

# QUANTUM COMPUTING AND INFORMATION

SUMMER OF SCIENCE 2022

---

PRERAK CONTRACTOR

*Mentors: Aditya Sriram and Aryaman Mihir Seth*

[preerakcontractor@gmail.com](mailto:preerakcontractor@gmail.com)

---

# Contents

<b>I</b>	<b>Introduction To Quantum Mechanics</b>	<b>1</b>
<b>1</b>	<b>Linear Algebra</b>	<b>1</b>
1.1	Pauli Matrices	2
1.2	Inner Products	2
1.3	Eigenvectors and Eigenvalues	3
1.4	Adjoint and Hermitian Operators	4
1.5	Tensor Products	6
1.6	Operator Functions	6
1.7	Commutator and Anticommutator	7
1.8	Polar and Singular Value Decompositions	7
<b>2</b>	<b>Postulates of Quantum Mechanics</b>	<b>8</b>
2.1	Postulate 1	8
2.2	Postulate 2	8
2.2.1	Postulate 2'	8
2.3	Postulate 3	9
2.4	Postulate 4	10
2.4.1	Entangled States	10
2.5	Density Operator	10

---

# Introduction To Quantum Mechanics

## SECTION 1

### Linear Algebra

Fundamental objects in Linear Algebra are **Vectors Spaces**.

Elements of vector space are **vectors**, denoted by column matrix notation:

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$$

Standard quantum mechanics notation for vector is  $|\psi\rangle$ , sometimes called *ket*.  
Vector Spaces also contain a special *zero vector* 0.

Multiplication by scalar and Addition Operations are defined on a vector space, with the vector space being closed under these operations.

**Definition 1** Vector Subspaces:  $W$  is a vector subspace of vector space  $V$  if  $W \subset V$  and  $W$  is itself a vector space.

**Definition 2** Spanning Set of vector space  $V$ : A set of vectors  $|v_1\rangle, \dots, |v_n\rangle$  such that any vector  $|v\rangle$  in  $V$  can be written as linear combination  $|v\rangle = \sum_{i=1}^n a_i |v_i\rangle$

**Definition 3** Linear Dependence: A set of vectors  $|v_1\rangle, \dots, |v_n\rangle$  are said to be linearly dependent if there exists a set of scalars  $a_1, \dots, a_n$  (with at least one being non-zero) such that  $\sum_{i=1}^n a_i |v_i\rangle = 0$

**Definition 4** Basis of Vector Space  $V$ : A spanning set of vector space which is linearly independent.  
Note: Any basis of given vector space will have same number of elements. The number of elements in any basis is called *dimension* of vector space.

**Definition 5** Linear Operator (Denoted by  $A|v\rangle$ ): Defined as a function  $A$  from vector spaces  $V \rightarrow W$  which is linear in inputs:

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

The most common example of vector spaces is  $\mathbb{C}^n$ , the space of all n-tuples  $(z_1, z_2, \dots, z_n)$ ,  $z_i \in \mathbb{C}$

A set of vectors are linearly independent iff  $\sum_{i=1}^n a_i |v_i\rangle = 0 \implies a_1 = a_2 = \dots = a_n = 0$  i.e., if it is not a linearly dependent set.

Two important linear operators are:

- Identity Operator  $I_V$  or  $I$ :  $I|v\rangle \equiv |v\rangle$
- Zero Operator 0:  $0|v\rangle \equiv 0$

Another interpretation is that of matrix multiplication, with  $A$  being a  $m \times n$  matrix and  $|v\rangle$  being a  $n \times 1$  column matrix being mapped to  $m \times 1$  column matrix. The matrix  $[A_{ij}]$  is determined by the input and output bases of  $V$  and  $W$  as follows:

$$A|v_j\rangle = \sum_i A_{ij}|w_i\rangle$$

**Both the viewpoints for linear operators are equivalent.**

Composition Notation:

$$BA|v\rangle \equiv B(A(|v\rangle))$$

#### SUBSECTION 1.1

### Pauli Matrices

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

#### SUBSECTION 1.2

### Inner Products

A function which takes two vectors  $|v\rangle$  and  $|w\rangle$  from a space as input, and gives a complex number as output.

