Quantum Computing – AI Guild

Rajprasath Subramanian

Agenda

What is Quantum computing and why it is relevant now

Basic concepts of quantum computing

Quantum Algorithms

Business opportunity for quantum computing

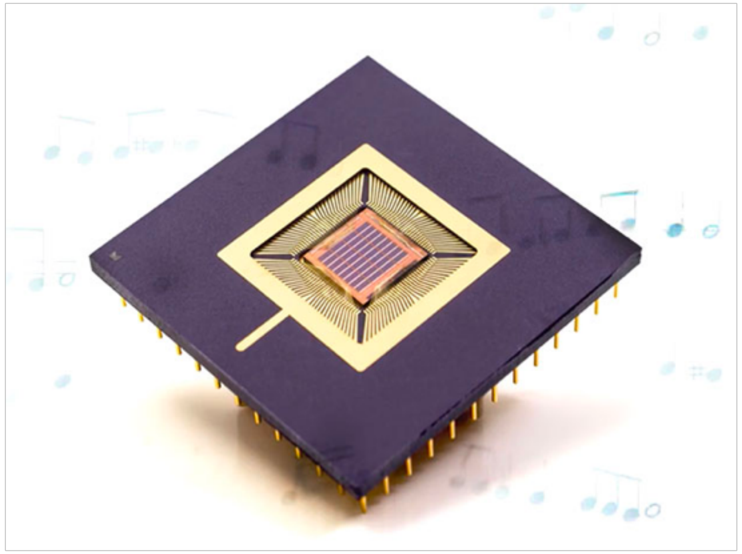
Companies status with Quantum

Where to start

Computing Taxonomies

- **Classical**
  - Silicon-based computing where computations are performed via a set of electrical transmissions
  - basis is binary (0 or 1)
  - Central processor made up of million of transistors that switches on and off to transfer and process data

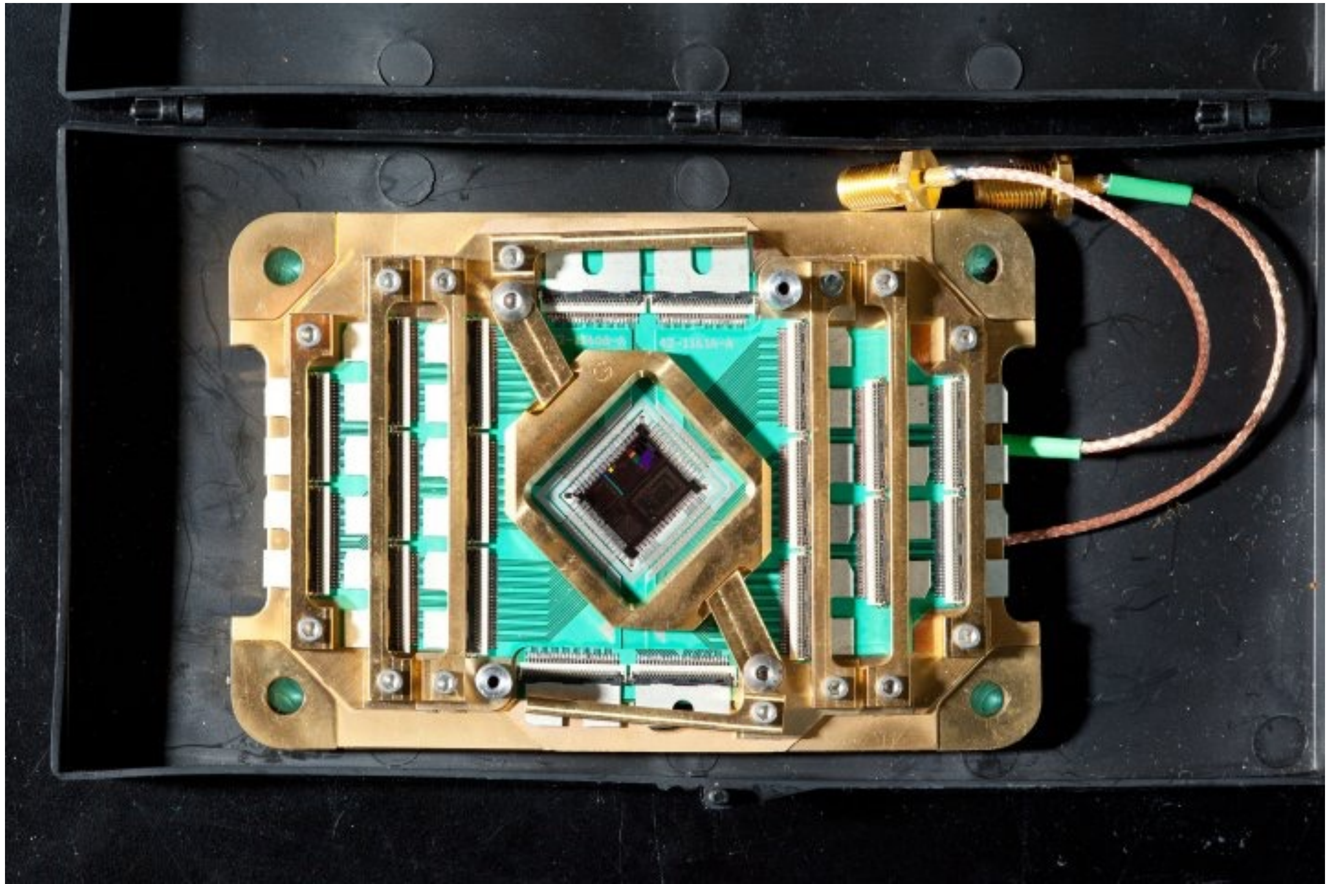
- **Neuromorphic**
  - Ability of a computer to think like a human brain, which simplistically speaking is network of neurons
  - enabled by neuromorphic chips-contains small computing units corresponding to artificial neurons
  - computing units cannot perform a lot of different operations. They have just enough power to perform the mathematical function of a single neuron.
  - Suitable for AI jobs



