Introduction to Quantum Computation

Part - I

Ritajit Majumdar, Arunabha Saha

University of Calcutta

September 9, 2013

Classical Computation vs Quantum Computation

- It may be tempting to say that a quantum computer is one whose operation is governed by the laws of quantum mechanics. But since the laws of quantum mechanics govern the behaviour of all physical phenomena, this temptation must be resisted.

Classical Computation vs Quantum Computation

- It may be tempting to say that a quantum computer is one whose operation is governed by the laws of quantum mechanics. But since the laws of quantum mechanics govern the behaviour of all physical phenomena, this temptation must be resisted.
- Moore's law roughly stated that computer power will double for constant cost approximately once every two years. This worked well for a long time. However, at present, quantum effects are beginning to interfere in the functioning of electronic devices as they are made smaller and smaller.

Classical Computation vs Quantum Computation

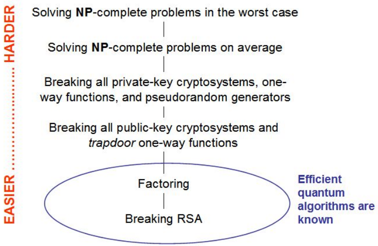
- It may be tempting to say that a quantum computer is one whose operation is governed by the laws of quantum mechanics. But since the laws of quantum mechanics govern the behaviour of all physical phenomena, this temptation must be resisted.
- Moore's law roughly stated that computer power will double for constant cost approximately once every two years. This worked well for a long time. However, at present, quantum effects are beginning to interfere in the functioning of electronic devices as they are made smaller and smaller.
- One possible solution is to move to a different computing paradigm. One such paradigm is provided by the theory of quantum computation, which is based on the idea of using quantum mechanics to perform computations, instead of classical physics.

Classical Computation vs Quantum Computation

- Quantum systems are exponentially powerful. A system of 500 particles has 2^{500} "computing power". Quantum Computers provide a neat shortcut for solving a range of mathematical tasks known as NP-complete problems.

Classical Computation vs Quantum Computation

- Quantum systems are exponentially powerful. A system of 500 particles has 2^{500} "computing power". Quantum Computers provide a neat shortcut for solving a range of mathematical tasks known as NP-complete problems.
- For example, factorisation is an exponential time task for classical computers. But Shor's quantum algorithm for factorisation is a polynomial time algorithm. It has successfully broken RSA cryptosystem.



Motivations for Quantum Computation

- Faster than light (?) communication.

Motivations for Quantum Computation

- Faster than light (?) communication.
- Highly parallel and efficient quantum algorithms.

Motivations for Quantum Computation

- Faster than light (?) communication.
- Highly parallel and efficient quantum algorithms.
- Quantum Cryptography.

Motivations for Quantum Computation

- Faster than light (?) communication.
- Highly parallel and efficient quantum algorithms.
- Quantum Cryptography.
- and many more...

Qubits: The building blocks of Quantum Computer

In classical computer, bits of digital information are either 0 or 1. In a quantum computer, these bits are replaced by a "superposition" of both 0 and 1.

[1] or their linear combination.

Qubits: The building blocks of Quantum Computer

In classical computer, bits of digital information are either 0 or 1. In a quantum computer, these bits are replaced by a "superposition" of both 0 and 1.

Qubits are represented as $|0\rangle$ and $|1\rangle$ [1]. Qubits have been created in the laboratory using photons, ions and certain sorts of atomic nuclei.

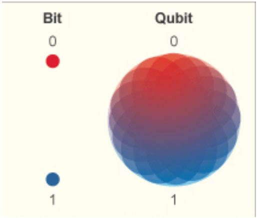
[1] or their linear combination.

Superposition Principle

Suppose we have a k-level system. So there are k distinguishable or classical states for the system.
The possible classical states for the system: $0, 1, ..., k-1$.

Superposition Principle

If a quantum system can be in one of k states, it can also be in any linear superposition of those k states.



A bit can only be a 0 or 1

Superposition can be represented anywhere on a sphere.

Superpostition Principle

$|0\rangle$, $|1\rangle$, ..., $|k-1\rangle$ are called the basis states. The superposition is denoted as a linear combination of these basis.

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle + ... + \alpha_{k-1} |k-1\rangle$$

where,

$$\alpha_i \in \mathbf{C}$$

$$\sum_i |\alpha_i|^2 = 1$$

(more on this later)

Two level systems are called **qubits**. (k = 2)

Qubit: Physical Interpretation

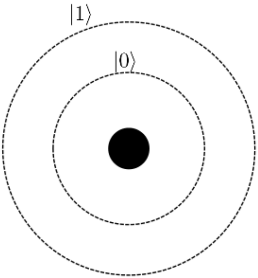
- We may have various interpretations of qubits.

Qubit: Physical Interpretation

- We may have various interpretations of qubits.
- Consider a Hydrogen atom. This atom may be treated as a qubit. To do so, we define the ground energy state of the electron as $|0\rangle$ and the first energy state as $|1\rangle$.

Qubit: Physical Interpretation

- We may have various interpretations of qubits.
- Consider a Hydrogen atom. This atom may be treated as a qubit. To do so, we define the ground energy state of the electron as $|0\rangle$ and the first energy state as $|1\rangle$.
- The electron dwells in some linear superposition of these two energy levels. But during measurement, we shall find the electron in any one of the energy states.



Other examples of Qubits

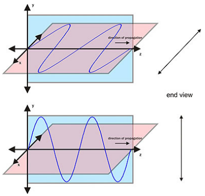


Figure : Photon Polarization: The orientation of electrical field oscillation is either horizontal or vertical.

Other examples of Qubits

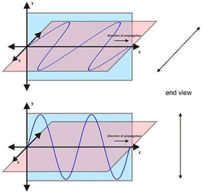


Figure : Photon Polarization: The orientation of electrical field oscillation is either horizontal or vertical.

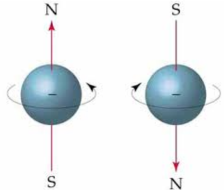


Figure : Electron spin: The spin is either up or down

Qubit: Mathematical model

Mathematically, a quantum state (which, as we shall see later, is a vector) is represented by a column matrix. The two fundamental states that we introduced before, $|0\rangle$ and $|1\rangle$ form an orthonormal basis. We shall see more of orthonormality when we see inner products.

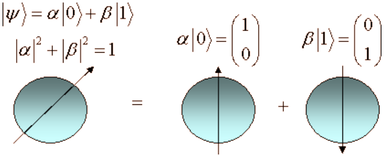
The matrix representation of $|0\rangle$ and $|1\rangle$:

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

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

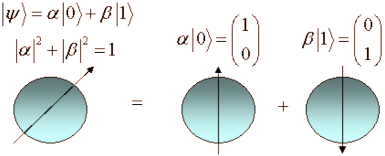
Qubit: Mathematical model

So a general quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is represented as



Qubit: Mathematical model

So a general quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is represented as



The matrix notation will be

$$|\psi\rangle = \begin{bmatrix} \alpha + 0 \\ 0 + \beta \end{bmatrix}$$

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

Qubit: Sign Basis

$|0\rangle$ and $|1\rangle$ are called bit basis since they can be thought of as the quantum counter-parts of classical bits 0 and 1 respectively. However, they are not the only possible basis. We may have infinitely many orthonormal basis for a given space.