Notations:  $(|v\rangle, |w\rangle)$  OR  $\langle v|w\rangle$

*Remark* The notation  $\langle v|$  is used for dual vector of  $|v\rangle$ . The dual is a linear operator from inner product space  $V$  to  $\mathbb{C}$  defined by

$$\langle v|(|w\rangle) \equiv \langle v|w \equiv (|v\rangle, |w\rangle)$$

Conditions for a function from  $V \times V$  to  $\mathbb{C}$  to be inner product:

- $(|v\rangle, \sum \lambda_i |w_i\rangle) = \sum \lambda_i (|v\rangle, |w_i\rangle)$
- $(|v\rangle, |w\rangle) = (|w^*\rangle, |v^*\rangle)$
- $(|v\rangle, |v\rangle) \geq 0$  with equality only when  $|v\rangle = 0$

A vector space equipped with inner product is called *Inner Product Space*, which is equivalent to *Hilbert Space* for the case of finite dimensional vector spaces.

Two vectors are orthogonal if their inner product is zero.

The norm of vector  $\|v\| \equiv \sqrt{\langle v|v\rangle}$ . A *unit vector* has norm 1. A set of unit vectors which are pairwise orthogonal is called *orthonormal set*.

### Matrix Representation of Inner Product in Hilbert Space

Consider a Hilbert Space with a orthonormal basis  $|i\rangle$ . Let  $|w\rangle = \sum_i w_i |i\rangle$  and  $|v\rangle = \sum_j v_j |j\rangle$ . Then the inner product will be:

$$\begin{aligned}\langle v|w\rangle &= \left( \sum_j v_j |j\rangle, \sum_i w_i |i\rangle \right) \\ &= \sum_{ij} v_j^* w_i \delta_{ij} \\ &= \sum_i v_i^* w_i \\ &= \begin{bmatrix} v_1^* & \cdots & v_n^* \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}\end{aligned}$$

*Remark* An interpretation of dual vector  $\langle v|$  from above is the conjugate transpose of matrix representation of  $|v\rangle$

**Definition 6** Outer Product ( $|w\rangle\langle v|$ ): A linear operator from  $V$  to  $W$  with action:

$$|w\rangle\langle v| (|v'\rangle) \equiv |w\rangle \langle v|v'\rangle = \langle v|v'\rangle |w\rangle$$

### Completeness Relation

Consider a Hilbert Space  $V$  with orthonormal basis  $|i\rangle$ . Let  $v = \sum_i v_i |i\rangle$ .

Then,

$$\begin{aligned}\sum_i |i\rangle\langle i| (|v\rangle) &= \sum_i |i\rangle \langle i|v\rangle \\ &= \sum_i |i\rangle v_i \\ &= v\end{aligned}$$

Which implies:

$$\boxed{\sum_i |i\rangle\langle i| = I}$$

#### SUBSECTION 1.3

### Eigenvectors and Eigenvalues

**Definition 7** For a linear operator  $A$ , a non-zero vector  $|v\rangle$  which satisfies  $A|v\rangle = v|v\rangle$  is known as its eigenvector with eigenvalue  $v$ .

Eigenspace of an eigenvalue  $v$  is the set of vectors which have eigenvalue  $v$ . It is a vector subspace of vector space on which  $A$  acts.

When an eigenstate has more than one dimensions, it is called *degenerate*.

## Diagonal Representation of Operator

**Definition 8** An operator  $A$  is said to be diagonalisable if it can be *represented* as  $A = \sum \lambda_i |i\rangle\langle i|$ , where  $|i\rangle$  is an orthonormal set of eigenvectors of  $A$  with eigenvalues  $\lambda_i$

SUBSECTION 1.4

## Adjoint and Hermitian Operators

For any linear operator  $A$  on a Hilbert Space  $V$ , there exists a unique linear operator  $A^\dagger$  (called *adjoint* or *Hermitian conjugate*) such that

$$(|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle)$$

For vectors, it is defined as:  $|v\rangle^\dagger = \langle v|$

In matrix representation,

$$A^\dagger = (A^*)^T$$

(transpose of conjugate)

$A$  is *Hermitian* or *self-adjoint* if  $A = A^\dagger$

## Projectors

**Definition 9** Consider a  $k$ -dimensional vector subspace  $W$  of  $d$ -dimensional vector space  $V$ . We can construct an orthonormal basis  $|1\rangle, \dots, |d\rangle$  of  $V$  and its subset  $|1\rangle, \dots, |k\rangle$  as orthonormal basis of  $W$ . Then the projector  $P$  onto  $W$  is defined as:

$$P \equiv \sum_{i=1}^k |i\rangle\langle i|$$

The *orthogonal complement* of  $P$  is defined as  $Q \equiv I - P$ , and is a projector of span of  $|k+1\rangle, \dots, |d\rangle$ .