Computing Taxonomies

- **Quantum computing**
  - A new computational technology at the intersection of quantum physics and computer science, with the potential to provide significantly higher computing performance for specific types of problems.
  - Qubits are the building blocks of quantum computers

Quantum Computing = Math + Physics + Computer Science



What kind of problems that Quantum computers solve today

Quantum computers can solve two types of problems extremely well:

- **Problems with vast amounts of variables and**
- **Problems with huge numbers of possible answers.**

These are exactly the types of problems that many organizations are increasingly struggling with to develop breakthrough solutions in their markets or research fields (e.g., develop currently inconceivable new materials, discover pharmaceutical molecules currently too complex, and optimize transportation routing that no HPC or supercomputer deployment can solve today).

Different application domains of Quantum today are :

***Quantum Computing** – Solving optimization problems and ML

***Quantum Communication** – Quantum Cryptography

***Quantum Sensing-** Performing highly sensible measurements (Ex: Quantum Gravimeter,Gyroscope,Gradiometer)

***Quantum Simulation-** Simulating Molecules, Materials discovery etc

Quantum Communication:

- Uses quantum physics and quantum mechanics (i.e., superpositioning) to protect (using quantum cryptography) and transfer data (using teleportation) via quantum networks. Data transfer happens by Physics (Ex: Quantum Key Distribution)

- Public key cryptography is the foundation of secure communication on the internet. Modern eCommerce and internet banking as well as other forms of secure internet communication are all based on TLS, which in turn uses public-key cryptography. The latter is based on the computational hardness of problems such as large factorization.

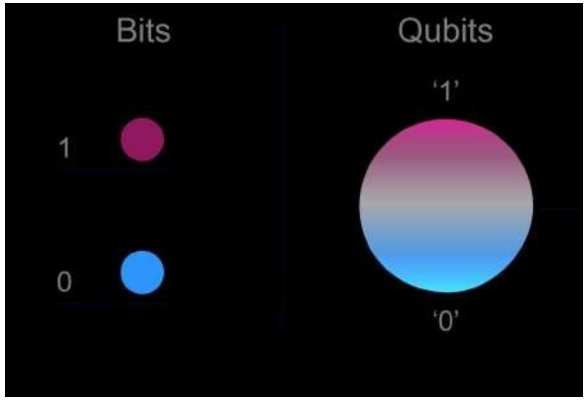
- Shor’s algorithm with scalable quantum computer would break all of modern public-key cryptography. This is resulting in developing quantum-safe classical cryptography (also known as post-quantum cryptography).

- Quantum information theory is also expected to revolutionize network communication by providing provable secure cryptography (via quantum key distribution) and efficient information transfer (via quantum teleportation and super-dense coding)

