

Module 1 : Basics of Quantum Computing

Lecture 1 : Introduction to Quantum Computers

Introduction to Quantum Computing

Anirban Pathak
Jaypee Institute of Information Technology
A10, Sector 62, Noida

C-DAC Accelerated Knowledge Enhancement Scheme (CAKEs) on Introduction to Quantum Computing
Module 1: Basics of quantum computing
Lecture 1: Introduction to quantum computing

Quantumness → Discreteness → First Quantum Revolution

Level 3, E_3, N_3
Level 2, E_2, N_2
Level 1 (ground state), E_1, N_1

R (fast, radiationless transition)
P (pump transition)
I (slow, laser transition)

overlap
Conduction band
Bandgap
Valence band

metal semiconductor insulator

Emitter Base Collector

diffusion drift

n-type p-type n-type

diffusion depletion region depletion region

E_C E_f E_v

GPS

Hg Ion Clock in Hosted Payload

IndusNET

DMSPFM

GPS Correlation

Life would have been boring in completely classical world, specially during lockdowns

an overview of the progression from classical to quantum mechanics, highlighting the concept of discreteness and the first quantum revolution:

Classical Mechanics:

Classical mechanics, formulated by Isaac Newton in the 17th century, describes the motion of macroscopic objects. It is based on Newton's laws of motion and the concept

of determinism, where the state of a system at one time uniquely determines its state at any future time.

Discreteness:

Discreteness refers to the idea that certain physical quantities, such as energy or momentum, can only take on specific, quantized values rather than continuous values. This concept challenges the classical notion of continuous quantities.

First Quantum Revolution:

The first quantum revolution occurred in the early 20th century, primarily driven by the work of scientists like Max Planck, Albert Einstein, Niels Bohr, Werner Heisenberg, and Erwin Schrödinger. Key developments during this period include:

Planck's Quantum Hypothesis (1900):

Max Planck proposed that energy is quantized, meaning it can only exist in discrete packets or "quanta". This idea laid the foundation for quantum theory.

Einstein's Photoelectric Effect (1905):

Albert Einstein explained the photoelectric effect by proposing that light consists of discrete packets of energy called "photons", which helped validate the concept of quantization.

Bohr's Model of the Hydrogen Atom (1913):

Niels Bohr introduced a model of the hydrogen atom based on quantized electron orbits. He proposed that electrons can only occupy certain discrete energy levels, or "quantum states", around the nucleus.

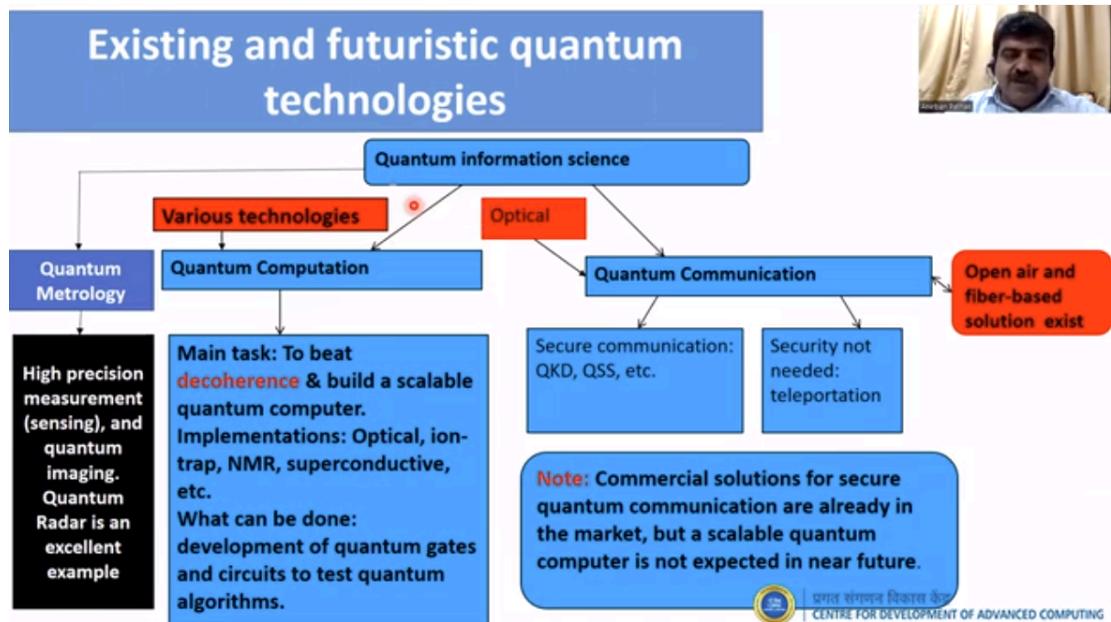
Heisenberg's Uncertainty Principle (1927):

Werner Heisenberg formulated the uncertainty principle, which states that it is impossible to simultaneously determine certain pairs of physical properties, such as position and momentum, with arbitrary precision. This fundamentally limits the predictability of microscopic systems.

Schrödinger's Wave Equation (1926):

Erwin Schrödinger developed a wave equation that describes the behavior of quantum mechanical systems. This equation, along with its solutions, provided a mathematical framework for understanding the wave-like nature of particles.

These groundbreaking discoveries marked a profound shift in our understanding of the physical world, challenging classical notions of determinism and introducing the probabilistic nature of quantum mechanics. The first quantum revolution laid the groundwork for further developments in quantum theory and its applications in various fields, including quantum computing, quantum cryptography, and quantum chemistry.



In []:

Existing and Futuristic Quantum Technologies

Quantum Metrology:

High-precision measurement using quantum imaging, magnetometry, and radar. This technology is already in existence.

Quantum Computation:

Main goal: Overcome decoherence and build a scalable quantum computer. Current implementations include NMR, superconducting traps, and ion traps. Researchers are working on developing quantum gates and circuits to test algorithms.

Quantum Communication:

Focus on secure communication. Examples: Quantum Key Distribution (QKD), Quantum Secret Sharing (QSS), etc. Commercial solutions exist but scalable quantum communication infrastructure (like air fiber) is a future goal.

It's all about speed up: Classes of problem quantum algorithms are expected to solve



EXPTIME: classically solvable in exponential time
Unrestricted chess on an $n \times n$ board

PSPACE: classically solvable in polynomial space
Restricted chess on an $n \times n$ board

QMA: quantumly verifiable polynomial time

NP: classically verifiable in polynomial time

NP-Complete: hardest problems in NP
Traveling salesman problem

P: classically solvable in polynomial time
Testing whether a number is prime
Integer factorization

BQP: quantumly solvable in polynomial time

QMA-Complete: hardest problems in QMA
Quantum Hamiltonian ground state problem

Rev. Mod. Phys. 94 (2022) 015004; relations between classes are not proven. Restricted \Rightarrow polynomial upper bound on the number of moves.

See its position

NQM Immigration office

For a green card answer: Is $P = NP?$ Is $BQP \subseteq NP?$

What is an algorithm? What is complexity of an algorithm?

1231
2312

3543
12
X34

48
36X

408

You are doing addition with an algorithm which takes n steps to add two n digit numbers. Multiplication is more complex, but not too complex, but factorization of product of two large primes is too complex.

Let me give you $N = pq$, where p and q are large primes, and ask you to find p and q , what will

WPI RESEARCHERS DO?
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Problem Classes:

EXPTIME: Represents problems solvable in exponential time.

PSPACE: Refers to problems solvable using polynomial space.

QMA: Quantum Merlin-Arthur complexity class.

NP: Non-deterministic polynomial time.

P: Problems solvable in polynomial time.

BQP: Quantum analog of P.

QMA-Complete: Quantum analog of NP-Complete.

Definition of an Algorithm:

An algorithm is a well-defined sequential computational technique that accepts input values and produces the desired output(s) needed to solve a specific problem.

Think of it as a set of instructions or rules guiding a computer or software in performing a particular task or solving a problem.

An algorithm can be understood as a logical step-by-step procedure, acting as a blueprint for programmers.

Characteristics and Importance:

Efficiency: Algorithms perform tasks quickly and accurately, making them essential for calculations, data processing, and complex operations.

Consistency: They produce consistent results every time they are executed, crucial for dealing with large data or complex processes.

Scalability: Algorithms can handle large datasets or complex problems, making them useful for various applications.

Automation: They automate repetitive tasks, freeing up time for other activities.

Standardization: Algorithms can be shared and standardized across teams or organizations.

Real-Life Examples:

Cooking a Recipe: Just like following a recipe to turn raw ingredients into a delicious dish, an algorithm provides a procedure to achieve the desired output.

Clock Mechanism: Ever wondered how a clock keeps ticking? There's an algorithm behind setting those nuts and bolts to move the hands every minute or hour.

Sorting Algorithms: Bubble Sort, Insertion Sort, and others organize data in specific formats.

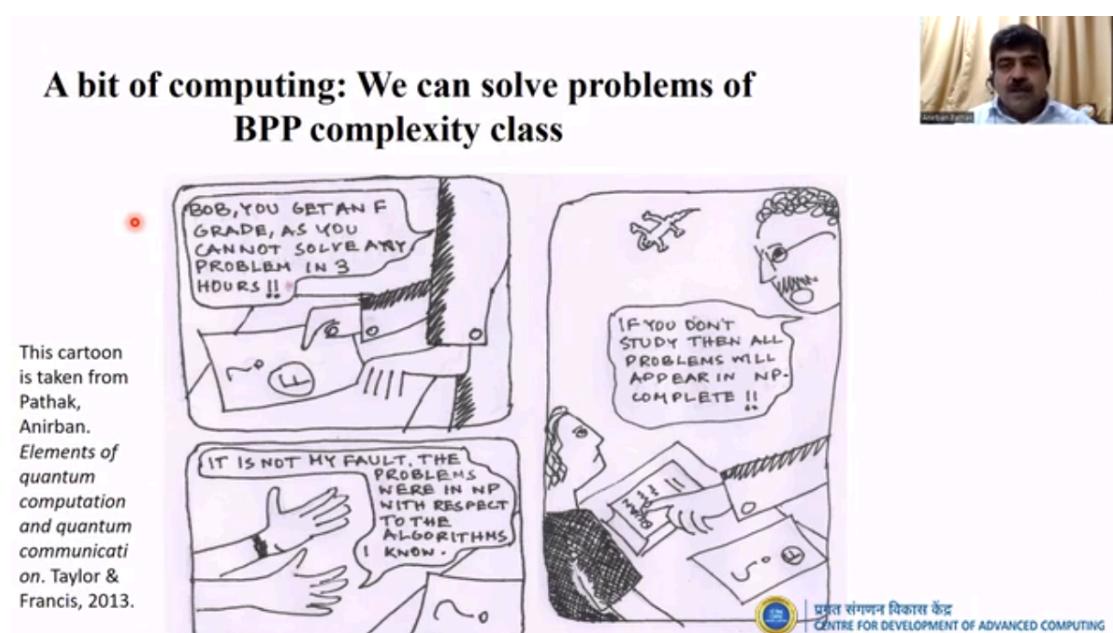
Algorithmic Complexity:

The complexity of an algorithm refers to the amount of computing resources (time and memory) it requires to run. It's crucial to predict how fast an algorithm will run and how much memory it will need before writing the code. Complexity is often measured asymptotically as input size approaches infinity.

Quantum Mechanics, Hilbert Space and Qubits

<https://medium.com/analytics-vidhya/quantum-mechanics-hilbert-space-and-qubits-e411a9bfc6d2>

In []:



Classification of algorithms and popular quantum algorithms



Deutsch and Deutsch-Jozsa algorithms: These promise algorithms have no practical applications.

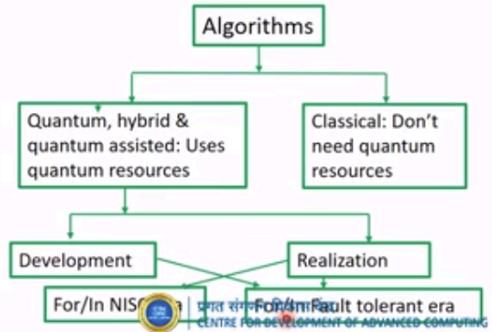
Grover: Can be applied to all problems in NP but quadratic saving would not help much. Note: Circuit SAT is an important unstructured search problem.

Shor: Complexity=>Classical ($\exp(O(\log N)^{1/3}(\log \log N)^{2/3}))$, Quantum $O(\log N)^3$

HHL (Harrow, Hassidim, and Lloyd): Solves linear systems of equations

Quantum Walk-based algos: Spatial search, graph-related problems, simulating dynamics in physical systems.

Variational Quantum Algorithms (VQAs): Analogous to machine-learning methods. Hybrid in nature, starts with a guess (ansatz) and involves quantum and classical devices. Say, a parametrized quantum circuit is to be run on the quantum device, but optimization of the parameters is done on a classical device. VQE and QAOA are special cases of VQA.



