy you have to use per unit of computation

3.) There's an upper bound on how fast a computation can be.

PROBLEMS SOLVED BY QC

QC can store almost 10,000 time more than today's system

The fundamental reason being that quantum computers work (mostly) via unitary operations. A unitary operation is a reversible operation, or, in other words, an operation during which no information is lost to the environment. Such an operation is basically "perfectly" energy efficient. They use PHOTNIC CHIPS which are extremely energy efficient

Roughly A QC is 100 million times faster than any normal or classical computers Today

Quantum Gates

- In quantum computing and specifically the quantum circuit model of computation, a **quantum logic gate** (or simply **quantum gate**) is a basic quantum circuit operating on a small number of qubits. They are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits.
- Unlike many classical logic gates, quantum logic gates are reversible.

Qubits

- In quantum computing, a **qubit** or **quantum bit** (sometimes **qbit**) is the basic unit of quantum information—the quantum version of the classical binary bit physically realized with a two-state device.
- n a classical system, a bit would have to be in one state or the other. However, quantum mechanics allows the qubit to be in a coherent superposition of both states/levels simultaneously, a property which is fundamental to quantum mechanics and quantum computing.

Various Quantum Gates

- **Hadamard (H) gate**
- **Pauli-X gate**
- **Pauli-Y gate**
- **Pauli-Z gate**
- **Phase shift gate**
- **Swap gate**

Hadamard gate

- The Hadamard gate is a single-qubit operation that maps the basis state
- $|0\rangle$ to $(|0\rangle+|1\rangle)/(2^1/2)$
  and
- $|1\rangle$ to $(|0\rangle-|1\rangle)/(2^1/2)$

thus creating an equal superposition of the two basis states.

$$H = 1/(2^{1/2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The Hadamard gate can also be expressed as a 90° rotation around the Y-axis, followed by a 180° rotation around the X-axis.

Controlled (cX cY cZ) gates

- Controlled gates act on 2 or more qubits, where one or more qubits act as a control for some operation. For example, the controlled NOT gate (or CNOT or cX) acts on 2 qubits, and performs the NOT operation on the second qubit only when the first qubit is |1> , and otherwise leaves it unchanged.

Toffoli (CCNOT) gate

- The Toffoli gate, named after Tommaso Toffoli; also called CCNOT gate ;is a 3 bit gate. If the first two bits are in state|1> it applies NOT on the third bit , else it does nothing.

The Pauli gates

- The Pauli gates are named after Wolfgang Pauli.

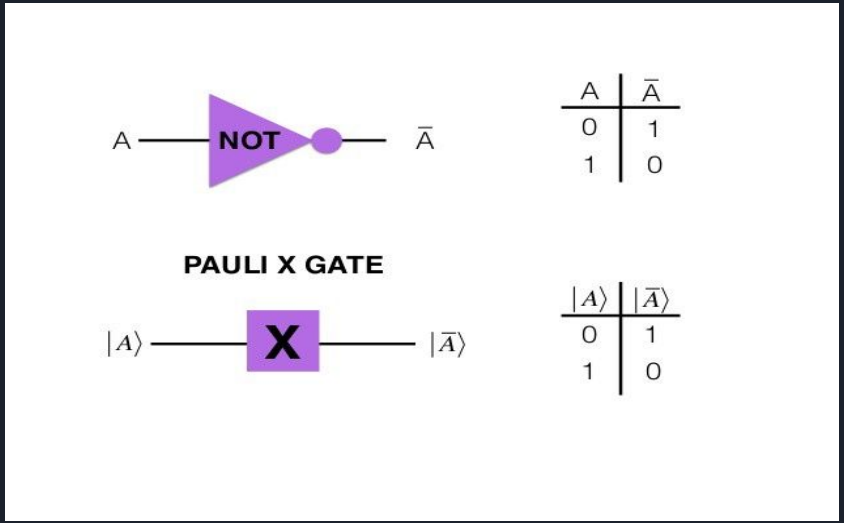
- The Pauli gates are based on the better-known Pauli matrices (aka *Pauli spin matrices)* which are incredibly useful for calculating changes to the spin of a single electron

- In mathematical physics and mathematics, the **Pauli matrices** are a set of three 2 × 2 complex matrices which are Hermitian and unitary.
- They are usually indicated by the Greek letter sigma (σ)

There are 3 types of Pauli’s gates
The Pauli X - gate
The Pauli Y – gate
The Pauli Z – gate

The Pauli X-gate

- The Pauli X-gate corresponds to a classical NOT gate. For this reason, the X-gate is often called *the quantum NOT gate* as well.



Pauli-Y gate

- The Pauli-Y gate acts on a single qubit. It equates to a rotation around the Y-axis of the Bloch sphere by pi radians. It maps $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$ It is represented by the PauliY matrix:

The Pauli spin matrices

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Pauli-Z (R pi) gate

- The Pauli-Z gate acts on a single qubit. It equates to a rotation around the Z-axis of the Bloch sphere by Pi radians. Thus, it is a special case of a *phase shift gate* with phi=pi . It leaves the basis state |0> unchanged and maps |1> to|-1> . Due to this nature, it is sometimes called phase-flip. It is represented by the Pauli Z matrix:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Phase shift ( ) gates

- This is a family of single-qubit gates that leave the basis state unchanged and map to . The probability of measuring a or is unchanged after applying this gate, however it modifies the phase of the quantum state. This is equivalent to tracing a horizontal circle (a line of latitude) on the Bloch sphere by radians. where is the *phase shift*.