Three important properties of Quantum phenomena

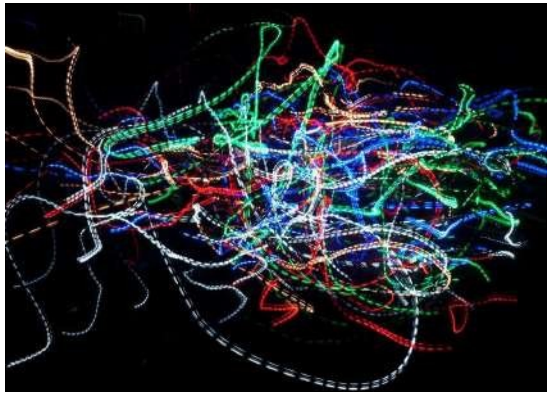
Superposition

parallelization



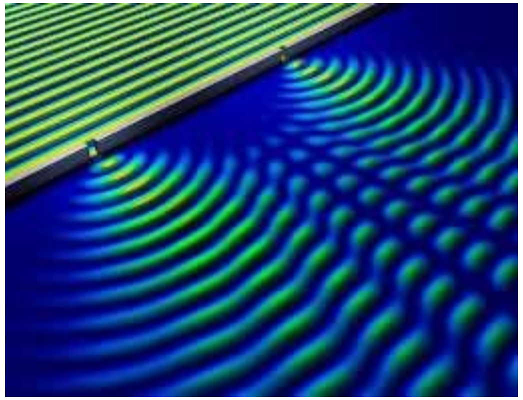
Entanglement

correlations



Quantum interference

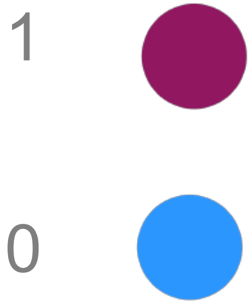
sieving results

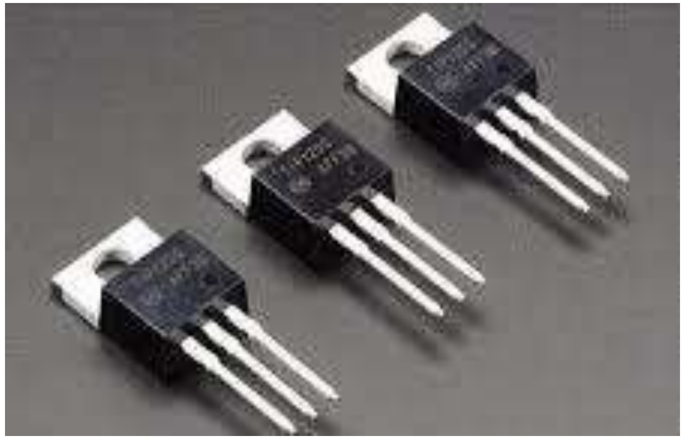


Source : Classiq and https://ieee.nitk.ac.in/blog/future-of-computing-quantum-computing/

Bits & Qubits

Classical computing-Bits

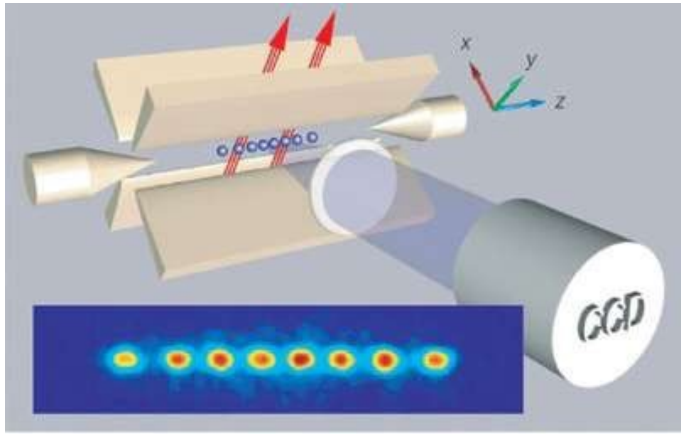




Source:Classiq

$|0\rangle$ and $|1\rangle$ are bit 1 and bit 2

Quantum computing-QuBit



Source:Classiq

$a|0\rangle + b\,|1\rangle$ are bit 1 and bit 2

1 Qubit can be in two states where a and b indicates how much of |0> and |1> in the system

"a" and "b" here are amplitude and their squares are probabilities of finding the state in the system (probability amplitude)

Qubit a|0> + b|1> is linear combination of states |0> and |1> which means they are in superposition

The Hadamard Gate

$$|\psi_1\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

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

$$|\psi_2\rangle = H|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

- In this example we have moved to a state of "superposition" of $|0\rangle$ and $|1\rangle$.