Quantum gates

A gate is something which maps an input state uniquely to an output state. You fix H and t and you have a quantum gate. Further, each gate really performs a computation. For example a NOT gate computes $f(x) = \bar{x}$.

$$\begin{aligned}
 H|\psi\rangle &= E|\psi\rangle \\
 H|\psi\rangle &= i\hbar \frac{\partial|\psi\rangle}{\partial t} \\
 |\psi(t)\rangle &= \exp\left(-\frac{iHt}{\hbar}\right)|\psi(0)\rangle \\
 U &= \exp\left(-\frac{iHt}{\hbar}\right) \\
 \Rightarrow U^+ &= U^{-1} \Rightarrow \text{Unitary}
 \end{aligned}$$

- U represents a unitary operation and this is what we understand as a quantum gate. See that it's always reversible!



Lucid introduction to a few ideas before we conclude this lecture

- What is information?
- Is information physical?
- What led to the appearance of the domain of quantum information?
- Why do we need quantum computers?
- What kind of mathematics is primarily used in introductory quantum computing?
- What will we learn in the next few lectures?



In []:

In []:

Lecture 2 : Linear Algebra

Title of course: Introduction to Quantum Computing
Module 1: Basics of quantum computing
Topic of session: Linear algebra 1



Speaker Name: Anirban Pathak

Bra-ket notation:

https://medium.com/@Brain_Boost/quantum-mechanics-what-is-bra-ket-notation-a69b505f9cc4

<https://logosconcarne.com/2021/03/22/qm-101-bra-ket-notation/>

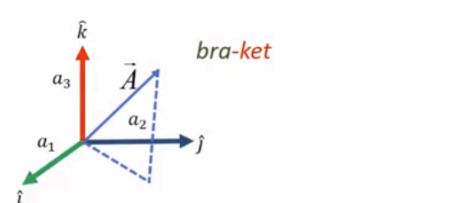
Bra-ket notaiton



Consider a vector A in 3D Euclidean space, $A \in \mathbb{R}^3$. It is easy to see equivalences between ordinary notation and bra-ket notation in vector A . Vector A is the linear combination of the basis vectors represent the coordinates.

$$\begin{aligned}\vec{A} &= a_1\hat{i} + a_2\hat{j} + a_3\hat{k} \\ &= a_1\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + a_2\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + a_3\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} a_1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ a_3 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}\end{aligned}$$

$\langle \quad | \quad \rangle \longrightarrow \langle bra | ket \rangle$



Centre for Development of Advanced Computing

Bra-ket notation continued

Now consider a vector \mathbf{B} in an N dimensional vector complex space $\mathbf{B} \in \mathbb{C}^N$. Vector \mathbf{B} can be represented by a linear combination of basis vectors or a column matrix as:

$$\mathbf{B} = \sum_{n=1}^N b_n e_n = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix}$$

- Ket notation for vectors**

Conventional vector is written in bold type, over/under-arrows, underscores etc., symbolically, A , \vec{A} and \underline{A} . In Dirac's notation for a vector uses vertical bars and angular brackets; vector can be written as $|A\rangle$. Therefore,

$$|A\rangle = a_1|i\rangle + a_2|j\rangle + a_3|k\rangle = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$



Bra-ket notation continued

Or simply one can write 3D vector in terms of ket in simple notation

$$|A\rangle = a_1|1\rangle + a_2|2\rangle + a_3|3\rangle = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

Similarly, for N dimensional vector complex space $\mathbf{B} \in \mathbb{C}^N$ in **ket** notation

$$|B\rangle = \sum_{n=1}^N b_n |e_n\rangle = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix}$$



Bra-ket notation continued

Or simply one can write 3D vector in terms of ket in simple notation

$$|A\rangle = a_1|1\rangle + a_2|2\rangle + a_3|3\rangle = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

Similarly, for N dimensional vector complex space $\mathbf{B} \in \mathbb{C}^N$ in **ket** notation

$$|B\rangle = \sum_{n=1}^N b_n |e_n\rangle = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix}$$



Inner product, Outer Product and Tensor Product

<https://andisama.medium.com/qubit-an-intuition-2-inner-product-outer-product-and-tensor-product-in-bra-ket-notation-9d598cbd6bc>

Inner product

$\langle A | B \rangle = \text{inner product of ket } |A\rangle \text{ with ket } |B\rangle$

$$= \sum_{n=1}^N a_n^* e_n^* \textcolor{red}{a_n} \textcolor{red}{e_n} = (a_1^* \ a_2^* \ \dots \ a_N^*) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix}$$

where a_i^* denotes the complex conjugate of a_i and $\langle A |$ is the conjugate of **ket A** ($|A\rangle$) called **bra A**. The **bra-ket** notation splits inner product in pieces **bra** and **ket**.

$\langle \quad | \quad \rangle \longrightarrow \langle \text{bra} | \text{ket} \rangle$
bra-ket



Arshad Fattah

Example:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow \langle 0 | = (1 \ 0)$$

$$\therefore \langle 0 | 0 \rangle = (1 \ 0) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1.$$

Similarly,

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow \langle 1 | = (0 \ 1)$$

$$\therefore \langle 1 | 0 \rangle = (0 \ 1) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0.$$

 प्रगत तकनीक संविकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Outer product

Outer products are defined as $|A\rangle\langle B|$

They are extremely useful in describing density operators, quantum gates, etc.

Example:

A not gate can be written as $NOT = |0\rangle\langle 1| + |1\rangle\langle 0|$



Arshad Fattah

Examples:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow \langle 0 | = (1 \ 0)$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow \langle 1 | = (0 \ 1)$$

$$\therefore |0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(0 \ 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Similarly,

$$|1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}(1 \ 0) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Thus,

$$|0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

 प्रगत तकनीक संविकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Outer product and quantum gates



Check

$$NOT|0\rangle = |1\rangle \text{ and } NOT|1\rangle = |0\rangle$$

$$\text{as } \langle 0|0\rangle = \langle 1|1\rangle = 1 \text{ and } \langle 1|0\rangle = \langle 0|1\rangle = 1$$

do check

$$NOT|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$NOT|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

A gate can be expressed as a matrix
or as a sum of outer products

• Hadamard gate:

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

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

$$H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

प्रगत संगणना विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Hadamard Gate -

https://www.irjmets.com/uploadedfiles/paper/volume2/issue_5_may_2020/1275/1628083

Superposition - <https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-superposition>

Outer Product in Quantum Computing

The outer product is a fundamental operation in quantum mechanics. It allows us to combine two quantum states to create a composite system. Mathematically, if we have two quantum states represented by vectors $|\psi\rangle$ and $|\phi\rangle$, their outer product yields a new state:

$$[|\psi\rangle \otimes |\phi\rangle]$$

In this expression, \otimes denotes the outer product. The resulting state is a composite state that describes the joint behavior of the two original states.

Quantum Gates -

Quantum gates are analogous to classical logic gates but operate on quantum bits (qubits). They manipulate the quantum state of a qubit. Some common quantum gates include:

1. Hadamard Gate (H):

Creates superpositions by transforming the basis states $|0\rangle$ and $|1\rangle$ into equal-weighted superpositions.

2. Pauli-X Gate (X):

Flips the state of a qubit (similar to a classical NOT gate).

3. CNOT Gate (Controlled-X):

Entangles two qubits, where the second qubit's state depends on the first qubit's state.

4. Toffoli Gate (CCNOT):

A three-qubit gate that performs a controlled-controlled-X operation.

https://en.wikipedia.org/wiki/Quantum_logic_gate

Suggested further readings



For the beginners:

- Pathak, Anirban. *Elements of quantum computation and quantum communication*. Boca Raton: CRC Press, 2013.
- Kaye, Phillip, Raymond Laflamme, and Michele Mosca. *An introduction to quantum computing*. OUP Oxford, 2006.
- McMahon, David. *Quantum computing explained*. John Wiley & Sons, 2007.

Only for advanced readers:

- Nielsen, Michael A., and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010.



Which famous physicist is credited with coining the term "quantum computing"?

- Albert Einstein
- Richard Feynman
- Niels Bohr
- Werner Heisenberg

✓ Your Answer was right!

Which renowned physicist proposed the concept of quantum teleportation in 1993, a fundamental component of quantum computing?

- Richard Feynman
- Albert Einstein
- Charles Bennett
- Peter Shor

✓ Your Answer was right!

Title of course: Introduction to Quantum Computing
Module 1: Basics of quantum computing
Topic of session: Linear algebra 2

Speaker Name: Anirban Pathak



Tensor product

$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} c \\ d \end{bmatrix} \\ b \begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$

$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

Similarly,

$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

Mathematica command for performing tensor product of matrices A and B is KroneckerProduct[A,B], In Matlab it is kron(A,B)



inner product ==> scalar

outer product ==> square matrix

Tensor product: Simple examples continued

$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

Similarly,

$|11\rangle = |1\rangle \otimes |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Dimension of Hilbert space (a vector space where inner products are well defined, complex projection is allowed and there is no restriction on the dimension) increases quickly in the quantum world.

$|0_1 0_2 0_3 \dots 0_n\rangle$ is a column matrix with 2^n rows and any operator (gate or circuit) that can operate on this and transform it into a state vector of the same dimension will be a $2^n \times 2^n$ matrix.

This can be used to explain why do we need quantum computing and the meaning of entanglement

Some tensor product facts



$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}$$



Some tensor product facts continued



$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \otimes \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} =$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \left(\begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \otimes \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \right)$$

Physicists use this very often, say when you write $a_1 a_2 |n_1, n_2\rangle = \sqrt{(n_1 - 1)(n_2 - 1)}|n_1 - 1, n_2 - 1\rangle$. You use $(a_1 \otimes a_2)(|n_1\rangle \otimes |n_2\rangle) = (a_1|n_1\rangle) \otimes (a_2|n_2\rangle) = \sqrt{(n_1 - 1)}|n_1 - 1\rangle \otimes \sqrt{(n_2 - 1)}|n_2 - 1\rangle = \sqrt{(n_1 - 1)(n_2 - 1)}|n_1 - 1, n_2 - 1\rangle$

$$(Av) \otimes (Bw) = (A \otimes B)(v \otimes w)$$

$$H|0\rangle \otimes H|0\rangle = (H \otimes H)(|0\rangle \otimes |0\rangle) = (H \otimes H)|00\rangle$$



Tensor product and quantum circuit



$$H|0\rangle \otimes I_2|0\rangle = (H \otimes I_2)(|0\rangle \otimes |0\rangle) = (H \otimes I_2)|00\rangle$$

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

$$|0\rangle \xrightarrow{\quad} |0\rangle$$

$$\left[\begin{array}{c} |0\rangle + |1\rangle \\ \hline \sqrt{2} \end{array} \right] \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

$$\Rightarrow \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$H \otimes I_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$H \otimes I_2|00\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$



Tensor product leads to the definition of entangled states

If you cannot express a bipartite (or two mode) state vector as the tensor product of the state vectors of the individual particle (mode), the composite state is called entangled, i.e., inseparable

Thus,

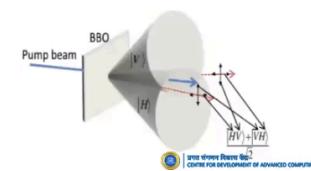
$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B \Rightarrow$ Entangled; Example:

$$|\psi\rangle_{AB} = \frac{(|00\rangle + |11\rangle)_{AB}}{\sqrt{2}}$$

Similarly, state is separable if $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$

Example: $|00\rangle, |10\rangle, |01\rangle, |11\rangle, \frac{|00\rangle \pm |01\rangle}{\sqrt{2}}$

Entanglement is superposition in the tensor product space



Suggested further readings

For the beginners:

- Pathak, Anirban. *Elements of quantum computation and quantum communication*. Boca Raton: CRC Press, 2013.

Only for advanced readers:

- Nielsen, Michael A., and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010.



Title of course: Introduction to Quantum Computing
Module 1: Basics of quantum computing
Topic of session: Linear algebra 3

Speaker Name: Anirban Pathak



Recall: Outer product, tensor product and quantum gates again

- A gate A in general:

$$A = \sum_i |output_i\rangle\langle input_i|$$

- SWAP Gate**

$$|xy\rangle \rightarrow |yx\rangle$$

$$\therefore |00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |10\rangle,$$

$$|10\rangle \rightarrow |01\rangle, |11\rangle \rightarrow |11\rangle$$

$$SWAP = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|$$

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

Similarly,

CNOT maps

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle,$$

$$|10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$$

$$SWAP = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

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

You can write
your own code to
simulate
quantum circuits

प्रातः प्रगति विद्यालय
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Suggested further readings

For the beginners:

- Pathak, Anirban. *Elements of quantum computation and quantum communication*. Boca Raton: CRC Press, 2013.
- Kaye, Phillip, Raymond Laflamme, and Michele Mosca. *An introduction to quantum computing*. OUP Oxford, 2006.
- McMahon, David. *Quantum computing explained*. John Wiley & Sons, 2007.