Another basis, called the sign basis, is denoted as $|+\rangle$ and $|-\rangle$.

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

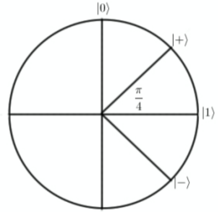


Figure : Geometrical model of bit basis and sign basis

Qubit: Change of Basis

Measure $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ in $|+\rangle / |-\rangle$ basis.

Qubit: Change of Basis

Measure $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ in $|+\rangle/|-\rangle$ basis.

It can be checked that:

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

Qubit: Change of Basis

Measure $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ in $|+\rangle/|-\rangle$ basis.

It can be checked that:

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

$|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$

Qubit: Change of Basis

Measure $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ in $|+\rangle/|-\rangle$ basis.

It can be checked that:

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

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \\ &= \frac{1}{2}\left(\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\right) + \frac{\sqrt{3}}{2}\left(\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\right) \end{aligned}$$

Qubit: Change of Basis

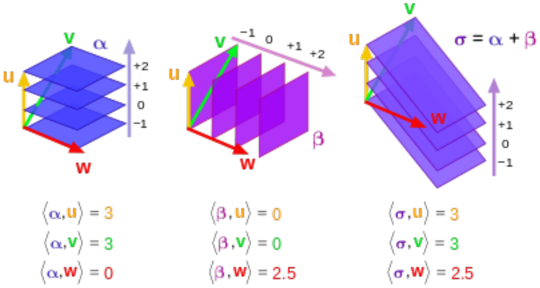
Measure $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ in $|+\rangle/|-\rangle$ basis.

It can be checked that:

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

$$\begin{aligned}|\psi\rangle &= \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \\ &= \frac{1}{2}\left(\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\right) + \frac{\sqrt{3}}{2}\left(\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\right) \\ &= \left(\frac{1}{2\sqrt{2}} + \frac{\sqrt{3}}{2\sqrt{2}}\right)|+\rangle + \left(\frac{1}{2\sqrt{2}} - \frac{\sqrt{3}}{2\sqrt{2}}\right)|-\rangle\end{aligned}$$

Linear Algebra



Linear Algebra

A very short introduction

Vector Space

A **vector space** consists of **vectors**($|\alpha\rangle, |\beta\rangle, |\gamma\rangle$), together with a set of **scalars**(a, b, c,....)[2], which is **closed** under two operations:

- Vector addition

[2] the scalars can be complex numbers

Vector Space

A **vector space** consists of **vectors**($|\alpha\rangle, |\beta\rangle, |\gamma\rangle$), together with a set of **scalars**(a, b, c,....)[2], which is **closed** under two operations:

- Vector addition
- Scalar multiplication

[2] the scalars can be complex numbers

Vector Addition

- The sum of any two vectors is another vector

$$|\alpha\rangle + |\beta\rangle = |\gamma\rangle$$

[3] $|0\rangle$ and 0 are different

Vector Addition

- The sum of any two vectors is another vector

$$|\alpha\rangle + |\beta\rangle = |\gamma\rangle$$

- Vector addition is **commutative**

$$|\alpha\rangle + |\beta\rangle = |\beta\rangle + |\alpha\rangle$$

[3] $|0\rangle$ and 0 are different

Vector Addition

- The sum of any two vectors is another vector

$$|\alpha\rangle + |\beta\rangle = |\gamma\rangle$$

- Vector addition is **commutative**

$$|\alpha\rangle + |\beta\rangle = |\beta\rangle + |\alpha\rangle$$

- It is **associative** also

$$|\alpha\rangle + (|\beta\rangle + |\gamma\rangle) = (|\alpha\rangle + |\beta\rangle) + |\gamma\rangle$$

[3] $|0\rangle$ and 0 are different

Vector Addition

- The sum of any two vectors is another vector

$$|\alpha\rangle + |\beta\rangle = |\gamma\rangle$$

- Vector addition is **commutative**

$$|\alpha\rangle + |\beta\rangle = |\beta\rangle + |\alpha\rangle$$

- It is **associative** also

$$|\alpha\rangle + (|\beta\rangle + |\gamma\rangle) = (|\alpha\rangle + |\beta\rangle) + |\gamma\rangle$$

- There exists a **zero**(or **null**) **vector**[3] with the property

$$|\alpha\rangle + |0\rangle = |\alpha\rangle\,, \quad \forall\,|\alpha\rangle$$

[3] $|0\rangle$ and 0 are different

Vector Addition

- The sum of any two vectors is another vector

$$|\alpha\rangle + |\beta\rangle = |\gamma\rangle$$

- Vector addition is **commutative**

$$|\alpha\rangle + |\beta\rangle = |\beta\rangle + |\alpha\rangle$$

- It is **associative** also

$$|\alpha\rangle + (|\beta\rangle + |\gamma\rangle) = (|\alpha\rangle + |\beta\rangle) + |\gamma\rangle$$

- There exists a **zero**(or **null**) **vector**[3] with the property

$$|\alpha\rangle + |0\rangle = |\alpha\rangle\,, \quad \forall\,|\alpha\rangle$$

- For every vector $|\alpha\rangle$ there is an **associative inverse vector**($|-\alpha\rangle$) such that

$$|\alpha\rangle + |-\alpha\rangle = |0\rangle$$

[3] $|0\rangle$ and 0 are different

Scalar Multiplication

- The product of any scalar with any vector is another vector

$$a\,|\alpha\rangle = |\gamma\rangle$$

Scalar Multiplication

- The product of any scalar with any vector is another vector

$$a|\alpha\rangle = |\gamma\rangle$$

- Scalar multiplication is **distributive** w.r.t vector addition

$$a(|\alpha\rangle + |\beta\rangle) = a|\alpha\rangle + a|\beta\rangle$$

Scalar Multiplication

- The product of any scalar with any vector is another vector

$$a\,|\alpha\rangle = |\gamma\rangle$$

- Scalar multiplication is **distributive** w.r.t vector addition

$$a(|\alpha\rangle + |\beta\rangle) = a\,|\alpha\rangle + a\,|\beta\rangle$$

- And with respect to scalar addition also

$$(a + b)\,|\alpha\rangle = a\,|\alpha\rangle + b\,|\alpha\rangle$$

Scalar Multiplication

- The product of any scalar with any vector is another vector

$$a\,|\alpha\rangle = |\gamma\rangle$$

- Scalar multiplication is **distributive** w.r.t vector addition

$$a(|\alpha\rangle + |\beta\rangle) = a\,|\alpha\rangle + a\,|\beta\rangle$$

- And with respect to scalar addition also

$$(a+b)\,|\alpha\rangle = a\,|\alpha\rangle + b\,|\alpha\rangle$$

- It is also **associative** w.r.t ordinary scalar multiplication

$$a(b\,|\alpha\rangle) = (ab)\,|\alpha\rangle$$

Scalar Multiplication

- The product of any scalar with any vector is another vector

$$a\,|\alpha\rangle = |\gamma\rangle$$

- Scalar multiplication is **distributive** w.r.t vector addition

$$a(|\alpha\rangle + |\beta\rangle) = a\,|\alpha\rangle + a\,|\beta\rangle$$

- And with respect to scalar addition also

$$(a+b)\,|\alpha\rangle = a\,|\alpha\rangle + b\,|\alpha\rangle$$

- It is also **associative** w.r.t ordinary scalar multiplication

$$a(b\,|\alpha\rangle) = (ab)\,|\alpha\rangle$$

- Multiplication by scalars 0 and 1 has the effect

$$0\,|\alpha\rangle = |0\rangle\,; \quad 1\,|\alpha\rangle = |\alpha\rangle$$

Basis Vectors

Linear combination of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,... is of the form

$$|\alpha\rangle + |\beta\rangle + |\gamma\rangle + \dots$$

- A vector $|\lambda\rangle$ is said to be **linearly independent** of the set of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$, $\dots$, if it cannot be written as a linear combination of them.