Source:Classiq

More than One qubits

Qubit system is the all applicable states in superposition

For 2 qubits, states will be

a|00> + b|01> + c|10> + d|11>

Where a,b,c,d are amplitudes

This may lead to something called “Entanglement” in coming slides ☺

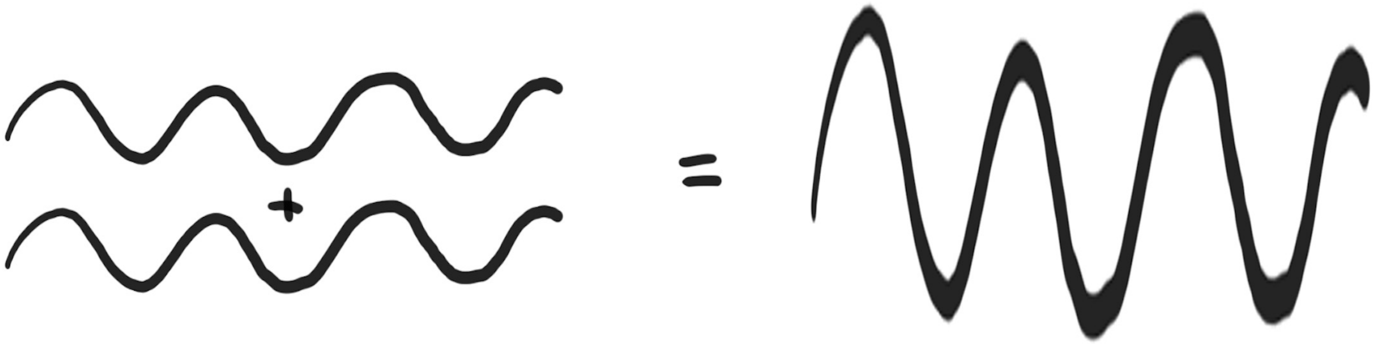
Similarly for 3 qubits, there will be 8 possible states

a|000> + b|001> + c|010> + d|011> +a|100> + b|101> + c|110> + d|111>

Amplitude can be positive or negative . As a result, interference happens

Interference (Property of waves)

CONSTRUCTIVE INTERFERENCE



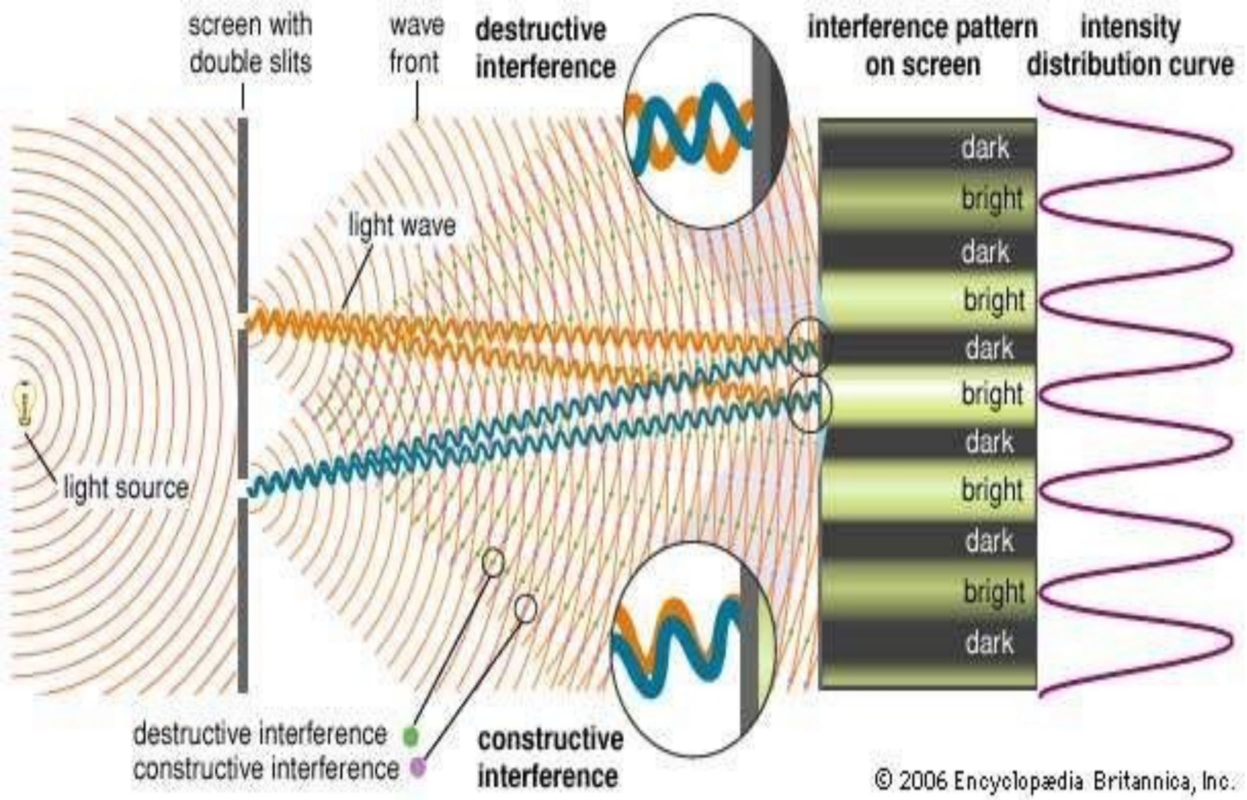
Amplitude can add up - Constructive interference