Only for advanced readers:

- Nielsen, Michael A., and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010.

Recall: Outer product, tensor product and quantum gates again

- A gate A in general:

$$A = \sum_i |output_i\rangle\langle input_i|$$

- SWAP Gate**

$$|xy\rangle \rightarrow |yx\rangle$$

$$\therefore |00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |10\rangle,$$

$$|10\rangle \rightarrow |01\rangle, |11\rangle \rightarrow |11\rangle$$

$$SWAP = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|$$

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

Similarly,

CNOT maps

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle,$$

$$|10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$$

$$SWAP = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

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

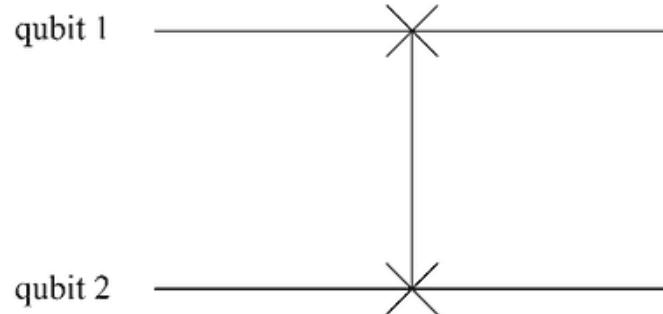
You can write
your own code to
simulate
quantum circuits

प्रातः प्रगति विद्यालय
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

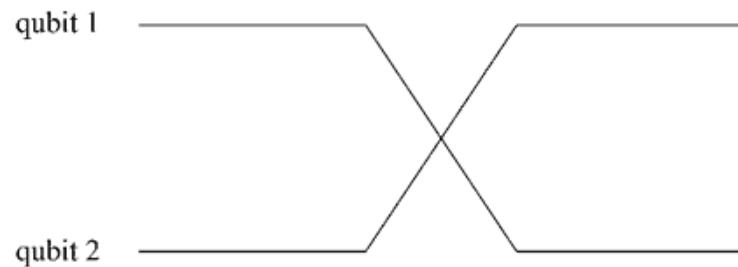
SWAP Gate

The SWAP gate is a logic gate in quantum computing that swaps the states of two qubits.

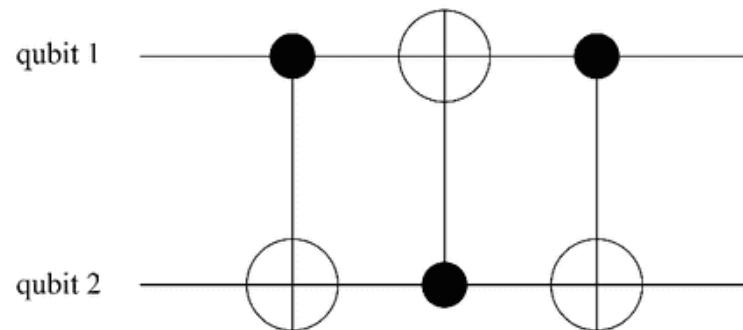
The diagram below shows how a SWAP gate is represented in quantum circuits.



It can also be represented as



The process of exchanging two states can be achieved using three CNOT gates, as shown below.



making-a-swap-gate-from-cnot-gates Thus, the SWAP gate symbols can be thought of as just convenient shorthand for this sequence of gates.

Symbolically, we write this action as

$$\text{SWAP}(|\phi_1\rangle \otimes |\phi_2\rangle) = |\phi_2\rangle \otimes |\phi_1\rangle$$

The SWAP gate can be represented in matrix form as

$$\text{SWAP} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

The SWAP gate is frequently used in hardware where not all connections between qubits are possible to allow linking non-adjacent qubits. It may also appear as a necessary part in building the quantum Fourier transform or in other routines such as the SWAP test.

```
In [ ]: from qiskit import QuantumCircuit
from qiskit.visualization import circuit_drawer

# Create a quantum circuit
qc = QuantumCircuit(2)
qc.swap(0, 1) # Apply SWAP gate

# Draw the circuit
circuit_drawer(qc, output='mpl')
```

CNOT Gate

The CNOT gate is two-qubit operation, where the first qubit is usually referred to as the control qubit and the second qubit as the target qubit. Expressed in basis states, the CNOT gate:

- leaves the control qubit unchanged and performs a Pauli-X gate on the target qubit when the control qubit is in state $|1\rangle$;
- leaves the target qubit unchanged when the control qubit is in state $|0\rangle$.

A traditional NOT gate inverts the input: if the input is 0, the output is 1. In a quantum system, we can use a CNOT Gate, or Controlled Quantum Gate. In this case, we have an input qubit and a target cubit. The CNOT gate can be used to create an entangled state into the two-qubit model. There are several variations on the CNOT gate, and they are used to generate a set of logic gates for quantum computing.

In the CNOT gate, one qubit is a control qubit, and the second is the target qubit.

Figure shows a schematic of the quantum circuit. The circle with the cross indicates entanglement.

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

Eigenvalue equations

Operators, Eigenfunctions and eigenvalues

$$\hat{O} f(x) = \lambda f(x)$$

Example: function $\rightarrow \sin 2x$
operator $\rightarrow -\frac{d^2}{dx^2}$
eigenvalue $\rightarrow ?$

Solution: $-\frac{d^2}{dx^2}(\sin 2x) = 4(\sin 2x)$

Note: In Quantum mechanics, the allowed eigenfunction must be *finite, single valued and continuous for all x*

Quantum mechanics at a glance

- Anything that is physically measurable in classical world is called physical observable. For example: mass, momentum, time, etc., are physical observable.
- For every classical observable, there exist a corresponding quantum mechanical operator
momentum in x direction $p_x \Rightarrow -i\hbar \frac{\partial}{\partial x}$ and energy $E \Rightarrow i\hbar \frac{\partial}{\partial t}$
- The operators satisfies an eigen value equation of the form $A_{\Psi}\Psi(x) = \lambda\Psi(x)$
 $\Psi(x)$ is eigen function (in quantum mechanics it is called wave function and is a solution of Schrödinger equation) and λ is eigenvalue, these are the values of the corresponding physical observable which can be observed in an experiment. Since λ is discrete, only certain values of the observable are possible.
- If and only if any two operator A and B satisfies $AB = BA$ then the corresponding observable can be measured simultaneously with arbitrary accuracy. **This is uncertainty principle**

If cloning was allowed uncertainty principle would have been violated

Schrodinger Eq.
 $H\Psi = E\Psi$
It has two forms time-dependent and time-independent

1. Operators and Eigenvalues:

In quantum mechanics, operators represent physical observables, such as position, momentum, energy, etc. For example, the position operator (\hat{x}) gives the position of a particle, while the momentum operator (\hat{p}) gives the momentum.

The Schrödinger equation describes how the quantum state of a physical system changes over time. For a time-independent case, the Schrödinger equation is typically written as:

$$\hat{H}\psi(x) = E\psi(x)$$

Where:

- \hat{H} is the Hamiltonian operator, representing the total energy of the system.
- $\psi(x)$ is the wavefunction, representing the state of the system.
- E is the eigenvalue corresponding to the energy of the system.

Here, E represents the energy that the system can possess. $\psi(x)$ is the corresponding wavefunction (eigenfunction) of the system.

2. Eigenvalues and Observables:

Eigenvalues (E in this case) represent the possible values of a physical observable (energy in this case) that can be measured in an experiment. The wavefunction ($\psi(x)$) gives the probability amplitude for finding the particle at position x .

3. Uncertainty Principle:

The uncertainty principle, formulated by Werner Heisenberg, states that there is a fundamental limit to the precision with which certain pairs of physical properties of a particle, like position and momentum, can be simultaneously known. Mathematically, it can be expressed as:

$$\Delta A \cdot \Delta B \geq \frac{\hbar}{2}$$

Where:

- ΔA is the uncertainty in the measurement of observable A.
- ΔB is the uncertainty in the measurement of observable B.
- \hbar is the reduced Planck constant.

This implies that if two operators \hat{A} and \hat{B} commute ($[\hat{A}, \hat{B}] = 0$), then their corresponding observables can be measured simultaneously with arbitrary accuracy.

4. Time-Dependent and Time-Independent Schrödinger Equations:

The Schrödinger equation comes in two forms:

a. Time-Dependent Schrödinger Equation:

$$i\hbar \frac{\partial \psi}{\partial t} = \hat{H}\psi$$

This equation describes how the wavefunction evolves with time, where \hbar is the reduced Planck constant.

b. Time-Independent Schrödinger Equation:

$$\hat{H}\psi = E\psi$$

This equation describes the stationary states of a quantum system, where the energy of the system is not changing with time.

Cloning and the Uncertainty Principle:

Cloning in quantum mechanics refers to the hypothetical process of creating an identical copy of a quantum state. If cloning were allowed, it would violate the uncertainty principle because we could clone a particle's state with perfect precision, thus violating the limits imposed by the uncertainty principle.

In summary, the Schrödinger equation describes the behavior of quantum systems, operators and eigenvalues represent physical observables, and the uncertainty principle imposes limits on our ability to measure certain pairs of observables simultaneously.

Example of Uncertainty Principle

Example:

Let's consider the position (\hat{x}) and momentum (\hat{p}) operators in one dimension. The uncertainty principle for position and momentum can be expressed as:

$$\Delta x \cdot \Delta p_x \geq \frac{\hbar}{2}$$

Here, Δx is the uncertainty in position, and Δp_x is the uncertainty in momentum along the x-axis.

Now, let's consider a particle in a particular quantum state described by the wavefunction $\psi(x)$.

The uncertainty in position Δx can be defined as the standard deviation of the position operator:

$$\Delta x = \sqrt{\langle (\hat{x} - \langle \hat{x} \rangle)^2 \rangle} = \sqrt{\langle \hat{x}^2 \rangle - \langle \hat{x} \rangle^2}$$

Similarly, the uncertainty in momentum Δp_x can be defined as the standard deviation of the momentum operator:

$$\Delta p_x = \sqrt{\langle (\hat{p}_x - \langle \hat{p}_x \rangle)^2 \rangle} = \sqrt{\langle \hat{p}_x^2 \rangle - \langle \hat{p}_x \rangle^2}$$

If we consider a particle in a state that is an eigenstate of both position and momentum, then the uncertainties are minimized, and the product $\Delta x \cdot \Delta p_x$ satisfies the uncertainty principle.

For example, consider the state $\psi(x)$ which is an eigenstate of both \hat{x} and \hat{p}_x . In this case, the product $\Delta x \cdot \Delta p_x$ can be made as small as desired, satisfying the uncertainty principle.

However, if the operators corresponding to \hat{x} and \hat{p}_x do not commute, their eigenstates cannot be simultaneous and exact. In that case, there's always some uncertainty, and the product $\Delta x \cdot \Delta p_x$ cannot be reduced below a certain limit, as dictated by the uncertainty principle.

**Basic Ideas of Quantum Mechanics:
Repeated again**



1. For every physical observable there is an operator.
2. The operator satisfies eigen value equation, where eigen function is the wave function and eigen values are discrete values that a measurement can yield.
3. Operators corresponding to physical observables are Hermitian to give real eigenvalues.
4. Time evolution of a quantum state is described by an unitary operator, but measurement operators are non-unitary, and thus, irreversible. Kraus operators for noise are also irreversible.

Measurement operators $M_i = |i\rangle\langle i|$,
 $[M_0, M_+] = M_0 M_+ - M_+ M_0 \neq 0$
 We cannot perform simultaneous measurements using $\{|0\rangle, |1\rangle\}$ & $\{|+\rangle, |-\rangle\}$ basis

On measurement a quantum state collapses to one of the allowed eigenstates

 TIFAC-CDA | TATA INSTITUTE OF Fundamental RESEARCH
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTATION

1. Operators and Observables:

In quantum mechanics, every physical observable (like position, momentum, energy, etc.) corresponds to a Hermitian operator. This operator acts on the wavefunction, which represents the state of the system. When this operator acts on the wavefunction, it gives back the same wavefunction (up to a constant) or a scaled version of it. This relationship is described by the eigenvalue equation:

$$\hat{A}\psi(x) = a\psi(x)$$

Where:

- \hat{A} is the operator corresponding to the observable.
- $\psi(x)$ is the wavefunction (eigenfunction).
- a is the eigenvalue corresponding to the observable.