Basis Vectors

Linear combination of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,... is of the form

$$|\alpha\rangle + |\beta\rangle + |\gamma\rangle + \dots$$

- A vector $|\lambda\rangle$ is said to be **linearly independent** of the set of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,$\dots$,if it cannot be written as a linear combination of them.
- A *set* of vectors is **linearly independent** if each one is independent of all the rest.

Basis Vectors

Linear combination of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,... is of the form

$$|\alpha\rangle + |\beta\rangle + |\gamma\rangle + \dots$$

- A vector $|\lambda\rangle$ is said to be **linearly independent** of the set of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,$\dots$,if it cannot be written as a linear combination of them.
- A *set* of vectors is **linearly independent** if each one is independent of all the rest.
- If every vector can be written as a linear combination of members of this set then the collection of vectors said to **span** the space.

Basis Vectors

Linear combination of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,... is of the form

$$|\alpha\rangle + |\beta\rangle + |\gamma\rangle + \dots$$

- A vector $|\lambda\rangle$ is said to be **linearly independent** of the set of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,. . . ,if it cannot be written as a linear combination of them.
- A *set* of vectors is **linearly independent** if each one is independent of all the rest.
- If every vector can be written as a linear combination of members of this set then the collection of vectors said to **span** the space.
- A set of *linearly independent* vectors that spans the space is called a **basis**.

Basis Vectors

Linear combination of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,... is of the form

$$|\alpha\rangle + |\beta\rangle + |\gamma\rangle + \dots$$

- A vector $|\lambda\rangle$ is said to be **linearly independent** of the set of vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$,$\dots$,if it cannot be written as a linear combination of them.
- A *set* of vectors is **linearly independent** if each one is independent of all the rest.
- If every vector can be written as a linear combination of members of this set then the collection of vectors said to **span** the space.
- A set of *linearly independent* vectors that spans the space is called a **basis**.
- The number of vectors in any basis is called the **dimension** of space.

Inner product

An *inner product* is a function which takes two vectors as input an gives a complex number as output.
The **dual**(or **complex conjugate**) of any vector $|\alpha\rangle$ is $\langle\alpha|$

$$|\alpha\rangle^* = \langle\alpha|$$

The inner product of two vectors ($|\alpha\rangle$, $|\beta\rangle$) written as $\langle\alpha|\beta\rangle$[4] which has the properties:

$$\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^*$$

[4]This is a complex number;$\langle\alpha|\beta\rangle \in \mathbf{C}$

Inner product

An *inner product* is a function which takes two vectors as input an gives a complex number as output.
The **dual**(or **complex conjugate**) of any vector $|\alpha\rangle$ is $\langle\alpha|$

$$|\alpha\rangle^* = \langle\alpha|$$

The inner product of two vectors ($|\alpha\rangle$, $|\beta\rangle$) written as $\langle\alpha|\beta\rangle$[4] which has the properties:

$$\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^*$$

$$\langle\alpha|\alpha\rangle \geqslant 0, \ \ \textit{and}\ \langle\alpha|\alpha\rangle = 0 \Leftrightarrow |\alpha\rangle = |0\rangle$$

[4] This is a complex number;$\langle\alpha|\beta\rangle \in \mathbf{C}$

Inner product

An *inner product* is a function which takes two vectors as input an gives a complex number as output.
The **dual**(or **complex conjugate**) of any vector $|\alpha\rangle$ is $\langle\alpha|$

$$|\alpha\rangle^* = \langle\alpha|$$

The inner product of two vectors $(|\alpha\rangle, |\beta\rangle)$ written as $\langle\alpha|\beta\rangle$[4] which has the properties:

$$\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^*$$

$$\langle\alpha|\alpha\rangle \geqslant 0, \quad \textit{and}\ \langle\alpha|\alpha\rangle = 0 \Leftrightarrow |\alpha\rangle = |0\rangle$$

$$\langle\alpha|\left(b\,|\beta\rangle + c\,|\gamma\rangle\right) = b\,\langle\alpha|\beta\rangle + c\,\langle\alpha|\gamma\rangle$$

[4] This is a complex number; $\langle\alpha|\beta\rangle \in \mathbf{C}$

Inner Product Space

A vector space with an inner product is called **inner product space**.
i.e. the above conditions satisfied for any vectors $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle \in V$ and for any scalar c

e.g. $\mathbf{C}^n$ has an inner product defined by

$$\langle\alpha|\beta\rangle \equiv \sum_i a_i^* b_i = [a_1^* \dots a_n^*] \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

$$\text{where } |\alpha\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \; and \; |\beta\rangle = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

Orthonormal Set

Inner product of any vector with itself gives a **non-negative** number — its square-root of is *real* which is called **norm**

$$\parallel \alpha \parallel = \sqrt{\langle \alpha | \alpha \rangle}$$

It also termed as *length* of the vector.
A **unit vector** one whose norm is 1 is said to be **normalized**[5].

[5] Normalization: $|e_k\rangle = \frac{|k\rangle}{||k||}$

Orthonormal Set

Inner product of any vector with itself gives a **non-negative** number — its square-root of is *real* which is called **norm**

$$\parallel \alpha \parallel = \sqrt{\langle \alpha | \alpha \rangle}$$

It also termed as *length* of the vector.
A **unit vector** one whose norm is 1 is said to be **normalized**[5].

Two vectors whose inner product is **zero** is said to be **orthogonal**

$$\langle \alpha | \alpha \rangle = 0$$

[5] Normalization: $|e_k\rangle = \frac{|k\rangle}{\| k \|}$

Orthonormal Set

Inner product of any vector with itself gives a **non-negative** number — its square-root of is *real* which is called **norm**

$$\parallel \alpha \parallel = \sqrt{\langle \alpha | \alpha \rangle}$$

It also termed as *length* of the vector.
A **unit vector** one whose norm is 1 is said to be **normalized**[5].

Two vectors whose inner product is **zero** is said to be **orthogonal**

$$\langle \alpha | \alpha \rangle = 0$$

A mutually collection of **orthogonal normalized** vectors is called an **orthonormal set**

$$\langle \alpha_i | \alpha_j \rangle = \delta_{ij}, \quad where \quad \delta_{ij} \begin{cases} = 0, & \mathrm{i} = \mathrm{j} \\ \neq 0, & \mathrm{i} \neq \mathrm{j} \end{cases}$$

[5]Normalization: $|e_k\rangle = \frac{|k\rangle}{||k||}$

Orthonormal Set(Contd.)