CURRENT developments in QC

A list of public companies with known efforts in Quantum Computing.

Accenture

Accenture Labs has formed a research group that is partnering with 1QBit to explore potential use cases for quantum computing by industry. They have recently publicized some work they are doing with 1QBit and Biogen to apply quantum computing to accelerate drug discovery

Airbus Group

Airbus has set up a new research group in Newport, Wales to explore the potential use of quantum computing in aerospace activities. Potential applications could include searching big data, designing air vehicles and systems, designing new materials, and debugging complex software.

Alibaba Group
Alibaba Quantum Computing Laboratory in Shanghai, China combines the technical advantages of Alibaba in classical calculation algorithms, structures and cloud computing with those of the Chinese Academy of Science in quantum computing, quantum analog computing and quantum artificial intelligence. It is conducting research in quantum theory with a view towards discovering ground-breaking security techniques for e-commerce and data centers, as well as to enhancing computing performance.

Archer Exploration Limited
Archer Exploration Limited, vision is to develop and integrate advanced materials for use in reliable energy, human health, and quantum technologies for the betterment of society.

IBM

IBM's approach appears to be based upon utilization of superconducting circuits coupled with error correction. In April 2015, they announced an advance with a circuit that can detect both bit-flip and phase-flip errors together. Most recently in December 2015, IBM was awarded an iARPA grant to use this technology under the Logical Qubits (LogiQ) program to overcome the limitation of current quantum systems by building a logical qubit from a number of imperfect physical qubits.

Although Intel previously did not have any research efforts devoted to quantum computing they did just commit to provide
QuTech, the quantum research institute of Delft University of Technology (TU Delft) and the Dutch Organisation of Applied
Research (TNO), with $50 million in funding and provide engineering support over a ten years collaboration to support
their efforts. A press kit describing Intel's activities in quantum computing can accessed here. Many people have been
forecasting that Moore's Law will end at some point and it seems that Intel wanted to hedge their bets on this

Lockheed Martin

One of the unique areas that Lockheed has researched is the usage of quantum computers for verification and validation of complex software such as flight control systems. Lockheed is also a participant in the iARPA QEO (Quantum Enhanced Optimization) for quantum annealing as well as an industry partner in the NSF Enabling Practical Scale Quantum Computing programs.

Microsoft Quantum Architectures and Computation Group (QuArC)

Microsoft's QuArC group is focused on designing software architectures and algorithms for use on a scalable, fault-tolerant quantum computer. They collaborate with a number of universities worldwide and have published many technical papers in the past several years. One of the most significant results of their efforts is the release of the Language-Integrated Quantum Operations: LIQUi|> software architecture and tool suite.

APPLICATION OF QC

- Artificial Intelligence

A primary application for quantum computing is artificial intelligence (AI). AI is based on the principle of learning from experience, becoming more accurate as feedback is given, until the computer program appears to exhibit “intelligence.”
This feedback is based on calculating the probabilities for many possible choices, and so AI is an ideal candidate for quantum computation. It promises to disrupt every industry, from automotives to medicine, and it’s been said AI will be to the twenty-first century what electricity was to the twentieth.

For example, Lockheed Martin plans to use its D-Wave quantum computer to test autopilot software that is currently too complex for classical computers, and Google is using a quantum computer to design software that can distinguish cars from landmarks. We have already reached the point where AI is creating more AI, and so its importance will rapidly escalate.

Molecular Modeling

Another example is precision modeling of molecular interactions, finding the optimum configurations for chemical reactions. Such “quantum chemistry” is so complex that only the simplest molecules can be analyzed by today’s digital computers.

Chemical reactions are quantum in nature as they form highly entangled quantum superposition states.

But fully-developed quantum computers would not have any difficulty evaluating even the most complex processes. Google has already made forays in this field by simulating the energy of hydrogen molecules. The implication of this is more efficient products, from solar cells to pharmaceutical drugs, and especially fertilizer production; since fertilizer accounts for 2 percent of global energy usage, the consequences for energy and the environment would be profound

Particle Physics

Models of particle physics are often extraordinarily complex, confounding pen-and-paper solutions and requiring vast amounts of computing time for numerical simulation. This makes them ideal for quantum computation, and researchers have already been taking advantage of this.

HOW will QC design our FUTURE

Quantum computing has the potential to shape a range of different industries and sectors. A few examples would include:

Healthcare - Research into certain diseases may be aided through complex simulations of organs and tissues. Quantum computers could also have the ability to analyse DNA to determine the genetic heritage of a person to help provide more personalised treatment.

Scientific Research - Nasa is already using their D-Wave quantum computer to analyse vast amounts of data captured by telescopes in the Kepler search for exoplanets. It could also be used to simulate chemical reactions to improve manufacturing processes or to simulate the Big Bang to find out more about the origins of the universe. Machine Learning and AI - Essentially the huge amount of power provided by quantum computing could rapidly advance these areas, driving forward technologies such as image recognition or self-driving cars.

THANK YOU