2. Hermitian Operators:

Operators corresponding to physical observables are Hermitian. This ensures that the eigenvalues are real, which is a requirement for physical observables. Hermitian operators have the property that their adjoint (conjugate transpose) is equal to themselves:

$$\hat{A}^\dagger = \hat{A}$$

3. Time Evolution and Unitary Operators:

The time evolution of a quantum state is described by the unitary operator, typically denoted by $U(t)$. The unitary operator ensures that the norm of the state vector is preserved, meaning probabilities sum to 1. Mathematically, it's described by the Schrödinger equation:

$$i\hbar \frac{\partial}{\partial t} \psi(t) = \hat{H}\psi(t)$$

Where \hat{H} is the Hamiltonian operator.

4. Measurement Operators:

Measurement operators are non-unitary and irreversible. When we measure an observable, the act of measurement "collapses" the wavefunction to one of its eigenstates corresponding to the measured value. This collapse is non-reversible, meaning we can't recover the original state.

5. Kraus Operators for Noise:

In the context of quantum error correction and quantum information theory, Kraus operators are used to describe noisy quantum processes. These operators model the evolution of the quantum state due to the presence of noise or decoherence. They are also non-unitary and irreversible, leading to information loss and decoherence in quantum systems.

In summary, in quantum mechanics, operators correspond to physical observables, and their eigenvalues give the possible outcomes of measurements. Hermitian operators ensure real eigenvalues. Time evolution is governed by unitary operators, while measurement and noise processes are described by non-unitary and irreversible operators.

In []:

Operators v/s Gates

Operators in Quantum Mechanics:

Operators in quantum mechanics are mathematical entities that operate on wavefunctions or state vectors to perform various operations or measurements. They are represented by matrices or differential operators.

- 1. Observable Operators:** These operators correspond to physical observables. For example, the position operator (\hat{x}) corresponds to the observable of position, the momentum operator (\hat{p}) corresponds to momentum, and so on.
- 2. Unitary Operators:** These operators preserve the norm of the state vector and are used to describe time evolution in quantum mechanics. The time evolution operator ($U(t)$) in the Schrödinger equation is a unitary operator.

Gates in Quantum Computing:

Quantum gates, on the other hand, are specific types of unitary operators used in quantum computing. They act on qubits (quantum bits) to perform operations that manipulate quantum information. These gates are analogous to classical logic gates but operate on quantum states.

- 1. Single-Qubit Gates:** These gates operate on a single qubit and can perform operations such as rotations, flips, and phase shifts. Examples include the Hadamard gate, Pauli gates (X, Y, Z), and phase gates (S, T).
- 2. Multi-Qubit Gates:** These gates operate on multiple qubits and perform operations that entangle or disentangle qubits. Examples include the Controlled-NOT (CNOT) gate, controlled-phase gate (CPHASE), and SWAP gate.

Differences and Similarities:

- Purpose:** Operators in quantum mechanics describe physical observables and time evolution, while quantum gates in quantum computing manipulate qubits to perform quantum algorithms.
- Mathematical Representation:** Both operators and gates are represented by matrices, but they serve different purposes and may have different properties.
- Unitarity:** In quantum mechanics, unitary operators describe reversible processes, while in quantum computing, gates must be unitary to preserve the quantum state's normalization.

In summary, while operators in quantum mechanics represent observables and time evolution, quantum gates in quantum computing manipulate qubits to perform computations. However, they both involve mathematical operations on quantum states, often represented by matrices.

The operators and equations that you need to know



- The operators corresponding to physical observables in position space:

Position: $x \rightarrow \hat{x}$

Momentum: $p \rightarrow \hat{p} = -i\hbar \frac{\partial}{\partial x}$

Energy: $E \rightarrow \hat{E} = i\hbar \frac{\partial}{\partial t}$,

annihilation operator: $\hat{a} = \frac{1}{\sqrt{2\hbar m\omega}}(m\omega \hat{x} + i\hat{p})$,

creation operator: $\hat{a}^\dagger = \frac{1}{\sqrt{2\hbar m\omega}}(m\omega \hat{x} - i\hat{p})$,

photon number: $\hat{N} \rightarrow \hat{a}^\dagger \hat{a}$,

$$\frac{-\hbar^2}{2m} \nabla^2 \Psi(r) + V(r)\Psi(r) = E\Psi(r)$$

Time independent Schrodinger equation

Kinetic Energy + Potential Energy = Total Energy

Time dependent Schrodinger equation

$$H|\psi\rangle = E|\psi\rangle$$

$$H|\psi\rangle = i\hbar \frac{\partial |\psi\rangle}{\partial t}$$

$$|\psi(t)\rangle = \exp\left(-\frac{iHt}{\hbar}\right)|\psi(0)\rangle$$

$$U = \exp\left(-\frac{iHt}{\hbar}\right)$$

$$\Rightarrow U^+ = U^{-1} \Rightarrow \text{Unitary}$$

U represents a unitary operation and this is what we understand as a quantum gate

SIMPLY SPINNING BEATS
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Some examples of operators in quantum mechanics:

1. Position Operator (\hat{x}):

The position operator acts on the wavefunction to give the position of a particle in space. In one dimension, it's represented as:

$$\hat{x}\psi(x) = x\psi(x)$$

2. Momentum Operator (\hat{p}):

The momentum operator acts on the wavefunction to give the momentum of a particle. In one dimension, it's represented as:

$$\hat{p}\psi(x) = -i\hbar \frac{d\psi(x)}{dx}$$

3. Hamiltonian Operator (\hat{H}):

The Hamiltonian operator represents the total energy of a quantum system. It includes kinetic and potential energy terms. For a single particle in one dimension:

$$\hat{H}\psi(x) = -\frac{\hbar^2}{2m} \frac{d^2\psi(x)}{dx^2} + V(x)\psi(x)$$

Where $V(x)$ is the potential energy function.

4. Spin Operator (\hat{S}_z):

The spin operator represents the z-component of the spin angular momentum of a particle. It acts on the spinor representing the particle's spin state. For example, for a spin-1/2 particle:

$$\hat{S}_z \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} = \frac{\hbar}{2} \begin{pmatrix} \psi_1 \\ -\psi_2 \end{pmatrix}$$

5. Pauli Matrices:

The Pauli matrices ($\sigma_x, \sigma_y, \sigma_z$) are a set of operators used in quantum mechanics. They are used in various contexts, including representing spin states and as building blocks for quantum gates in quantum computing.

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

These are just a few examples of operators in quantum mechanics. There are many more, each corresponding to different physical observables or transformations.

Pauli matrices are quantum gates



Every gate computes a function. For example, NOT gate computes $f(x) = \bar{x}$.

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow X|0\rangle = |1\rangle; X|1\rangle = |0\rangle,$$

$$iY = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Rightarrow i\sigma_y|0\rangle = -|1\rangle; i\sigma_y|1\rangle = |0\rangle,$$

$$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow Z|0\rangle = |0\rangle; Z|1\rangle = -|1\rangle,$$

$$I = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow I|0\rangle = |0\rangle; I|1\rangle = |1\rangle,$$

We will use these gates to describe quantum teleportation as an example

Gates are sequentially added to form circuits and a group of circuits build quantum computer. To build a real quantum computer you need all single qubit gates and at least one real two qubit gate (say CNOT) which can not be decomposed into one qubit gates.

SNS TIFR
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

The action of the X-operator is to introduce the bit-flip, the action of the Z-operator is to introduce the phase-flip, and the action of the Y-operator is to simultaneously introduce the bit- and phase-flips.

Pauli Matrices -

<https://www.sharetechnote.com/html/QC/QuantumComputing.html#PauliMatrices>

1. σ_x (Pauli-X Gate):

The Pauli-X gate is analogous to the classical NOT gate. It flips the state of a qubit from $|0\rangle$ to $|1\rangle$ and vice versa. Mathematically, it's represented by the matrix:

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

2. σ_y (Pauli-Y Gate):

The Pauli-Y gate is similar to a combination of a bit flip and a phase flip. It performs a bit flip and introduces a phase change. Mathematically:

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

3. σ_z (Pauli-Z Gate):

The Pauli-Z gate flips the sign of the $|1\rangle$ state. It does not change the probability amplitudes but introduces a phase shift. Mathematically:

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

Properties:

- All Pauli matrices are Hermitian, unitary, and involutory, meaning that applying them twice gives the identity matrix.
- They form a basis for the space of 2×2 complex matrices.
- They are also self-adjoint, meaning they are equal to their own adjoint.

Circuit model of computation

Quantum circuit diagram:

```

    graph LR
      i1[i1] --> G1[G1]
      i2[i2] --> G2[G2]
      i3[i3] --> G3[G3]
      i4[i4] --> G4[G4]
      G1 --> o1[o1]
      G2 --> o2[o2]
      G3 --> o3[o3]
      G4 --> o4[o4]
  
```

Linear Algebra Formulation of the Circuit Model

Not gate:

$$X|0\rangle \rightarrow |1\rangle$$

$$X|1\rangle \rightarrow |0\rangle$$

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

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = (\beta|0\rangle + \alpha|1\rangle)$$

Quantum circuit model

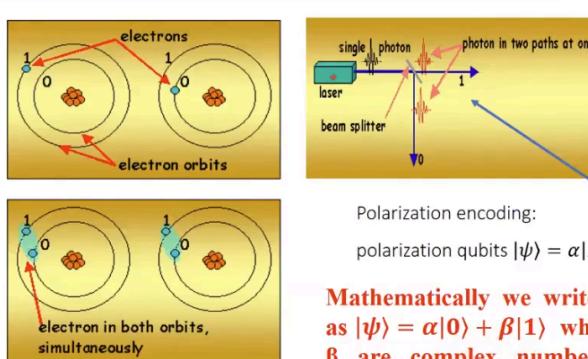
Diagram showing a Hadamard (H) gate followed by a CNOT gate between the first and second qubits, resulting in the state $\frac{|00\rangle + |10\rangle}{\sqrt{2}}$.

Title of course: Introduction to Quantum Computing
Module 1: Basics of quantum computing
Topic of session: Qubit and Bloch sphere



Speaker Name: Anirban Pathak

A Qubit is a two level quantum system: It can be realized in many ways



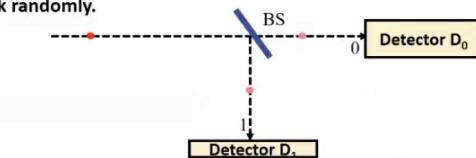

Position/path or spatial encoding
 polarization qubits $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$

Mathematically we write a qubit as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α and β are complex numbers which satisfies $|\alpha|^2 + |\beta|^2 = 1$.



A simple use of qubit: Send a single photon through a beam splitter

- Realize a qubit (basic building block of quantum computing): The photon in a superposition of both paths and so represents both 0 and 1 simultaneously. Now if we put detectors along both the paths, the detectors will click randomly.



- True random number generator (as God does not play dice!). See IdQuantique's Quantis
- In quantum world even Rajnikant does not know what will happen next!



You can check it using IBM quantum experience or another cloud based quantum computer

Quantum Circuit

(A) Quantum circuit diagram showing five qubits (q01 to q41) and one classical register (c). A CNOT gate is applied between q01 and q11.

(B) 1 time measurement plot showing a single bar at index 0 with value 1.000.

(C) 1 time measurement plot showing a single bar at index 0 with value 1.000.

(D) 1024 times measurement plot showing two bars at indices 0 and 1 with values 0.576 and 0.424 respectively.

(E) 4096 times measurement plot showing two bars at indices 0 and 1 with values 0.567 and 0.433 respectively.

(F) 8192 times measurement plot showing three bars at indices 0, 1, and 2 with values 0.565, 0.435, and 0.000 respectively.

SPARC Centre for Development of Advanced Computing

You can run NIST tests and check randomness

The screenshot shows the ANU QRNG website on the left and the NIST Statistical Test Suite on the right. Red arrows point from the NIST interface to specific data in the terminal window.

ANU QRNG

Random binary bits

NIST STS

GENERATOR SELECTION

File Edit Format View Help

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator	is (data/text1.txt)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10	P-VALUE PROPORTION STATISTICAL TEST
0 1 1 0 1 3 1 0 2 1	0.534146 10/10 Frequency

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 8 for a sample size = 10 binary sequences.

For further guidelines construct a probability table using the MAPLE program provided in the addendum section of the documentation.

> 0.01 means random.