If an **orthonormal basis** is chosen then the inner product of two vectors can be written as

$$\langle\alpha|\beta\rangle = a_1^* b_1 + a_2^* b_2 + \ldots + a_n^* b_n$$

hence the norm(squared)

$$\langle\alpha|\alpha\rangle = |a_1|^2 + |a_2|^2 + \ldots + |a_n|^2$$

each components are

$$a_j = \langle e_j|\alpha\rangle\,, \quad \text{where } e_j\text{'s are basis vector}$$

Linear Operator and Matrices

- A *linear operator* between vector spaces V and W is defined to be any function $A : V \rightarrow W$ which is linear in its inputs

$$A\left(\sum_i a_i \left|v_i\right\rangle\right) = \sum_i a_i A(\left|v_i\right\rangle)$$

Linear Operator and Matrices

- A *linear operator* between vector spaces V and W is defined to be any function $A : V \to W$ which is linear in its inputs

$$A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i A(|v_i\rangle)$$

- another linear operator on any vector space V is **Identity operator**, I_v defined as $I_v |v\rangle \equiv |v\rangle$.

Linear Operator and Matrices

- A *linear operator* between vector spaces V and W is defined to be any function $A : V \rightarrow W$ which is linear in its inputs

$$A\left(\sum_i a_i \left|v_i\right\rangle\right) = \sum_i a_i A(\left|v_i\right\rangle)$$

- another linear operator on any vector space V is **Identity operator**, I_v defined as $I_v \left|v\right\rangle \equiv \left|v\right\rangle$.
- **Zero operator** which maps all vectors to zero vector, $0\left|v\right\rangle \equiv \left|0\right\rangle$.

Linear Operator and Matrices

- A *linear operator* between vector spaces V and W is defined to be any function $A : V \to W$ which is linear in its inputs

$$A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i A(|v_i\rangle)$$

- another linear operator on any vector space V is **Identity operator**, I_v defined as $I_v |v\rangle \equiv |v\rangle$.
- **Zero operator** which maps all vectors to zero vector, $0|v\rangle \equiv |0\rangle$.
- Let V, W, X are vector spaces, and $A : V \to W$ and $B : W \to X$ are linear operators. Then the *composition* of operators B and A denoted by BA and defined by $(BA)(|v\rangle) \equiv B(A(|v\rangle))$

Matrix Representation of Linear Operators

- already we have seen that matrices can be regarded as linear operators..!!

Matrix Representation of Linear Operators

- already we have seen that matrices can be regarded as linear operators..!!
- does linear operators has a matrix representation..??!

Matrix Representation of Linear Operators

- already we have seen that matrices can be regarded as linear operators..!!
- does linear operators has a matrix representation..??!

yes it has..!!

Matrix Representation of Linear Operators

- already we have seen that matrices can be regarded as linear operators..!!
- does linear operators has a matrix representation..??!

yes it has..!!

- say, $A : V \rightarrow W$ is a linear operator between vector spaces V and W. Let the basis set for V and W are $(|\upsilon_1\rangle, \ldots, |\upsilon_m\rangle)$ and $(|\omega_1\rangle, \ldots, |\omega_n\rangle)$ respectively. Then we can say For each k in 1,2,....,m, there exist complex numbers A_{1k} through A_{nk} such that

$$A|\upsilon_k\rangle = \sum_i A_{ik}|\omega_i\rangle$$

The matrix whose entries are A_{ik} is the matrix representation of the linear operator.

Identity Matrix

The exotic way to express **1**

Definition

Identity matrix is one with the main diagonals and zeros everywhere. it is denoted by $\mathbb{I}_n$ or $\mathbb{I}$

- Matrix representation of Identity operator

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Identity Matrix

The exotic way to express **1**

Definition

Identity matrix is one with the main diagonals and zeros everywhere. it is denoted by $\mathbb{I}_n$ or $\mathbb{I}$

- Matrix representation of Identity operator

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

- It satisfies the property $\mathbb{I}_n A = A \mathbb{I}_n = A$

Identity Matrix

The exotic way to express **1**

Definition

Identity matrix is one with the main diagonals and zeros everywhere. it is denoted by $\mathbb{I}_n$ or $\mathbb{I}$

- Matrix representation of Identity operator

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

- It satisfies the property $\mathbb{I}_n A = A\mathbb{I}_n = A$
- compact notation: $(\mathbb{I}_n)_{ij} = \delta_{ij}$

Identity Matrix

The exotic way to express **1**

Definition

Identity matrix is one with the main diagonals and zeros everywhere. it is denoted by $\mathbb{I}_n$ or $\mathbb{I}$

- Matrix representation of Identity operator

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

- It satisfies the property $\mathbb{I}_n A = A\mathbb{I}_n = A$
- compact notation: $(\mathbb{I}_n)_{ij} = \delta_{ij}$
- It satisfies **Idempotent law**, $\mathbb{I}.\mathbb{I} = \mathbb{I}$

Pauli Matrices

- Pauli matrices are named after the physicist Wolfgang Pauli.

Pauli Matrices

- Pauli matrices are named after the physicist Wolfgang Pauli.
- These are a set of 2 x 2 complex matrices which are **Hermitian** and **unitary**.

Pauli Matrices

- Pauli matrices are named after the physicist Wolfgang Pauli.
- These are a set of 2 x 2 complex matrices which are **Hermitian** and **unitary**.
- They look like

$$\sigma_0 \equiv \mathbb{I} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Pauli Matrices(properties)

Some properties of Pauli matrices

- $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = -i\sigma_1\sigma_2\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}$

Pauli Matrices(properties)

Some properties of Pauli matrices

- $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = -i\sigma_1\sigma_2\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}$
- $det(\sigma_i) = -1$

Pauli Matrices(properties)

Some properties of Pauli matrices

- $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = -i\sigma_1\sigma_2\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}$
- $det(\sigma_i) = -1$
- $Tr(\sigma_i) = 0$

Pauli Matrices(properties)

Some properties of Pauli matrices

- $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = -i\sigma_1\sigma_2\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}$
- $det(\sigma_i) = -1$
- $Tr(\sigma_i) = 0$
- Each Pauli matrices has two eigenvalues $+1$ and -1.

Pauli Matrices(properties)

Some properties of Pauli matrices

- $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = -i\sigma_1\sigma_2\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}$
- $det(\sigma_i) = -1$
- $Tr(\sigma_i) = 0$
- Each Pauli matrices has two eigenvalues $+1$ and -1.
- Normalized eigenvectors are

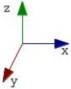
$$\psi_{x+} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \psi_{x-} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\psi_{y+} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad \psi_{y-} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$$

$$\psi_{z+} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \psi_{z-} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

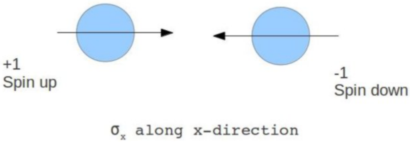
Pauli Matrices and Quantum Computation

Pauli matrices are used here as rotation[6] operators.



On the basis of Pauli matrices the X, Y, Z quantum gates[7] are designed.

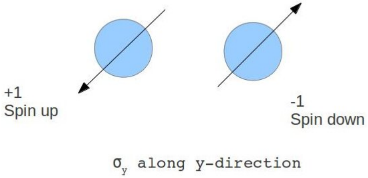
- The Pauli-X gate is the quantum equivalent of **NOT gate**. It maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$.