DESTRUCTIVE INTERFERENCE

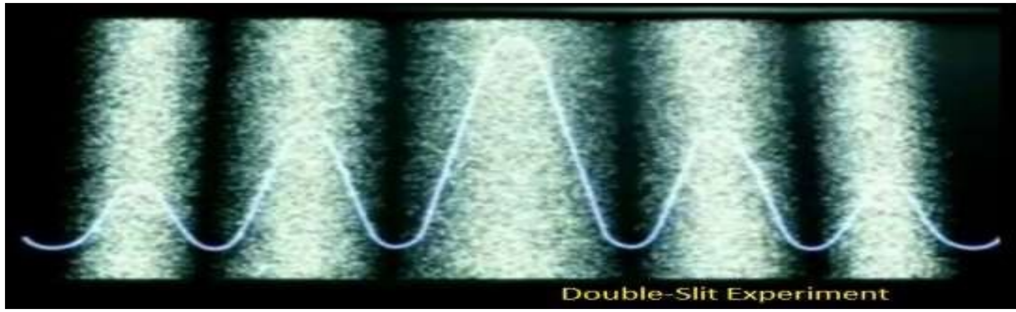
Amplitude can negate each other - Destructive interference

Double Slit Experiment - Interference

Famous double slit experiment is the direct manifestation of Quantum Interference



Result of Interference



So the things that we observe(Measurement) are the results of interference (Results from the constructive interference)

Entanglement

For 2 qubits, states will be

a|00> + b|01> + c|10> + d|11>

What if we put a|00> in superposition with d|11> or b|01> in superposition with c|10>?

1st qubit 2nd qubit 1st qubit 2nd qubit

a |0 0> + d|1 1>

Here if we measure the first qubit and get |0>, then the second qubit must be in |0> without measuring it.
The qubits are correlated . This is called Entanglement

Entanglement – Important points

When you change the state of an entangled qubit, then other does not change instantaneously (Don’t violate the “Speed of light” rule ☺)

But if we measure one, We will know what the other one is (i.e correlation)

Entanglement does not depend on distance

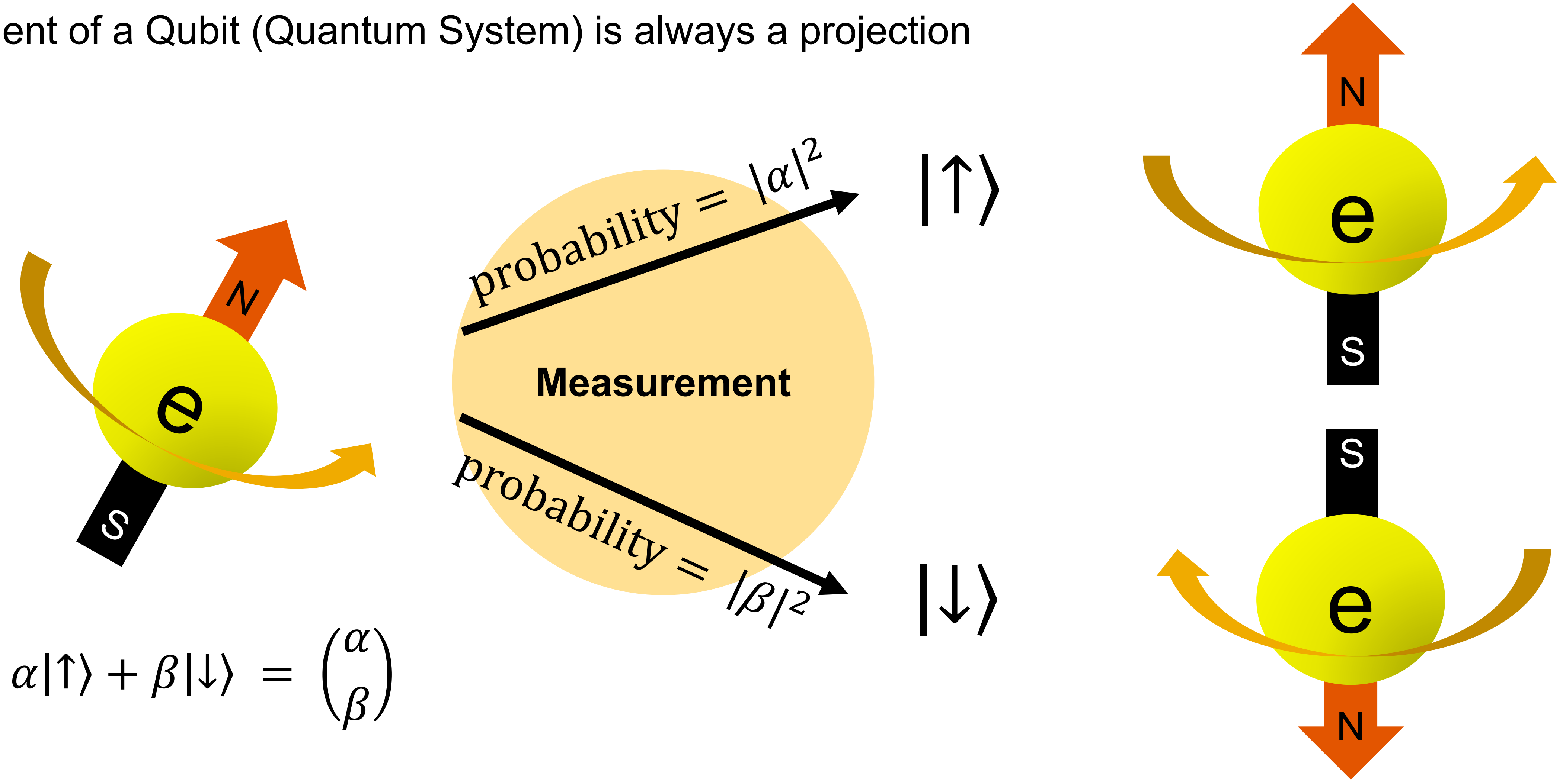
A special set of entangled two qubit state are called Bell States which we use in every quantum algorithm