SPARC Centre for Development of Advanced Computing

Background information for the introduction of Bloch sphere

- Note 1:** $|\psi(x)\rangle$ does not have a physical meaning. The meaning is associated with $|\psi(x)|^2$ (this is the probability of finding the system described by $|\psi(x)\rangle$ in position x . Thus, $|\psi(x)\rangle$ and $|\psi'(x)\rangle = e^{-i\phi}|\psi(x)\rangle$ are equivalent as the global phase ϕ will not change the probability (see $|\psi'(x)|^2 = |\psi(x)|^2$). Consequently such global phases can be ignored from the description of a state.
- Note 2:** A qubit is described as $\alpha|0\rangle + \beta|1\rangle$: $|\alpha|^2 + |\beta|^2 = 1$, here α and β are complex and $|\alpha|^2$ ($|\beta|^2$) is the probability of getting the state in $|0\rangle$ ($|1\rangle$) when measured using $\{|0\rangle, |1\rangle\}$ basis.

SPARC Centre for Development of Advanced Computing

Background information for the introduction of Bloch sphere continued

- Note 3:** A complex number z can be expressed in polar decomposed form as $z = re^{i\eta}$ where r and η are real. Now, for a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$: $|\alpha|^2 + |\beta|^2 = 1$, α and β are complex and can be expressed as $\alpha = r_1 e^{i\eta_1}$ and $\beta = r_2 e^{i\eta_2}$.
- Thus, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = r_1 e^{i\eta_1}|0\rangle + r_2 e^{i\eta_2}|1\rangle = e^{i\eta_1}(r_1|0\rangle + r_2 e^{i(\eta_2-\eta_1)}|1\rangle)$. Ignoring global phase $e^{i\eta_1}$ and considering $(\eta_2 - \eta_1) = \phi$, we can write $|\psi\rangle = r_1|0\rangle + r_2 e^{i\phi}|1\rangle$. Further as r_1 and r_2 are real, $|\alpha|^2 + |\beta|^2 = 1$ implies $r_1^2 + r_2^2 = 1$ and allows out to parametrize r_1 and r_2 as $r_1 = \cos\frac{\theta}{2}$ and $r_2 = \sin\frac{\theta}{2}$. So we can write an arbitrary qubit as $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ which is a vector of unit magnitude and can be described by θ and ϕ alone. Space spanned by all such state vectors will be the surface a unit sphere with $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$, and such a unit sphere is lucidly called a Bloch sphere.



SATE SHIKSHA BHARAT
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Basic idea of density operator, pure state and mixed state

- Till now a quantum state is described as a state vector $|\psi\rangle$, but quantum state of a physical system can also be described with density operator (or density matrix) ρ . For a pure state $\rho = |\psi\rangle\langle\psi|$. So for state $|0\rangle$, $\rho_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} (1 \quad 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; and for state $|1\rangle$, $\rho_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (0 \quad 1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Similarly, for the state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\rho_+ = |+\rangle\langle +| = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \left(\begin{array}{cc} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{array} \right) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$
- Till now we have described pure states only. There can be a more general scenario where mixture of states is possible. Say, the system is in state ρ_0 with probability p_0 and in the state $\rho_1 = |1\rangle\langle 1|$ with probability $p_1 = 1 - p_0$, then the density matrix ρ for this quantum system will be $\rho = p_0\rho_0 + p_1\rho_1$. Consider $p_0 = \frac{1}{2}$ and see that $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \rho_+ \Rightarrow$ mixed states are different from equal superposition states.

If $|\psi'\rangle = U|\psi\rangle$, then $\rho' = |\psi'\rangle\langle\psi'| = U|\psi\rangle\langle\psi|U^\dagger = U\rho U^\dagger \Rightarrow$ true for mixed states, too and extremely useful in simulation.



A mixed state in general: $\rho = \sum_{i=1}^n p_i \rho_i : \sum_i^n p_i = 1$.
For both pure state and mixed state $Tr(\rho) = 1$, but for pure state $Tr(\rho^2) = 1$, whereas for mixed state $Tr(\rho^2) < 1$.
In Bloch sphere, mixed states are the points inside the sphere whereas pure states are the points on the surface.

SATE SHIKSHA BHARAT
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Quantum Measurement

<https://andisama.medium.com/qubit-an-intuition-3-quantum-measurement-full-and-partial-qubits-969340a6fb3>

Suggested further readings

For the beginners:

- Pathak, Anirban. *Elements of quantum computation and quantum communication*. Boca Raton: CRC Press, 2013.

Specially learn partial trace and partial transpose from Chapter 3 of this book.

Only for advanced readers:

- Nielsen, Michael A., and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010.



SATE SHIKSHA BHARAT
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Section No. 1 ➔ Question No. 1

You Gained 1 out of 1 Score

What challenge do quantum computers face due to the loss of quantum coherence over time?

- Superposition collapse
- Entanglement failure
- Decoherence
- Quantum loss

Your Answer was right!

Section No. 1 ➔ Question No. 2

You Gained 1 out of 1 Score

In quantum computing, what phenomenon occurs when particles exhibit behavior such as passing through energy barriers, they classically shouldn't be able to overcome?

- Superposition
- Entanglement
- Interference
- Tunneling

Your Answer was right!

Title of course: Introduction to Quantum Computing
Module 1: Basics of quantum computing
Topic of session: Superposition in the quantum world

**Speaker Name: Anirban Pathak**

Qubits

<https://www.quantum-inspire.com/kbase/what-is-a-qubit/>

<https://www.aliroquantum.com/blog/qn-basics-introduction-to-qubits-with-real-world-examples>

Understand quantum superposition

Note: Unavailability of special basis to Eve leads to security in QKD. Superposition alone is not enough, we need superposition in the tensor product space and collapse on measurement

Applications of Superposition

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a state in superposition of states $|0\rangle$ and $|1\rangle$.

Note: Schrodinger equation is a linear differential equation and for every linear differential equation superposition of allowed solutions is also a solution. The same is true for Maxwell's equation, too.

In the context of quantum key distribution (QKD), particularly in protocols like BB84, special basis refers to the set of basis states used by the legitimate parties, Alice and Bob, to encode and decode quantum information. These basis states are typically chosen to be orthogonal, meaning they are distinguishable from each other in a measurement.

Now, let's consider Eve, the eavesdropper, who tries to intercept the quantum communication between Alice and Bob. If Eve does not know the basis in which the qubits are encoded, her task becomes significantly harder.

The special basis used by Alice and Bob plays a crucial role in QKD security by making it difficult for Eve to gain information without detection. Eve's inability to determine the correct basis reduces her chances of successfully eavesdropping on the quantum communication.

Unavailability of special basis to Eve leads to security in QKD. Superposition alone is not enough, we need superposition in the tensor product space and collapse on measurement.

Unavailability of Special Basis:

One of the fundamental concepts in QKD is that a quantum state cannot be measured or copied without disturbing it. This means that if Eve tries to measure the quantum state being transmitted, it will unavoidably disturb the state, thus introducing errors that can be detected by the legitimate parties, Alice and Bob.

Superposition:

Superposition is indeed a key concept, but as you mentioned, it's not enough on its own for security. Superposition allows quantum states to exist in multiple states simultaneously, which is used in QKD for encoding information. However,

superposition alone doesn't guarantee security because Eve could potentially intercept the quantum state and try to measure it without being detected.

Tensor Product Space:

In QKD, quantum states are often represented in a tensor product space, which means combining the states of multiple quantum systems. By using the tensor product, Alice and Bob can create entangled states or encode information in a higher-dimensional space, making it harder for Eve to eavesdrop without disturbing the state.

Collapse on Measurement:

The collapse of the wave function upon measurement is crucial for QKD security. When Bob measures the quantum state sent by Alice, the superposition collapses into one of the basis states. If Eve tries to intercept the quantum state, her measurement attempt will disturb the state, causing errors that can be detected by Alice and Bob during the reconciliation phase. By combining these principles, QKD protocols ensure that any attempt by Eve to gain information about the quantum state being transmitted will be detected, providing a secure means for generating shared secret keys between Alice and Bob.

- (The reconciliation phase is a crucial step in quantum key distribution (QKD) protocols, where Alice and Bob compare their raw key data to correct errors and discrepancies that may have been introduced during the transmission due to noise or eavesdropping.)

Schrödinger equation is a linear differential equation and for every linear differential equation superposition of allowed solution is also a solution. The same is true for Maxwell's equation too.

The Schrödinger equation and Maxwell's equations are both examples of linear differential equations, which means they obey the principle of superposition.

Schrödinger Equation:

The time-dependent Schrödinger equation for a single particle is:

$$i\hbar \frac{\partial}{\partial t} \Psi(\mathbf{r}, t) = \hat{H} \Psi(\mathbf{r}, t)$$

Where:

- $\Psi(\mathbf{r}, t)$ is the wavefunction of the particle.
- \hat{H} is the Hamiltonian operator.
- \hbar is the reduced Planck constant.

This equation describes how the wavefunction of a quantum system evolves over time. It is linear, meaning if $\Psi_1(\mathbf{r}, t)$ and $\Psi_2(\mathbf{r}, t)$ are solutions to the equation, then any linear combination of them, say $a\Psi_1(\mathbf{r}, t) + b\Psi_2(\mathbf{r}, t)$ where a and b are constants, is also a solution.

Maxwell's Equations:

Maxwell's equations describe the behavior of electric and magnetic fields in classical electromagnetism. In their differential form, they are:

1. Gauss's Law for electric fields:

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\epsilon_0}$$

2. Gauss's Law for magnetic fields:

$$\nabla \cdot \mathbf{B} = 0$$

3. Faraday's Law of electromagnetic induction:

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$$

4. Ampère-Maxwell Law:

$$\nabla \times \mathbf{B} = \mu_0 \mathbf{J} + \mu_0 \epsilon_0 \frac{\partial \mathbf{E}}{\partial t}$$

These equations describe how electric and magnetic fields interact with each other and with sources (charges and currents). They are also linear, meaning that if \mathbf{E}_1 and \mathbf{E}_2 (and similarly for \mathbf{B}_1 , \mathbf{B}_2) are solutions to Maxwell's equations, then any linear combination $a\mathbf{E}_1 + b\mathbf{E}_2$ (and similarly for \mathbf{B}) is also a solution.

Explanation:

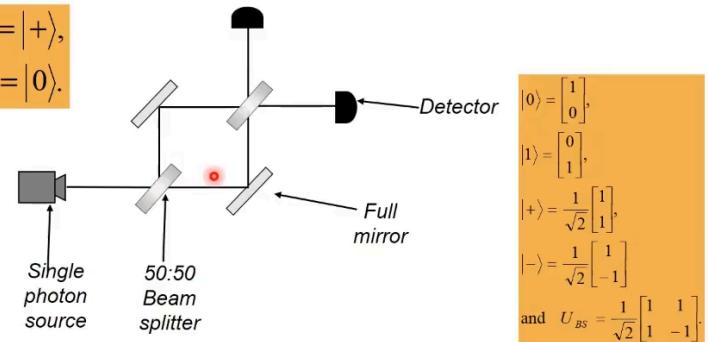
The linearity of these equations allows for the principle of superposition to hold. This means that if we have multiple solutions to these equations, we can add them together and still obtain a valid solution. This property is crucial in physics as it simplifies the analysis and allows for the construction of more complex solutions from simpler ones.

For example, in quantum mechanics, the principle of superposition allows for the construction of wavefunctions representing arbitrary quantum states by adding together simpler wavefunctions. In electromagnetism, superposition is essential for understanding phenomena like interference and diffraction, where fields from multiple sources combine.