[6] rotation of Bloch sphere
[7] all acts on single qubit

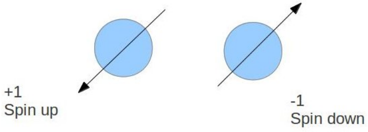
Pauli Matrices and Quantum Computation

- Pauli-Y gate maps $|0\rangle$ to $i\,|1\rangle$ and $|1\rangle$ to $-i\,|0\rangle$.



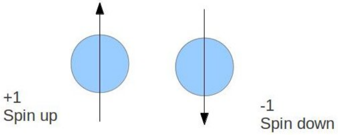
Pauli Matrices and Quantum Computation

- Pauli-Y gate maps $|0\rangle$ to $i\,|1\rangle$ and $|1\rangle$ to $-i\,|0\rangle$.



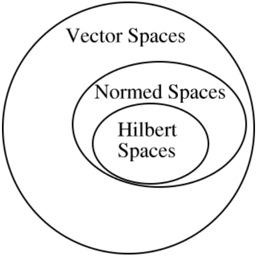
σ_y along y-direction

- Pauli-Z gate leaves the basis state $|0\rangle$ unchanged and maps $|1\rangle$ to -$|1\rangle$.



σ_z along z-direction

Hilbert Space



Wave functions live in Hilbert space

Hilbert Space: Few Basics

- The mathematical concept of **Hilbert space** named after David Hilbert, but this term coined by John von Neumann.

[8] any Cauchy sequence of functions in Hilbert space converges to a function that is also in the space.

Hilbert Space: Few Basics

- The mathematical concept of **Hilbert space** named after David Hilbert, but this term coined by John von Neumann.
- Basically this is the generalization of the notion of **Euclidean space** i.e. it extends the methods of algebra and calculus of 2D Euclidean plane and 3D space to space of any finite or infinite dimensions.

[8] any Cauchy sequence of functions in Hilbert space converges to a function that is also in the space.

Hilbert Space: Few Basics

- The mathematical concept of **Hilbert space** named after David Hilbert, but this term coined by John von Neumann.
- Basically this is the generalization of the notion of **Euclidean space** i.e. it extends the methods of algebra and calculus of 2D Euclidean plane and 3D space to space of any finite or infinite dimensions.
- Hilbert space is an abstract **vector space** with **inner product** defined in it, which allows length and angle to be measured.

[8] any Cauchy sequence of functions in Hilbert space converges to a function that is also in the space.

Hilbert Space: Few Basics

- The mathematical concept of **Hilbert space** named after David Hilbert, but this term coined by John von Neumann.
- Basically this is the generalization of the notion of **Euclidean space** i.e. it extends the methods of algebra and calculus of 2D Euclidean plane and 3D space to space of any finite or infinite dimensions.
- Hilbert space is an abstract **vector space** with **inner product** defined in it, which allows length and angle to be measured.
- Hilbert space must be **complete**.[8]

[8] any Cauchy sequence of functions in Hilbert space converges to a function that is also in the space.

Hilbert Space: Formal Approach

The set of all functions of x constitute a vector space. To represent a possible physical state,the wave function needed to be **normalized**

$$\int |\psi|^2 dx \equiv \langle\psi|\psi\rangle = 1$$

The set of all **square-integrable functions** on a specified interval,[9]

$$f(x) \text{ such that } \int_a^b |f(x)|^2 dx < \infty,$$

constitutes a smaller vector space. It is known to mathematician as $L^2(a,b)$; physicists call it **Hilbert space**.

Definition

A Euclidean space $\mathbb{R}^n$ is a vector space endowed with the inner product $\langle x|y\rangle = \langle y|x\rangle^*$ norm $\| x \| = \sqrt{\langle x|x\rangle}$ and associated metric $\| x - y \|$, such that every Cauchy sequence takes a limit in $\mathbb{R}^n$. This makes $\mathbb{R}^n$ a Hilbert space.

[9] The limits(a and b) can be $\pm\infty$

Observables

woow..! It looks good..!!

Observables

- A system **observable** is a measurable operator, where the property of the system state can be determined by some sequence of physical operations.

Observables

- A system **observable** is a measurable operator, where the property of the system state can be determined by some sequence of physical operations.
- In quantum mechanics the measurement process affects the state in a non-deterministic, but in a statistically predictable way. In particular, after a measurement is applied, the state description by a single vector may be destroyed, being replaced by a **statistical ensemble**.

Observables

- A system **observable** is a measurable operator, where the property of the system state can be determined by some sequence of physical operations.
- In quantum mechanics the measurement process affects the state in a non-deterministic, but in a statistically predictable way. In particular, after a measurement is applied, the state description by a single vector may be destroyed, being replaced by a **statistical ensemble**.
- In quantum mechanics each dynamical variable (e.g. position, translational momentum, orbital angular momentum, spin, total angular momentum, energy, etc.) is associated with a **Hermitian operator** that acts on the state of the quantum system and whose eigenvalues correspond to the possible values of the dynamical variable.

Observables

- e.g. let $|\alpha\rangle$ is an eigenvector of the observable **A**, with eigenvalue a and exits in a d-dimensional Hilbert space, then

$$\mathbf{A}\,|\alpha\rangle = a\,|\alpha\rangle$$

Observables

- e.g. let $|\alpha\rangle$ is an eigenvector of the observable **A**, with eigenvalue *a* and exits in a d-dimensional Hilbert space, then

$$\mathbf{A}\,|\alpha\rangle = a\,|\alpha\rangle$$

- This equation states that if a measurement of the observable **A** is made while the system of interest is in state $|\alpha\rangle$, then the observed value of the particular measurement must return the eigenvalue *a* with certainty. If the system is in the general state $|\phi\rangle \in \mathrm{H}$ then the eigenvalue *a* return with probability $|\langle\alpha|\phi\rangle|^2$(**Born rule**).

Observables

- e.g. let $|\alpha\rangle$ is an eigenvector of the observable **A**, with eigenvalue a and exits in a d-dimensional Hilbert space, then

$$\mathbf{A}\,|\alpha\rangle = a\,|\alpha\rangle$$

- This equation states that if a measurement of the observable **A** is made while the system of interest is in state $|\alpha\rangle$, then the observed value of the particular measurement must return the eigenvalue a with certainty. If the system is in the general state $|\phi\rangle \in \mathrm{H}$ then the eigenvalue a return with probability $|\langle\alpha|\phi\rangle|^2$(**Born rule**).
- More precisely, the observables are **Hermitian operator** so its represented by Hermitian matrix.

Hermitian Operator

Hermitian

hmmm...sounds like me!! is it a new breed ??!!

Hermitian Operator

No, its nothing new. Its the **self-adjoint operator**.

Definition

Hermitian matrix is a square matrix with complex entries that is equal to its own **conjugate transpose** i.e. the element in the i-th row and j-th column is equal to the complex conjugate of the element in the j-th row and i-th column, for all indices i and j.

mathematically $a_{ij} = a_{ji}^*$ or in matrix notation, $\mathbf{A} = (\mathbf{A}^T)^*$
In compact notation, $\mathbf{A} = \mathbf{A}^\dagger$

Hermitian Operators: Expectation Value

As previously said that the measurements are non-deterministic, so we can get a probabilistic measure of any observable, that is known as **expectation value**

$$\langle \hat{Q} \rangle = \int \psi^* \hat{Q} \psi = \left\langle \psi \middle| \hat{Q} \psi \right\rangle$$

Operators representing *observables* have the very special property that,

$$\left\langle f \middle| \hat{Q} f \right\rangle = \left\langle \hat{Q} f \middle| f \right\rangle \quad \forall f(x)$$

More strong condition for **hermiticity**,

$$\left\langle f \middle| \hat{Q} g \right\rangle = \left\langle \hat{Q} f \middle| g \right\rangle \quad \forall f(x) \text{ and } g(x)$$

Hermitian Operators:Properties

- Eigenvalues of Hermitian operators are **real**.