Bell states

$|\varphi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{2}$ and $|\phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{2}$

Measurement

Measurement of a Qubit (Quantum System) is always a projection



$$\Psi = \alpha|\uparrow\rangle + \beta|\downarrow\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Myth and reality about Quantum Computing

Myth

- Qubit is 0 and 1 at same time
- Wavefunction collapses to one outcome after measurement
- When qubits are entangled ,changing one qubit will instantaneously change other

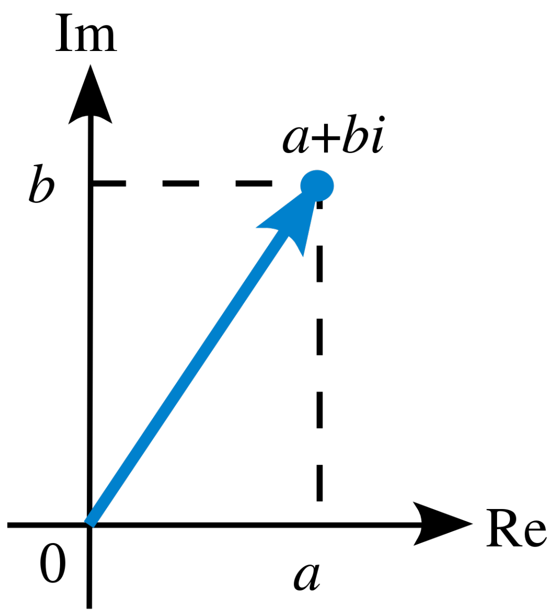
Reality

- Qubit uses linear combination (Superposition) of two states |0> and |1>
- Measurement result is the most probable outcome after constructive and destructive interference of the amplitudes
- Measurement results of entangled qubits are correlated. Measuring one will help us know about the entangled qubit due to correlation