Mach Zehnder Interferometer -

https://en.wikipedia.org/wiki/Mach%20Zehnder_interferometer

Understand quantum superposition through Mach–Zehnder interferometer

इति संस्कृत विद्यालय
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

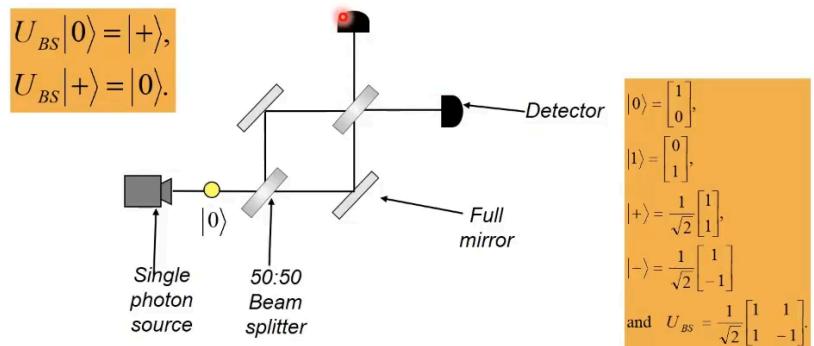
$$U|0\rangle = |+\rangle$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$$

$$U|+\rangle = |0\rangle$$

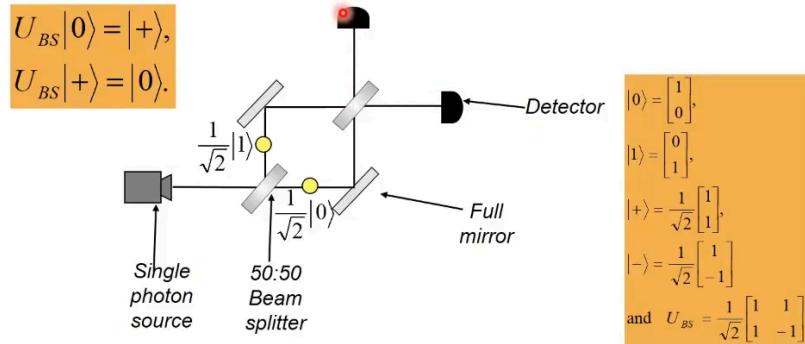
$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1+1 \\ 1-1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = |0\rangle$$

Understand quantum superposition through Mach–Zehnder interferometer

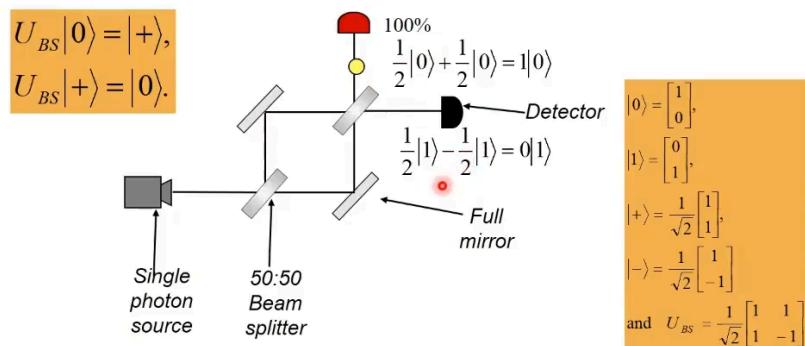
इति संस्कृत विद्यालय
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Understand quantum superposition through Mach-Zehnder interferometer

इन्हें संस्कृत भाषा में पढ़ने के लिए अधिक जानकारी।

Understand quantum superposition through Mach-Zehnder interferometer

इन्हें संस्कृत भाषा में पढ़ने के लिए अधिक जानकारी।

In Mach-Zehnder interferometers (MZIs), interference occurs when two coherent light beams interfere with each other after being split, then recombined. In constructive interference, the amplitudes of the two beams add up, leading to a higher intensity, while in destructive interference, they cancel each other out, resulting in a lower intensity.

Constructive Interference:

In constructive interference, the electric fields E_1 and E_2 of the two beams add up when they are recombined. The resulting electric field amplitude E_{total} is:

$$E_{\text{total}} = E_1 + E_2$$

The intensity of the combined beam, I_{total} , is proportional to the square of the electric field amplitude:

$$I_{\text{total}} \propto |E_{\text{total}}|^2 = |E_1 + E_2|^2$$

Destructive Interference:

In destructive interference, the electric fields E_1 and E_2 of the two beams cancel each other out when they are recombined. The resulting electric field amplitude E_{total} is:

$$E_{\text{total}} = E_1 - E_2$$

The intensity of the combined beam, I_{total} , is proportional to the square of the electric field amplitude:

$$I_{\text{total}} \propto |E_{\text{total}}|^2 = |E_1 - E_2|^2$$

Constructive Interference:

When the electric fields E_1 and E_2 are in phase (i.e., their peaks and troughs align), they add up, resulting in constructive interference. This increases the intensity of the combined beam.

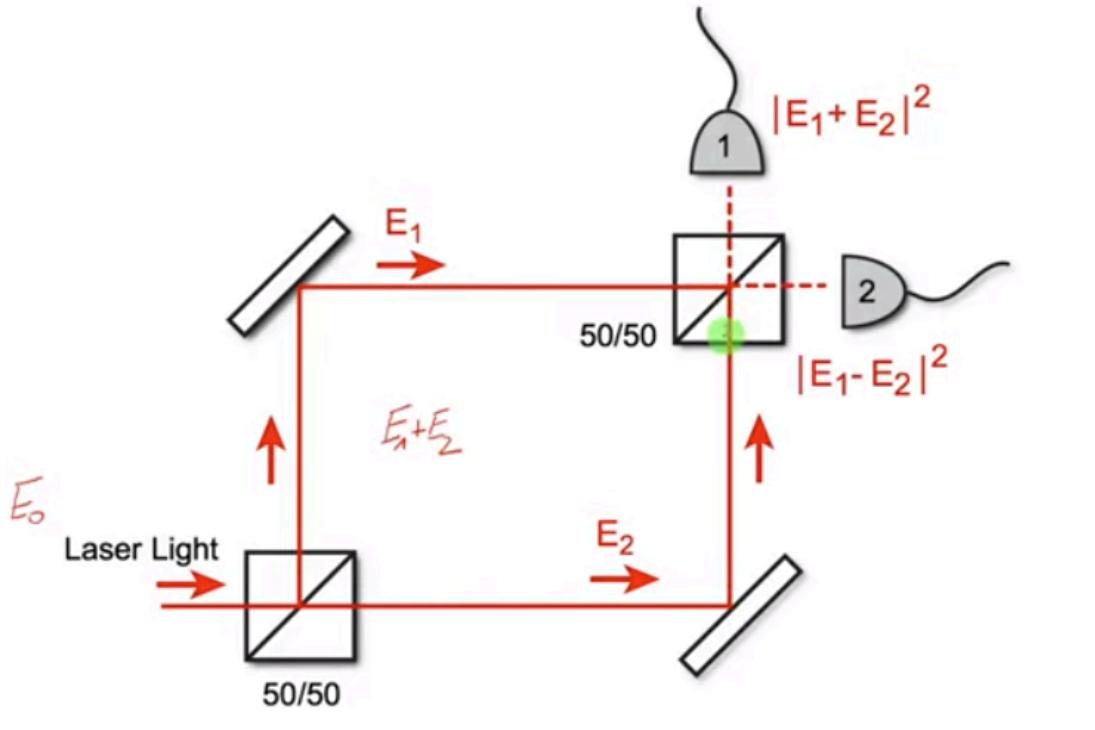
Destructive Interference:

When the electric fields E_1 and E_2 are out of phase (i.e., their peaks and troughs are misaligned), they cancel each other out, resulting in destructive interference. This decreases the intensity of the combined beam.

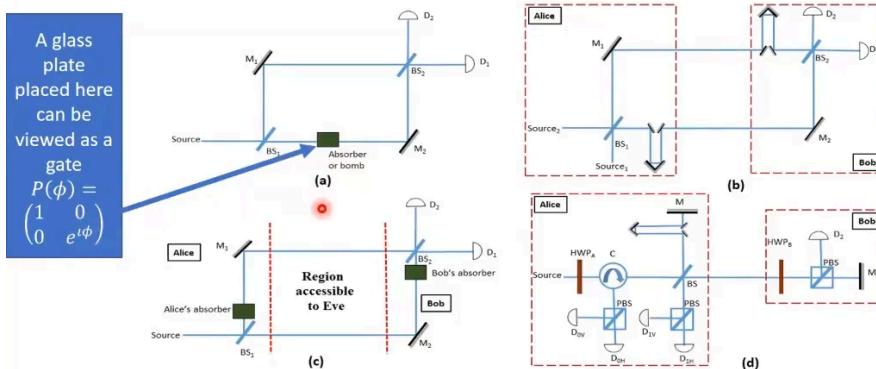
Importance in MZIs:

In an MZI, these interference effects are used to manipulate and control light. By adjusting the phase difference between the two paths, the interference can be tuned to be constructive or destructive. This property is exploited in various applications such as optical switches, modulators, and quantum information processing.

Mach-Zehnder Interferometer



Application of quantum superposition visualized through MZI and Michelson Interferometer



(a) A modified MZI. (b) A schematic diagram of MZI used to implement GV protocol. (c) Based on the idea of interaction free measurement a modified MZI can be used to realize Guo-Shi protocol of QKD. (d) Michelson interferometer is also used for counter-factual quantum communication.

 IIT BOMBAY RESEARCH FOUNDATION
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Fig(a): Modified MZI

If we direct project the photon beam on the bomb or the absorber, the bomb get explode. Thus we need MZI with application of superposition

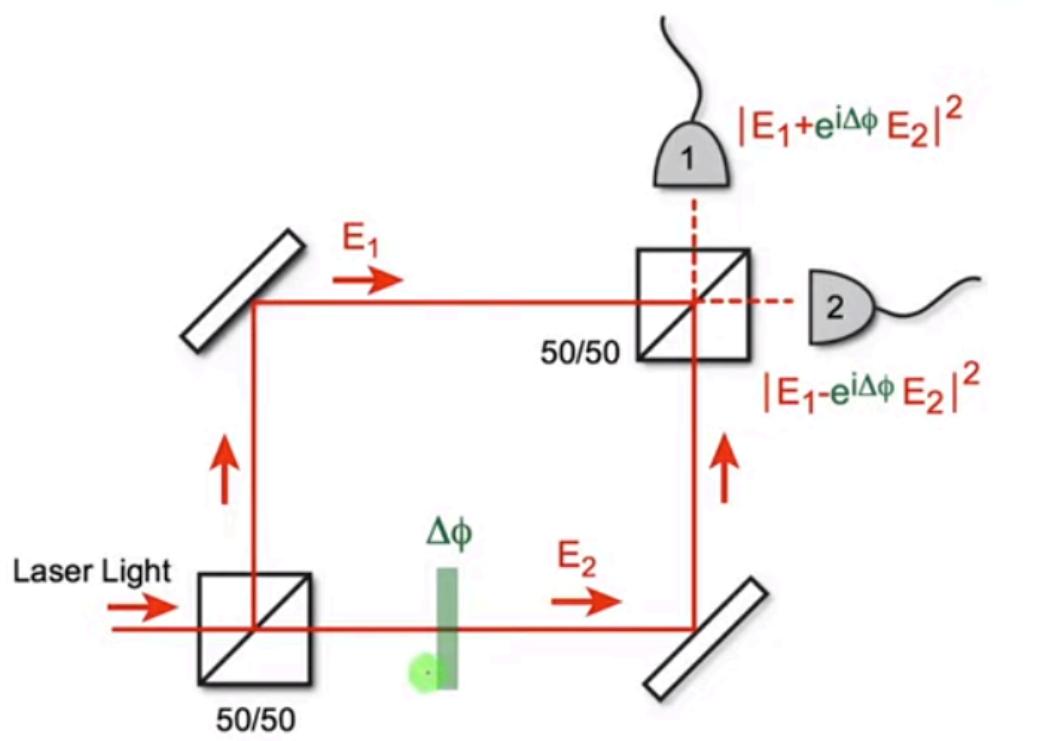
Operation Process:

- If there is no absorber (or inactive bomb), the photons follow two paths and then recombine. Due to constructive interference in the MZI, D2 detects photons.

- If the absorber (or bomb) is active, it absorbs 50% of the photons. The remaining 50% are redirected by the beam splitter and mirrors towards D1 and D2.
- At D1, 25% of the photons that were not absorbed by the absorber are detected. This indicates that the bomb is in an active state.
- At D2, only 25% of the original photons are detected.

In summary, the modified MZI with the absorber or bomb acts as a sensor for the active state of the bomb. D1 detects photons when the bomb is active, while D2 detects photons when the bomb is inactive. This setup combines interference phenomena with quantum measurement to provide information about the state of the absorber.

Mach-Zehnder Interferometer



Visualize use of linear algebra, quantum superposition, qubits, etc. in BB84 protocol for QKD

A photograph of a quantum optics experimental setup. A laser source on the left emits a beam through a series of optical components: a polarizer (labeled 'Alice's Laser Polarizer'), a beam splitter (BS), a lens (F), and a mirror (I). The beam then passes through a HWP (Half-Wave Plate) and a PBS (Polarization Beam Splitter). The light is split into two paths: one path goes through an AM (Analyzer) and a PM (Phase shifter) before reaching a detector labeled 'Bob's SPAD'. The other path goes through an AM before reaching the same detector. The setup is labeled 'Important for QKD'.

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$[M_+, M_0] = |+\rangle\langle+|0\rangle\langle0| - |0\rangle\langle0|+\rangle\langle+$$

$$= \frac{1}{\sqrt{2}}(|+\rangle\langle0| - |0\rangle\langle+|)$$

$$= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

$$= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

$$= \frac{1}{2} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq 0$$

IIT Kharagpur
CSD
Centre for Development of Advanced Computing

\$Non-commutativity:\$ One cannot simultaneously and accurately measure the values of two noncommuting observables.