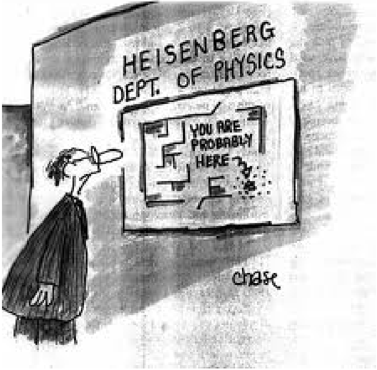
Hermitian Operators:Properties

- Eigenvalues of Hermitian operators are **real**.
- Eigenfunctions belonging to distinct eigenvalues are **orthogonal**.

Hermitian Operators:Properties

- Eigenvalues of Hermitian operators are **real**.
- Eigenfunctions belonging to distinct eigenvalues are **orthogonal**.
- The eigenfunctions of a Hermitian operator is **complete**. Any function(in Hilbert space) can be expressed as the linear combination of them.

Uncertainty Principle



Wave Particle Duality

According to de Broglie hypothesis:

$$p = \frac{h}{\lambda} = \frac{2\pi\hbar}{\lambda}$$

where p is the momentum, λ is the wavelength and h is called Plank's constant. It has a value of 6.63×10^{-34} Joule-sec. $\hbar = \frac{h}{2\pi}$ is called the reduced Plank constant.

Wave Particle Duality

According to de Broglie hypothesis:

$$p = \frac{h}{\lambda} = \frac{2\pi\hbar}{\lambda}$$

where p is the momentum, λ is the wavelength and h is called Plank's constant. It has a value of 6.63×10^{-34} Joule-sec. $\hbar = \frac{h}{2\pi}$ is called the reduced Plank constant.

This formula essentially states that every particle has a wave nature and vice versa.

Heisenberg Uncertainty Principle

The Uncertainty Principle is a direct consequence of the wave particle duality. The wavelength of a wave is well defined, while asking for its position is absurd. Vice versa is the case for a particle. And from de Broglie hypothesis, we get that momentum is inversely proportional to wavelength. Since every substance has both wave and particle nature -

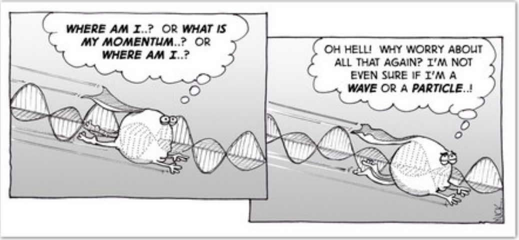
Uncertainty Principle

One can never know with perfect accuracy both the position and the momentum of a particle.

Uncertainty Principle: Mathematical Notation

According to Heisenberg, the uncertainty in the position and momentum of a substance must be at least as big as $\frac{\hbar}{2}$. So we can write the mathematical notation of the uncertainty principle:

$$\delta x.\delta p \geq \frac{\hbar}{2}$$

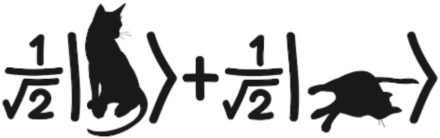


Photon self-identity issues

Introduction to Quantum Mechanics

'Not only is the Universe stranger than we think, it is stranger than we can think'

- Warner Heisenberg



Quantum Mechanics

- By the late nineteenth century the laws of physics were based on Mechanics and laws of Gravitation from Newton, Maxwell's equations describing Electricity and Magnetism and on Statistical Mechanics describing the state of large collection of matter.

Quantum Mechanics

- By the late nineteenth century the laws of physics were based on Mechanics and laws of Gravitation from Newton, Maxwell's equations describing Electricity and Magnetism and on Statistical Mechanics describing the state of large collection of matter.
- These laws of physics described nature very well under most conditions. However, some experiments of the late 19^{th} and early 20^{th} century could not be explained.

Quantum Mechanics

- By the late nineteenth century the laws of physics were based on Mechanics and laws of Gravitation from Newton, Maxwell's equations describing Electricity and Magnetism and on Statistical Mechanics describing the state of large collection of matter.
- These laws of physics described nature very well under most conditions. However, some experiments of the late 19^{th} and early 20^{th} century could not be explained.
- The problems with classical physics led to the development of Quantum Mechanics and Special Relativity.

Quantum Mechanics

- By the late nineteenth century the laws of physics were based on Mechanics and laws of Gravitation from Newton, Maxwell's equations describing Electricity and Magnetism and on Statistical Mechanics describing the state of large collection of matter.
- These laws of physics described nature very well under most conditions. However, some experiments of the late 19^{th} and early 20^{th} century could not be explained.
- The problems with classical physics led to the development of Quantum Mechanics and Special Relativity.
- Some of the problems leading to the development of Quantum Mechanics are
  - Black Body Radiation
  - Photoelectric Effect
  - Double Slit Experiment
  - Compton Scattering

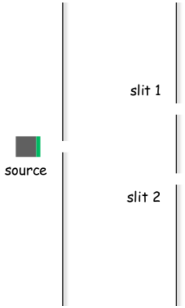
Double Slit Experiment: Setup

This experiment shows an aberrant result which cannot be explained using classical laws of physics.

Double Slit Experiment: Setup

This experiment shows an aberrant result which cannot be explained using classical laws of physics.

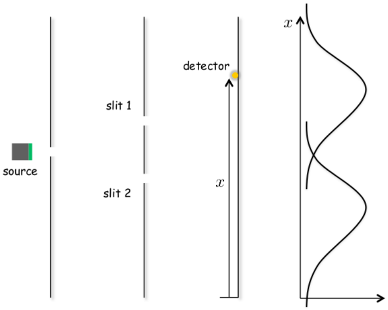
The experiment setup consists of a monochromatic source of light and two extremely small slits, big enough for only one photon particle to pass through it.



Double Slit Experiment: One Slit Open

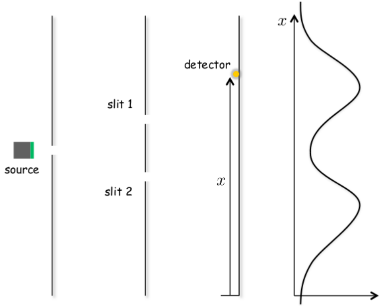
If initially only one slit is open, we get a probability distribution as shown in figure.

So if the two slits are opened individually, the two distinct probability distributations are obtained in the screen.