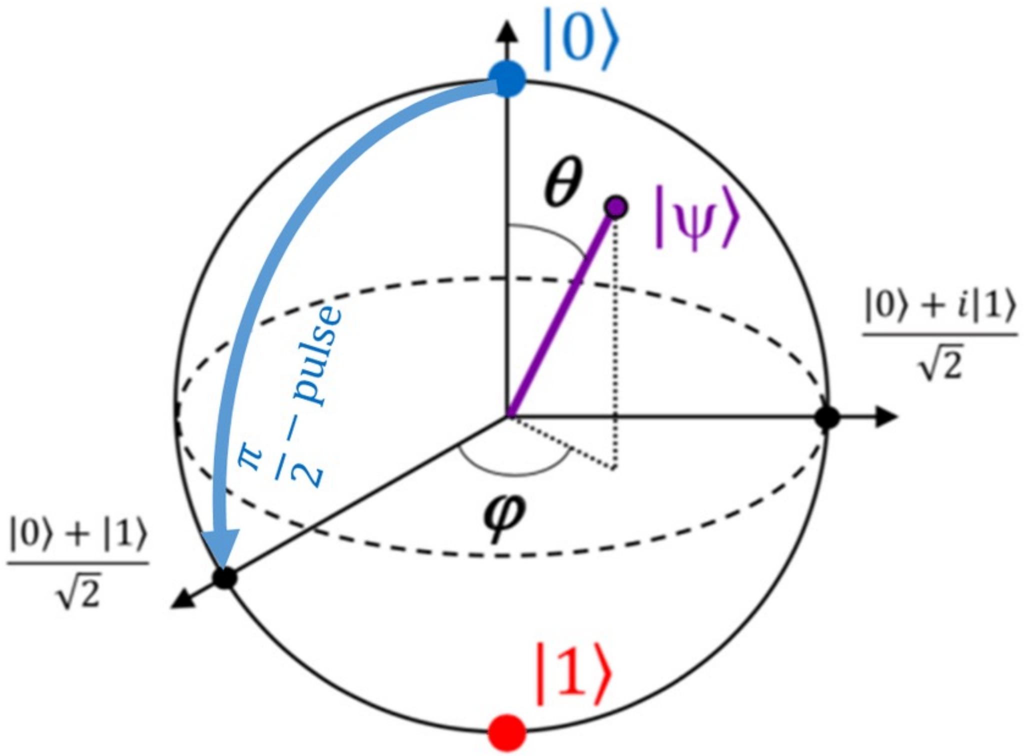
Bloch Sphere explained

Real Number

Complex Number



Bloch Sphere

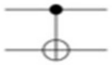
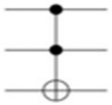


Changing the angles of the vector in bloch sphere lets us manipulate the qubit and obtain the arbitrary amplitude a and b

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

Quantum Gates

Gates are reversible

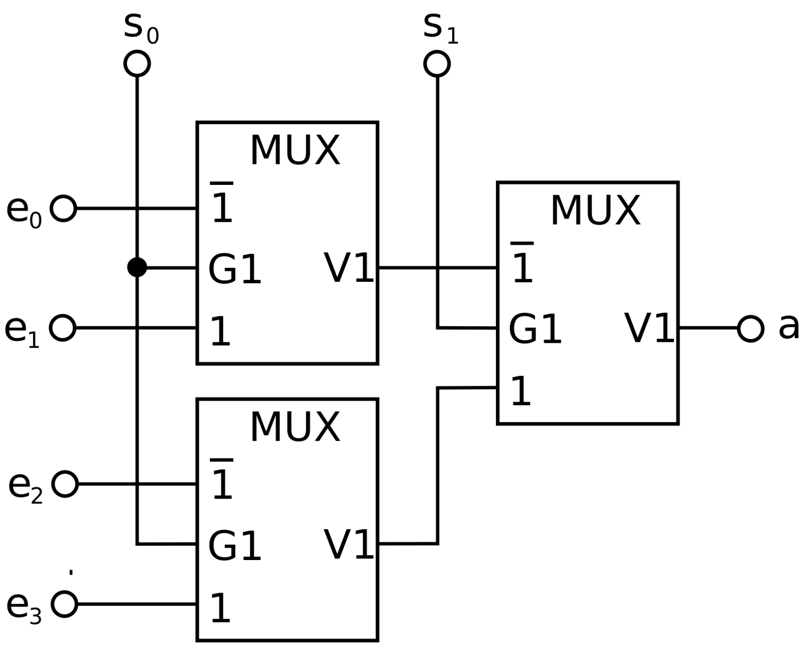
Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Source: Wikipedia