Example 8.2: Consider the single qubit measurement operators in computational basis $\{|M_0\rangle = |0\rangle\langle0|, |M_1\rangle = |1\rangle\langle1|\}$ and in diagonal basis $\{|M_0\rangle = |+\rangle\langle+|, |M_1\rangle = |-\rangle\langle-|\}$. Now it is easy to check that

$$[M_0, M_1] = M_0 M_1 - M_1 M_0 = |0\rangle\langle0|1\rangle\langle1| - |1\rangle\langle1|0\rangle\langle0| = 0,$$

$$[M_+, M_-] = M_+ M_- - M_- M_+ = |+\rangle\langle+| - |-\rangle\langle-| = 0,$$

but

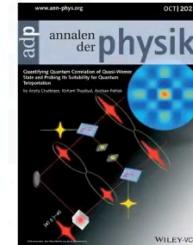
$$\begin{aligned} [M_+, M_0] &= M_+ M_0 - M_0 M_+ \\ &= |+\rangle\langle+|0\rangle\langle0| - |0\rangle\langle0|+\rangle\langle+| \\ &= \frac{|+\rangle\langle0| - |0\rangle\langle+|}{\sqrt{2}} \neq 0. \end{aligned}$$

Similarly, $[M_+, M_1] \neq 0$, $[M_-, M_0] \neq 0$, and $[M_-, M_1] \neq 0$. Thus we cannot simultaneously and accurately measure a state in computational basis and diagonal basis. This implies that we cannot simultaneously measure the polarization of a photon in vertical-horizontal basis and also in diagonal basis.

Wonderful things happen in the quantum world: one such phenomenon is teleportation

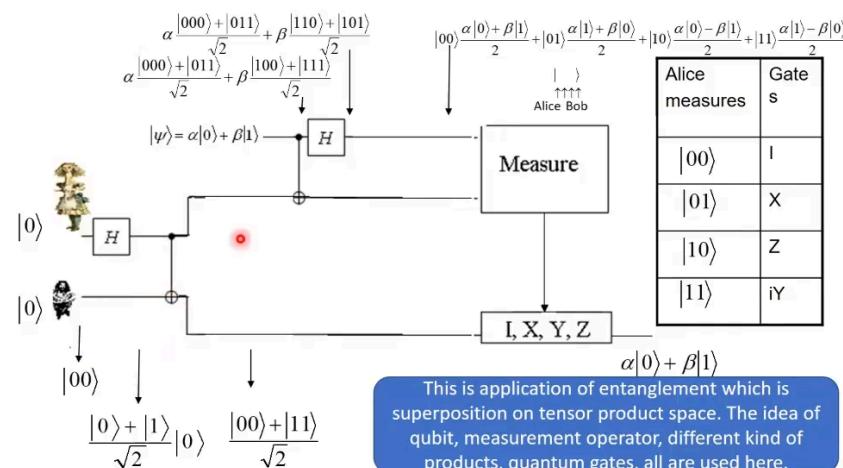


Cartoons used in this talk are from: Elements of Quantum Computation and Quantum Communication, A Pathak, CRC Press, Boca Raton, USA, (2013).



प्रति संस्कृत विद्यालय
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

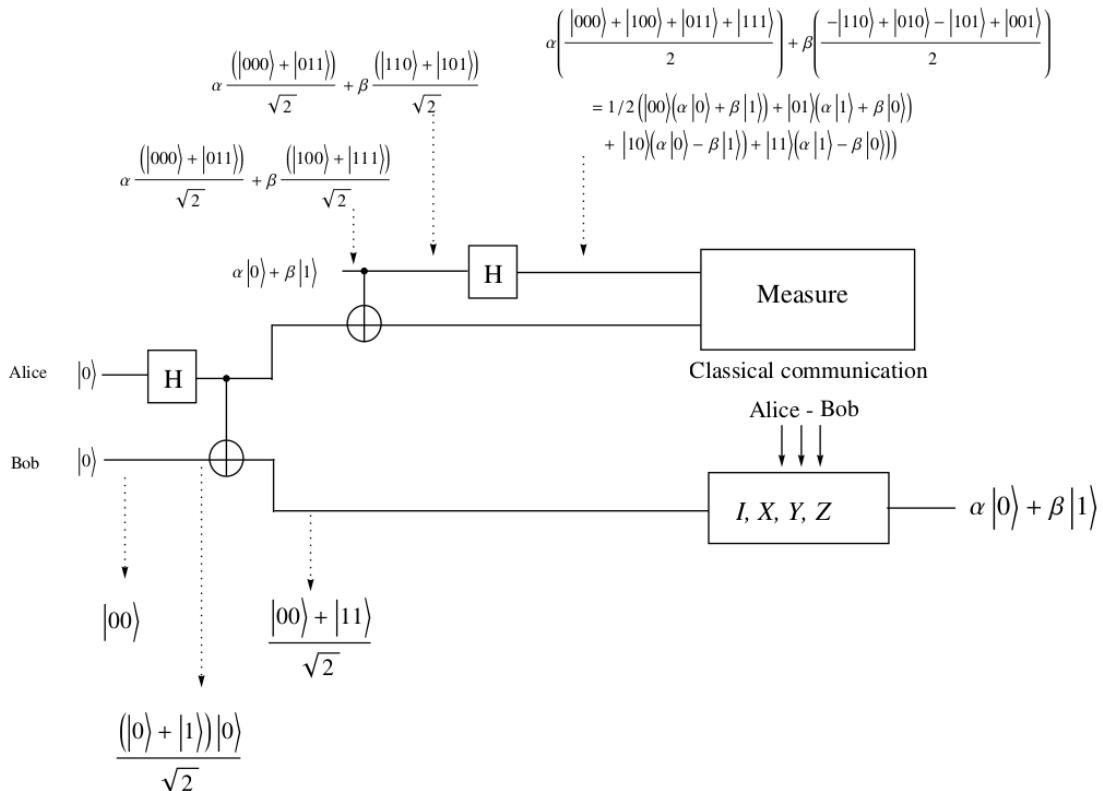
Quantum teleportation as an example where everything that we have learned is used



All quantum algorithms and quantum (physical) Turing machine exploits quantum superposition.



correct image



Section No. 1 Question No. 1

You Gained 1 out of 1 Score

Schrödinger's cat experiment is a thought experiment illustrating which concept?

- Quantum entanglement
- Superposition
- Quantum tunneling
- Quantum teleportation

Your Answer was right!

Section No. 1 Question No. 2

You Gained 1 out of 1 Score

What is the unique property of quantum bits (qubits) that allows them to exist in multiple states simultaneously?

- Entanglement
- Decoherence
- Superposition
- Tunneling

Your Answer was right!

Section No. 1 Question No. 3

You Gained 1 out of 1 Score

What phenomenon describes the interconnectedness between quantum particles, regardless of their separation distance?

- Superposition
- Entanglement
- Interference
- Tunneling

Your Answer was right!

Quantum Mechanics Postulates :

<https://www.sydney.edu.au/science/chemistry/~mjtj/CHEM3117/Resources/postulates.pdf>

https://chem.libretexts.org/Bookshelves/Physical_and_Theoretical_Chemistry_Textbook_I/

<https://web.mit.edu/8.05/handouts/jaffe1.pdf>

Introduction

- Quantum Mechanics is a mathematical framework for development of laws which a physical system must obey.
- The postulates of quantum mechanics provides a connection between physical world and mathematical formalism of quantum mechanics.
- We will study 3 important postulates:
 - State space Postulate
 - Evolution Postulate and
 - Measurement Postulate



SIDDHIVINAYAK RAI
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

State Space Postulate

A quantum mechanical system is completely described by a wavefunction $\Psi(r, t)$.

Born interpretation:

$\Psi^*(r, t)\Psi(r, t)$ gives probability density of particle at position r and time t.

$\Psi^*(r, t)\Psi(r, t) dx dy dz$ gives probability that the particle is in infinitesimally small volume element $d\tau$ at t

$$|\Psi|^2 d\tau$$

The state of an isolated physical system is completely described by unit vector $|\psi\rangle$ in Hilbert Space.



SIDDHIVINAYAK RAI
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

State Space Postulate



A qubit is the simplest quantum mechanical system with 2-dimensional state space.

We need two orthonormal basis vectors to describe an arbitrary state in this state space:

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

Therefore, the arbitrary qubit is described as $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, where α and β are complex nos.

Normalization constraint: $|\alpha|^2 + |\beta|^2 = 1$

A linear combination $\sum_i \alpha_i |\psi_i\rangle$ is a superposition of states $|\psi_i\rangle$ with amplitude α_i for state $|\psi_i\rangle$

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

The state of the system is in superposition of state $|0\rangle$ and $|1\rangle$ with amplitude

$\frac{1}{\sqrt{2}}$ for state $|0\rangle$ and amplitude $\frac{1}{\sqrt{2}}$ for state $|1\rangle$



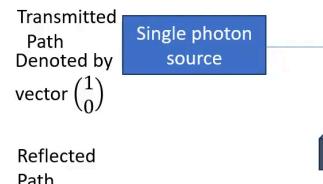
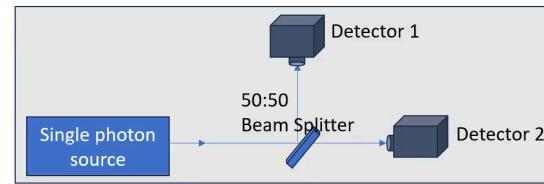
Dr. S. Suganya
Centre for Development of Advanced Computing

State Space Postulate



A quantum mechanical 2-level system can be a simple photon that can be a single photon that can be found in one of the distinct paths.

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



When photon starts out in path 0 then after passing through the beamsplitter:

$$\begin{aligned} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{i}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned}$$



Dr. S. Suganya
Centre for Development of Advanced Computing

Several different physical implementations of qubits are possible. A number of examples are the polarizations of a photon, two of the (multiple) discrete energy levels of an ion, a superconducting Transmon qubit, the nuclear spin states of an atom or the spin states of an electron.

Evolution Postulate



Evolution postulate: The time evolution of the state of a closed quantum system is described by a unitary transformation. To be precise, if the states of a closed quantum system at two different time t_1 and t_2 are $|\Psi_1\rangle$ and $|\Psi_2\rangle$ respectively then $|\Psi_1\rangle$ and $|\Psi_2\rangle$ are related by a unitary operator U such that

$$|\Psi_2\rangle = U |\Psi_1\rangle, \quad \text{---(1)}$$

where U depends on times t_1 and t_2 only.

Now, a continuous time evolution of a closed quantum system is given by the time dependent Schrodinger equation

$$H|\Psi\rangle = i\hbar \frac{d}{dt} |\Psi\rangle \quad \text{---(2)}$$

The solutions of this equation for a time-independent Hamiltonian at time t_1 and t_2 are related by

$$|\Psi_2\rangle = e^{-iH\hbar(t_2-t_1)} |\Psi_1\rangle. \quad \text{-----(3)}$$

Now it is easy to observe that

$$U = e^{-iH\hbar(t_2-t_1)}$$

is a unitary operator since H is a Hermitian operator. Thus the evolution postulate follows from the Schrodinger equation.



Dr. S. S. Venkateswaran
Centre for Department of Advanced Computing

Evolution Postulate



Consider unitary evolution operator operating on a single qubit.

- Pauli Operator $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $X |0\rangle \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv |1\rangle$
- $X |1\rangle \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv |0\rangle$

- Hadamard operator $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- $H |0\rangle \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
- $H |1\rangle \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}}$



Dr. S. S. Venkateswaran
Centre for Department of Advanced Computing

Measurement Postulate



Measurement postulate: A generalized quantum measurement is described by a set of measurement operators $\{M_m\}$, which operates on the state of the system to be measured. The label m refers to a particular outcome of the measurement.

The state of quantum system before the exp is $|\Psi\rangle$ then the probability that result m occurs is

$$p(m) = \langle \Psi | M_m^\dagger M_m | \Psi \rangle \quad \text{(4)}$$

and the state of the system after the measurement is

$$\frac{M_m |\Psi\rangle}{\sqrt{p(m)}} = \frac{M_m |\Psi\rangle}{\sqrt{\langle \Psi | M_m^\dagger M_m | \Psi \rangle}} \quad \text{(5)}$$

The measurement operators satisfy a completeness relation of the form $\sum_m M_m^\dagger M_m = I$.



Dr. S. S. Venkateswaran
Centre for Department of Advanced Computing

Measurement Postulate



We would like to provide a simple example to clarify the meaning of measurement operator.

Consider that the quantum measurement in two dimensions is described by the set of operators

$$\{M_0, M_1 : M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}. \quad \dots\dots (6)$$

Suppose these operators are used to measure the state of the qubit described by

$$(\alpha|0\rangle + \beta|1\rangle), \quad \dots\dots (7)$$

then the probability of getting $|0\rangle$ as the outcome is $p(0) = (\langle 0|\alpha^* + \langle 1|\beta^*) (|0\rangle\langle 0|0\rangle)(\alpha|0\rangle + \beta|1\rangle) = |\alpha|^2$

and the probability of getting $|1\rangle$ as the output is $p(1) = |\beta|^2$.