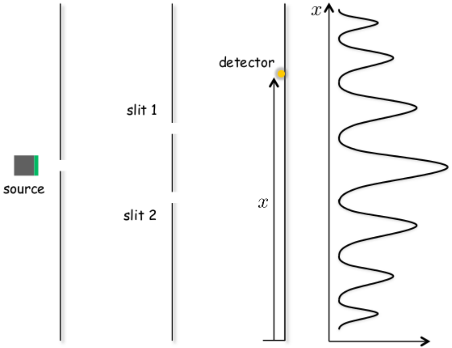
Double Slit Experiment: The Classical Expectation

Since the opening of two slits individually are independent events, classically we expect that if the two slits are opened together, the two probability distributions should add up giving the new probability distribution.



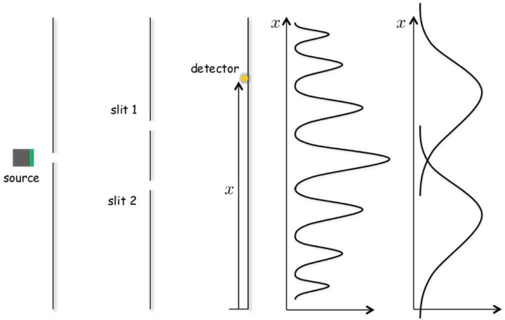
Double Slit Experiment: The Anomaly

What we observe in reality when both slits are opened together, is an interference pattern.



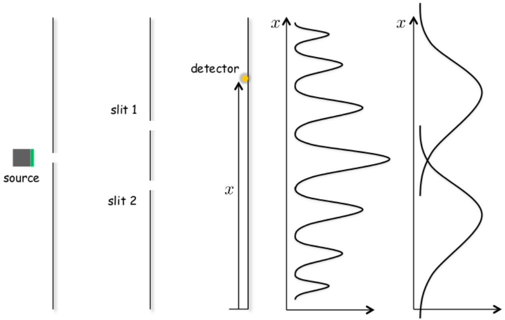
Double Slit Experiment: Quantum Explanation

- There is no classical explanation to this observation.



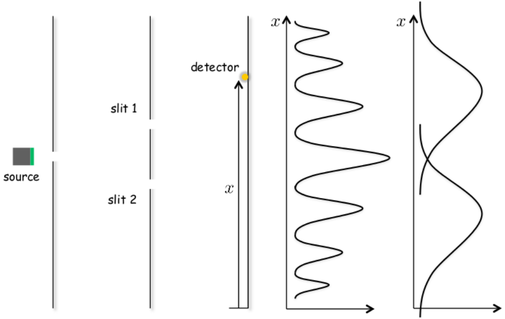
Double Slit Experiment: Quantum Explanation

- There is no classical explanation to this observation.
- However, using quantum mechanics, it can be explained.



Double Slit Experiment: Quantum Explanation

- There is no classical explanation to this observation.
- However, using quantum mechanics, it can be explained.
- It is the wave particle duality of light that is responsible for such aberrant observation. The wave nature of light is responsible for the interference pattern observed.



Double Slit Experiment: Complete Picture

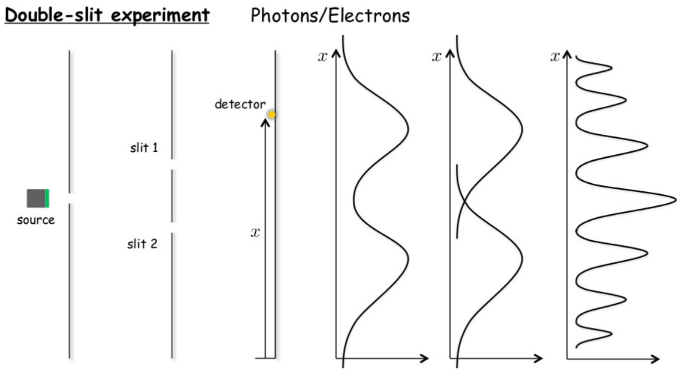


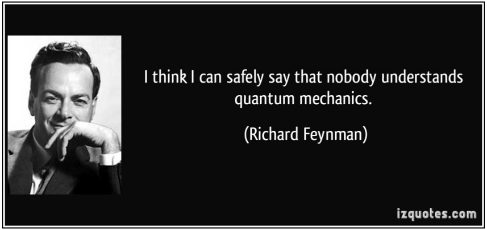
Figure : Double Slit Experiment showing the anomaly - deviation of the observed result from the one predicted by Classical Physics.

Nobody understands Quantum Mechanics

- Quantum mechanics is a very counter-intuitive theory. The results of quantum mechanics is nothing like what we experience in everyday life. It is just that nature behaves very strangely at the level of elementary particles. And this strange way is described by quantum mechanics.

Nobody understands Quantum Mechanics

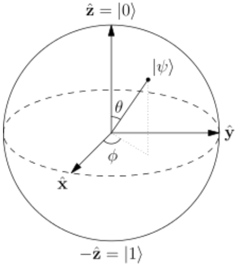
- Quantum mechanics is a very counter-intuitive theory. The results of quantum mechanics is nothing like what we experience in everyday life. It is just that nature behaves very strangely at the level of elementary particles. And this strange way is described by quantum mechanics.
- In fact, so strange is the theory that Richard Feynman once said



1st Postulate: State Space

Postulate 1

Associated to any isolated system is a Hilbert Space called the state space. The system is completely defined by the state vector, which is a unit vector in the state space.



State Vector: Mathematical Realisation

Let us consider a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Since a state is a unit vector, the norm of the vector must be unity, or in mathematical notation,

$$\langle\psi|\psi\rangle = 1$$

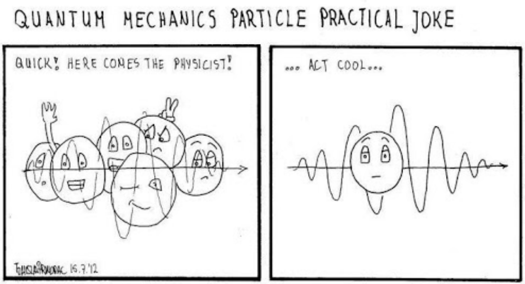
Hence, the condition that $|\psi\rangle$ is a unit vector is equivalent to

$$|\alpha|^2 + |\beta|^2 = 1$$

This condition is called the *normalization condition* of the state vector.

State: Why *unit* vector?

Let $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{k-1} |k-1\rangle$ be a quantum state. As we shall see later, the superposition is not observable. When a state is observed, it collapses into one of the basis states.



State: Why *unit* vector?

The square of the amplitude $|\alpha_i|^2$ gives the probability that the system collapses to the state $|i\rangle$.

Since the total probability is always 1, we must have:

$$\sum |\alpha_i|^2 = 1$$

This condition is satisfied *only* when the state vector is a unit vector.

2nd Postulate: Evolution

Postulate 2

The evolution of a *closed* quantum system is described by a unitary transformation.

That is, if $|\psi_1\rangle$ is the state of the system at time t_1 and $|\psi_2\rangle$ at time t_2, then:

$$|\psi_2\rangle = U(t_1, t_2)\,|\psi_1\rangle$$

where $U(t_1, t_2)$ is a unitary operator.

2nd Postulate: Evolution

Postulate 2

The evolution of a *closed* quantum system is described by a unitary transformation.

That is, if $|\psi_1\rangle$ is the state of the system at time t_1 and $|\psi_2\rangle$ at time t_2, then:

$$|\psi_2\rangle = U(t_1, t_2)\,|\psi_1\rangle$$

where $U(t_1, t_2)$ is a unitary operator.