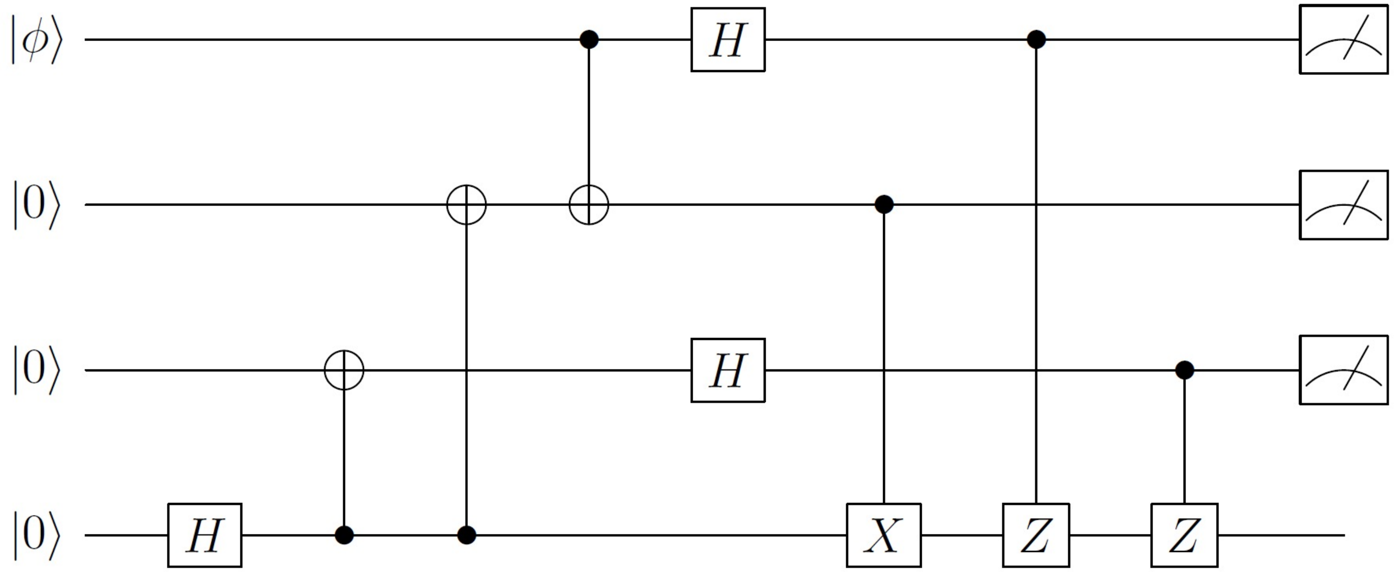
Fundamentals: Quantum algorithms

Entirely different ways of programming- Quantum circuits are formed using quantum gates

Classical gates



Quantum gates



Different Quantum Algorithms

More than 50 + algorithms leveraging quantum phenomena

Algorithm	Application	Expected speed-up
Quantum Fourier Transform	Signal processing, but interestingly it can also serve as a fundamental subcomponent of other algorithms	Exponential
Shor's Algorithm	Factorization and discrete logarithm . Important application is breaking the RSA encryption	Exponential
Grover	Unstructured search (Ex: Bitcoin mining), speed up complex optimization problems(Ex: Travelling salesman etc)	Quadratic
Variational Quantum Eigensolver (VQE) and VAOA	Quantum chemistry and optimization	Quadratic
HHL	Solving linear equations with large number of parameters (Quantum machine learning)	Quadratic
Quantum Recommender	Optimizing recommendations for retail	Quadratic
Quantum Monte-Carlo	quadratic speed-up over classical Markov chain Monte Carlo methods.	Quadratic

Quantum Taxonomy- 1 of 2

Segmentation	Sub-Segement	Companies
Quantum Computing hardware	Superconducting quantum computers (gate based)	IBM, Rigetti, Google,Microsoft
	Trapped ion quantum computers (gate based)	Honeywell, IonQ
	Spin-based quantum computers (gate based)	Intel, Zurich Instruments
	Topological quantum computers	Microsoft Quantum Labs
	Photonic quantum computers	Xanadu, NU Quantum
	Ultracold quantum computers	MIT-Harvard Center, ColdQuanta
Quantum inspired Computing system	Quantum simulators	IBM, Intel, Google
	Superconducting quantum annealers	D-Wave
	Digital annealers	Fujitsu

Source : IDC Quantum Taxonomy , 2021

Quantum Taxonomy- 2 of 2

Segmentation	Sub-Segement	Companies
Quantum computing software and software platforms	Quantum software development kits	IBM Qiskit, Rigetti Forest, Google Cirq, DWave Ocean, Xanadu PennyLane, Amazon Braket Python SDK, Microsoft Quantum Azure Quantum Development Kit for Q#
	Quantum computational platforms	IBM's Q Network, Rigetti's Quantum Cloud Service, D-Wave's Quantum Application Environment, Google Quantum Playground
	Enterprise software platforms	QCWare Forge, Zapata Orquestra, 1QBit
Quantum computing as a service (cloud based)	Quantum computing IaaS	IBM, Rigetti, D-Wave
	Quantum computing PaaS	Amazon Braket, Microsoft Quantum Azure
	Quantum computing SaaS	QCWare, Zapata, 1QBit
	Quantum computing–enabled PaaS	AWS Braket, Microsoft Quantum Azure
	Quantum computing–enabled SaaS	IBM

Source : IDC Quantum Taxonomy , 2021

Resource Links to start with

Coursera : Introduction to Quantum computing

https://www.coursera.org/learn/quantum-computing-algorithms

Linear Algebra: Gilbert Strang

https://www.youtube.com/playlist?list=PL49CF3715CB9EF31D

Complex numbers:

https://www.youtube.com/playlist?list=PLXrbSpZIvPW3XclVIwuUM-GsRJspDsIoz

Quantum Algorithms MOOC:

https://www.youtube.com/playlist?list=PLmRxgFnCIhaMgvot-Xuym_hn69lmzIokg

Book:

"Quantum Computation and Quantum Information"-10th Anniversary edition by Michael Nielsen and Isaac Cheung

Thank You

Reach me at:

Linkedin:

www.linkedin.com/in/rajprasath-subramanian-b384529b

E-Mail:

rajprasath89@gmail.com