Since global phase is unimportant, the state of the system after the measurement is

$$\text{Either } \frac{M_0(\alpha|0\rangle + \beta|1\rangle)}{\sqrt{p(0)}} = \frac{|0\rangle\langle 0|\sqrt{(\alpha|0\rangle + \beta|1\rangle)}}{\sqrt{p(0)}} = \frac{\alpha}{\sqrt{|\alpha|^2}}|0\rangle \approx |0\rangle \quad \text{or} \quad \frac{M_1(\alpha|0\rangle + \beta|1\rangle)}{\sqrt{p(1)}} = \frac{|1\rangle\langle 1|\sqrt{(\alpha|0\rangle + \beta|1\rangle)}}{\sqrt{p(1)}} = \frac{\beta}{\sqrt{|\beta|^2}}|1\rangle.$$

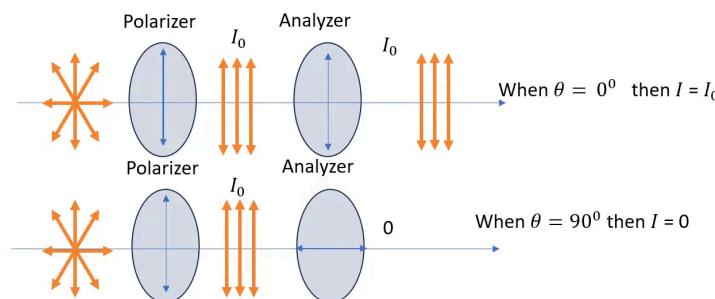
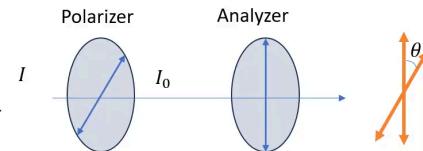


Measurement Postulate



$$\text{Malus Law: } \frac{I_0}{I} = \cos^2(\theta)$$

θ is the angle between transmission axis of Polarizer and Analyzer



When $\theta = 0^\circ$ then $I = I_0$

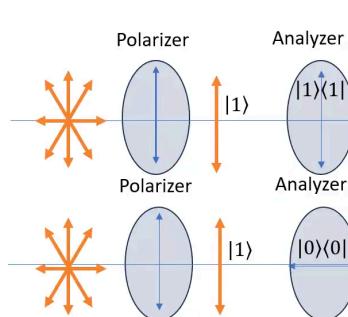
When $\theta = 90^\circ$ then $I = 0$

Measurement Postulate



$$|1\rangle \leftrightarrow |0\rangle$$

$$\begin{array}{cc} \text{Analyzer 1} & \text{Analyzer 2} \\ |1\rangle\langle 1| & |0\rangle\langle 0| \end{array}$$



$$p(|1\rangle) = \langle 1|1\rangle\langle 1|1\rangle = 1$$

the state of the system after the measurement is $\frac{M_m|\Psi\rangle}{\sqrt{p(m)}} = |1\rangle$

$\rightarrow p(|0\rangle) = \langle 1|0\rangle\langle 0|1\rangle = 0$
the state of the system after the measurement is *nil*

Experiment 1

When the diagonal state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ passes through the analyzer $|1\rangle\langle 1|$, we compute the inner product between the state and the analyzer:

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \cdot |1\rangle\langle 1| = \left(\frac{|0\rangle\langle 1|1\rangle+|1\rangle\langle 1|1\rangle}{\sqrt{2}}\right)$$

Since $\langle 1|1\rangle=1$, this simplifies to:

$$\left(\frac{|0\rangle\langle 1|1\rangle+|1\rangle\langle 1|1\rangle}{\sqrt{2}}\right) = \frac{|1\rangle}{\sqrt{2}}$$

So, the result after passing through the analyzer $|1\rangle\langle 1|$ is $\frac{|1\rangle}{\sqrt{2}}$

In []:

Experiment 2

When the diagonal state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ passes through the analyzer $|0\rangle\langle 0|$, we compute the inner product between the state and the analyzer:

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \cdot |0\rangle\langle 0| = \left(\frac{|0\rangle\langle 0|0\rangle+|1\rangle\langle 0|0\rangle}{\sqrt{2}}\right)$$

Since $\langle 0|0\rangle=1$ and $\langle 1|0\rangle=0$, this simplifies to:

$$\left(\frac{|0\rangle\langle 0|0\rangle+|1\rangle\langle 0|0\rangle}{\sqrt{2}}\right) = \frac{|0\rangle}{\sqrt{2}}$$

So, the result after passing through the analyzer $|0\rangle\langle 0|$ is $\frac{|0\rangle}{\sqrt{2}}$

In []:

Experiment 3

Take quantum state $|1\rangle$ and use a diagonal analyser with addition of 45 degree

To apply a diagonal analyzer with an addition of 45 degrees to the quantum state $|1\rangle$, we first need to express the diagonal analyzer in the computational basis.

The diagonal analyzer with an addition of 45 degrees can be represented as:

$$A = \begin{pmatrix} \cos(45^\circ) & -\sin(45^\circ) \\ \sin(45^\circ) & \cos(45^\circ) \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

Now, we apply the quantum state $|1\rangle$ to the analyzer:

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

$$A \cdot |1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

So, when the quantum state $|1\rangle$ passes through the diagonal analyzer with an addition of 45 degrees, the resulting state is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$

1. Practice Quiz

Section No. 1 Question No. 1

You Gained 1 out of 1 Score

In the double-slit experiment, particles demonstrate particle nature when

- Both slits are open and interference patterns are observed.
- Both slits are open and a single bright band is observed on the screen.
- Only one slit is open and a diffraction pattern is observed.
- Both slits are closed and no interference pattern is observed.

Your Answer was right!

1. Practice Quiz

Section No. 1 Question No. 2

You Gained 1 out of 1 Score

Which quantum gate is commonly used to create superposition of qubits?

- Hadamard gate (H gate)
- CNOT gate (Controlled-NOT gate)
- Pauli-X gate (X gate)
- Toffoli gate (CCNOT gate)

Your Answer was right!

Lab 1: Programming with Qiskit

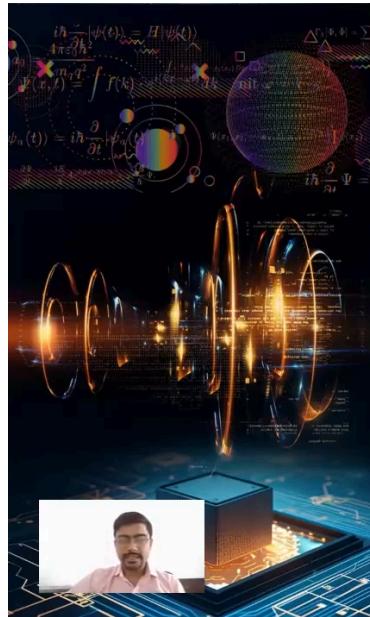
1. Prerequisite: Install Anaconda
 2. Create an environment
 3. Install Qiskit SDK
 4. Install Qiskit Runtime (to run jobs on quantum hardware)
 5. Install Qiskit[visualization]
 6. Install Qiskit Aer
 7. Create IBM Quantum Experience Account (<https://quantum.ibm.com/>)
 8. Copy your API token

Command Prompt Instructions:

```

1. conda create --name lab
2. conda activate lab
3. conda install python
4. pip install qiskit
5. pip install qiskit-ibm-runtime
6. pip install qiskit[visualization]
7. pip install qiskit-aer
    
```

IBM Quantum Experience Account will give you access to a cloud-based quantum computing platform with Open Plan: Up to 10 minutes/month



Outline

- IBM Quantum Composer
 - Overview
 - Interface
 - Visualizations
 - Basic Quantum Circuit

<https://quantum.ibm.com/>

4/6/2024 CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING 3
विश्व विद्यालय संसदीय केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

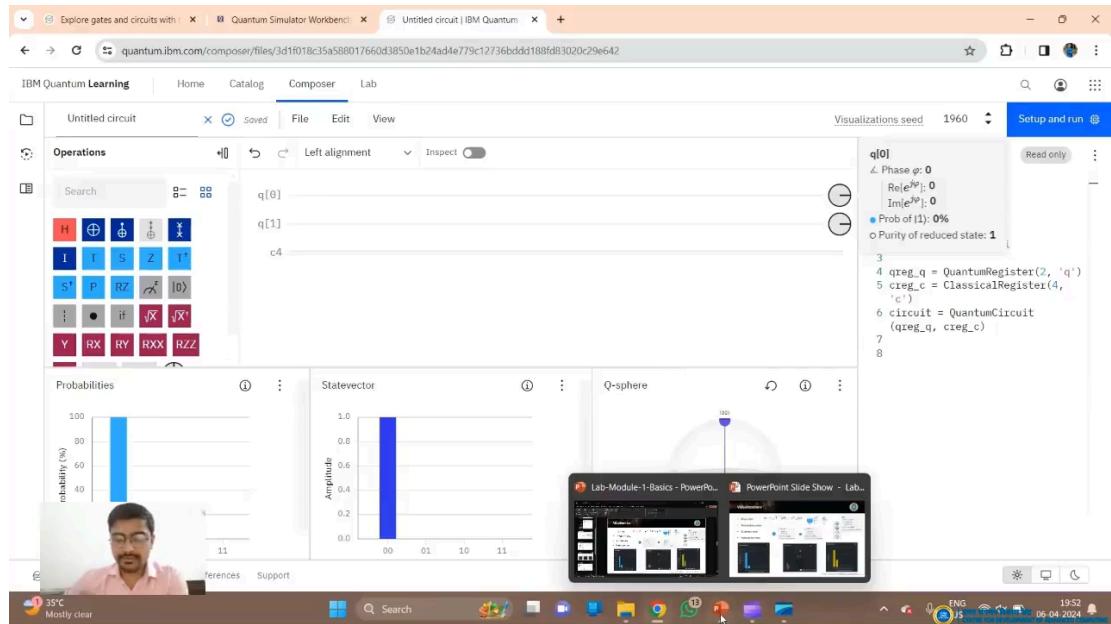
IBM Quantum Composer -

<https://learning.quantum.ibm.com/tutorial/explore-gates-and-circuits-with-the-quantum-composer#what-is-it>

The screenshot shows the IBM Quantum Composer interface. At the top, it says "IBM Quantum Composer". Below that is the "IBM Quantum Platform" dashboard, which includes a video player showing a person speaking, a "Platform" section with an API token, and a "Compute resources" section. To the right is a sidebar titled "IBM Quantum" with sections for "Sign in to IBM Quantum" (with a "Continue with IBMid" button), "New to IBM Quantum?", and "Having trouble signing in?". A blue box on the right lists features: "✓ Visualize qubit states", "✓ Run on quantum hardware", and "✓ Automatically generate code".

Build Quantum Circuit -

<https://learning.quantum.ibm.com/tutorial/explore-gates-and-circuits-with-the-quantum-composer#build-edit-and-inspect-quantum-circuits>



Run Circuits -

<https://learning.quantum.ibm.com/tutorial/explore-gates-and-circuits-with-the-quantum-composer#run-circuits-and-view-results>

Visualizations -

<https://learning.quantum.ibm.com/tutorial/explore-gates-and-circuits-with-the-quantum-composer#visualizations>

The screenshot highlights various visualization components. At the top, a "Visualizations" section lists: Phase disk, Probabilities view, Q-sphere view, and Statevector view. Below this, four detailed views are shown: 1) Phase disk showing a blue circle with a central dot; 2) Probabilities view showing a bar chart with a single bar at index 00; 3) Q-sphere view showing a 3D sphere with a point at the top; 4) Statevector view showing a bar chart with two bars at indices 00 and 01. The right side of the interface shows a summary of the current state: q[0] has phase 0, Re[e^{jφ}] = 0, Im[e^{jφ}] = 0, and probability of |1⟩ is 0%. The overall purity of the reduced state is 1.

Composer operations -

<https://learning.quantum.ibm.com/tutorial/explore-gates-and-circuits-with-the-quantum-composer#composer-operations-glossary>

Basic Quantum Circuit

Qiskit v Read only

```
1 from qiskit import
2 QuantumRegister,
3 ClassicalRegister,
4 QuantumCircuit
5 from numpy import pi
6
7 qreg_q = QuantumRegister(2, 'q')
8 creg_c = ClassicalRegister(4, 'c')
9
10 circuit = QuantumCircuit
11 (qreg_q, creg_c)
12
13 circuit.h(qreg_q[0])
14 circuit.cx(qreg_q[0], qreg_q[1])
15 circuit.measure(qreg_q[0], creg_c[0])
```

Operations

Probabilities

Statevector

Q-sphere

4/6/2024 CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING 7