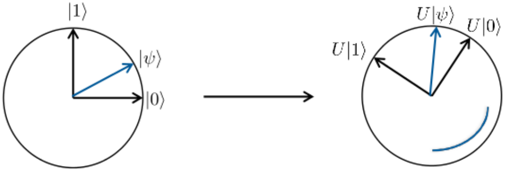


Figure : Quantum systems evolve by the rotation of the Hilbert Space

Time Evolution: Schrodinger Equation

The time evolution of a closed quantum system is given by the Schrodinger Equation:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where H is the hamiltonian and it is defined as the total energy (kinetic + potential) of the system.

Time Evolution: Schrodinger Equation

The time evolution of a closed quantum system is given by the Schrodinger Equation:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where H is the hamiltonian and it is defined as the total energy (kinetic + potential) of the system.

The connection between the hamitonian picture and the unitary operator picture is given by:

$$|\psi_2\rangle = \exp\frac{-iH(t_2-t_1)}{\hbar}|\psi_1\rangle = U(t_1,t_2)|\psi_1\rangle$$

where we define, $U(t_1,t_2) \equiv \exp\frac{-iH(t_2-t_1)}{\hbar}$

Attempt at 3rd Postulate

- Unlike classical physics, measurement in quantum mechanics is not deterministic. Even if we have the complete knowledge of a system, we can at most predict the probability of a certain outcome from a set of possible outcomes.

Attempt at 3rd Postulate

- Unlike classical physics, measurement in quantum mechanics is not deterministic. Even if we have the complete knowledge of a system, we can at most predict the probability of a certain outcome from a set of possible outcomes.

- If we have a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then the probability of getting outcome $|0\rangle$ is $|\alpha|^2$ and that of $|1\rangle$ is $|\beta|^2$.

Attempt at 3rd Postulate

- Unlike classical physics, measurement in quantum mechanics is not deterministic. Even if we have the complete knowledge of a system, we can at most predict the probability of a certain outcome from a set of possible outcomes.
- If we have a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then the probability of getting outcome $|0\rangle$ is $|\alpha|^2$ and that of $|1\rangle$ is $|\beta|^2$.
- After measurement, the state of the system collapses to either $|0\rangle$ or $|1\rangle$ with the said probability.

Attempt at 3rd Postulate

- Unlike classical physics, measurement in quantum mechanics is not deterministic. Even if we have the complete knowledge of a system, we can at most predict the probability of a certain outcome from a set of possible outcomes.

- If we have a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then the probability of getting outcome $|0\rangle$ is $|\alpha|^2$ and that of $|1\rangle$ is $|\beta|^2$.

- After measurement, the state of the system collapses to either $|0\rangle$ or $|1\rangle$ with the said probability.

- However, after measurement if the new state of the system is $|0\rangle$ (say), then further measurements in the same basis gives outcome $|0\rangle$ with probability 1.

3rd Postulate: Measurement

Postulate 3

Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ before experiment, then the probability that result m occurs is given by,

$$p(m) = \langle\psi| \, M_m \dagger . M_m \, |\psi\rangle$$

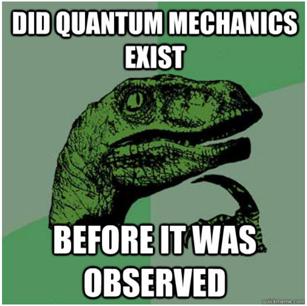
And the state of the system after measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m\dagger.M_m|\psi\rangle}}$$

So what is the *Big Deal?*

The postulate states that a quantum system stays in a superposition when it is not observed. When a measurement is done, it immediately collapses to one of its eigenstates. Hence we can never observe what the original superposition of the system was. We merely observe the state after it collapses.

This inherent ambiguity provides an excellent security in Quantum Cryptography.



Schrodinger's Cat

- This is a thought experiment proposed by Erwin Schrodinger.

Schrodinger's Cat

- This is a thought experiment proposed by Erwin Schrodinger.
- Place a cat in a steel chamber with a device containing a vial of hydrocyanic acid and a radioactive substance. If even a single atom of the substance decays, it will trip a hammer and break the vial which in turn kills the cat.

Schrodinger's Cat

- This is a thought experiment proposed by Erwin Schrodinger.
- Place a cat in a steel chamber with a device containing a vial of hydrocyanic acid and a radioactive substance. If even a single atom of the substance decays, it will trip a hammer and break the vial which in turn kills the cat.
- Without opening the box, an observer cannot know whether the cat is alive or dead. So the cat may be said to be in a superposition of the two states.

Schrodinger's Cat

- This is a thought experiment proposed by Erwin Schrodinger.
- Place a cat in a steel chamber with a device containing a vial of hydrocyanic acid and a radioactive substance. If even a single atom of the substance decays, it will trip a hammer and break the vial which in turn kills the cat.
- Without opening the box, an observer cannot know whether the cat is alive or dead. So the cat may be said to be in a superposition of the two states.
- However, when the box is opened, we observe deterministically that the cat is either dead or alive. We can, by no means, observe the superposition.

4th Postulate: Composite System

What we have seen so far was a single qubit system. What happens when there are multiple qubits? This is given by the last postulate:

Postulate 4

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have n systems, and the system number i is prepared in state $|\psi_i\rangle$, then the joint state of the total system is

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$$

Two Qubit System

Let us consider a two qubit system. Classically, with two bits, we can have 4 states - $00, 01, 10, 11$. A quantum system is a linear superposition of all these four states.

So, a general two qubit quantum state can be represented as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$ [10]

where,

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

[10] $|0\rangle \otimes |0\rangle \equiv |0\rangle|0\rangle \equiv |00\rangle$

Measurement in Two Qubit System

Measurement is similar to single qubit system. When we measure the two qubit system we get outcome j with probability $|\alpha_j|^2$ and the new state will be $|j\rangle$.

That is for the system

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

we get outcome $|00\rangle$ with probability $|\alpha_{00}|^2$ and the new state of the system will be $|00\rangle$.

Partial Measurement

So what if we want to measure only the first qubit? Or maybe only the second one?

We take the same two qubit system,

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

If only the first qubit is measured then we get the outcome $|0\rangle$ for the first qubit with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$

and the state collapses to

$$|\phi\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Coming up in next talk...

- Einstein-Polosky-Rosen (EPR) Paradox
- Bell State
- Quantum Entanglement
- Density Matrix Notation of Quantum Mechanics
- Quantum Gates

and many more...

Reference

- Michael A. Nielsen, Isaac Chuang
  Quantum Computation and Quantum Information
  Cambridge University Press
- David J. Griffiths
  Introduction to Quantum Mechanics
  Prentice Hall, 2nd Edition
- Umesh Vazirani, University of California Berkeley
  Quantum Mechanics and Quantum Computation
  https://class.coursera.org/qcomp-2012-001/
- Michael A. Nielsen, University of Queensland
  Quantum Computing for the determined
  http://michaelnielsen.org/blog/quantum-computing-for-the-determined/
- James Branson, University of California San Diego
  Quantum Physics (UCSD Physics 130)
  http://quantummechanics.ucsd.edu/ph130a/130_notes/130_notes.html

Reference

N. David Mermin, Cornell University
Lecture Notes on Quantum Computation

http://www.wikipedia.org