An operator is *normal* if  $A^\dagger A = AA^\dagger$ .

This definition is independent of choice of orthonormal basis used for  $W$ .

## Theorem 1 Spectral Theorem

Every Normal Operator  $M$  has a diagonal representation wrt some orthonormal basis. Conversely, any diagonalisable operator is normal.

**PROOF** Proof by Induction for dimension  $d$  of vector space  $V$ :

The theorem is true for  $d = 1$  ( $Mv_1 = v_1 \implies M = I$ ).

Let  $M$  have an eigenvalue  $\lambda$ . Let  $P$  be projector onto eigenspace of  $\lambda$ , and  $Q$  be the orthogonal complement. Then,

$$M = (P + Q)M(P + Q) = PMP + QMP + PMQ + QMQ$$

Using  $MP = \lambda P$ ,  $PMP = \lambda P^2 = \lambda P$  (implying it is diagonal) and  $QMP = \lambda QP = 0$ .

Let  $|v\rangle$  be a vector in subspace  $P$ . Then,  $MM^\dagger P = M^\dagger MP = \lambda M^\dagger |v\rangle$ . Hence  $M^\dagger |v\rangle$  is eigenvector with eigenvalue  $\lambda$ . Hence  $QM^\dagger P = 0$ . Taking adjoint,  $PMQ = 0$

Hence

$$M = PMP + QMQ$$

Now,  $QM = QM(P + Q) = QMQ$  and  $QM^\dagger = QM^\dagger Q$ . Hence,

$$\begin{aligned}
 QMQQM^\dagger Q &= QMQM^\dagger Q \\
 &= QMM^\dagger Q \\
 &= QM^\dagger MQ \\
 &= QM^\dagger QMQ \\
 &= QM^\dagger QMQMQ
 \end{aligned}$$

Hence  $QMQ$  is normal. By hypothesis of induction, it is diagonal. And  $PMP$  is already diagonal. Hence  $M$  is diagonal.  $\square$

A matrix  $U$  is said to be unitary if  $UU^\dagger = U^\dagger U = I$ . An operator is unitary iff each of its matrix representation is unitary.

*Remark* Unitary Operators preserve inner product between vectors, i.e.,

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|w\rangle$$

### Positive Operator

**Definition 10** An operator  $A$  is *positive operator* if  $\forall |v\rangle, |v\rangle, A|v\rangle \geq 0$ . If it is strictly greater than 0 for all non-zero  $|v\rangle$ , the operator is called *positive definite*.

**Theorem 2** **Hermiticity of Positive Operators**  
Every Positive Operator is a Hermitian Operator.

**PROOF** **Lemma 1:** Any arbitrary operator  $A$  can be represented as  $B + iC$  with  $B$  and  $C$  as Hermitian operators.

Proof:  $B = \frac{A+A^\dagger}{2}$  and  $C = \frac{A-A^\dagger}{2i}$  satisfies both the conditions.

Consider a positive operator  $A = B + iC$ . Then,

$$(|v\rangle, A|v\rangle) = (|v\rangle, B|v\rangle) + i(|v\rangle, C|v\rangle) \geq 0$$

By spectral theorem, both  $B$  and  $C$  must have a diagonal matrix representation.

$$\implies (|v\rangle, B|v\rangle) = (|v\rangle, \sum_i \lambda_i |i\rangle\langle i| |v\rangle) = \sum_i \lambda_i v_i^2 = b \in \mathbb{R}$$

Similarly,

$$i(|v\rangle, C|v\rangle) = ic, \quad c \in \mathbb{R}$$

$$\implies b + ic \geq 0$$

$$\implies c = 0$$

But since,  $c = \sum_i \lambda_i v_i^2$ , we can take  $v = |i\rangle$  to show  $\lambda_i = 0$  for all  $i$ . Hence  $C = 0$

Hence,  $A = B$ , which is a Hermitian matrix.  $\square$

SUBSECTION 1.5

# Tensor Products

Suppose  $V$  and  $W$  are Hilbert Spaces of dimensions  $m$  and  $n$ . Then  $V \otimes W$  is a vector space of dimension  $mn$ . The vectors of this vector space are linear combination of  $|v\rangle \otimes |w\rangle$  (also written as  $|v\rangle |w\rangle$ ,  $|v, w\rangle$ ,  $|vw\rangle$ )

**Properties**

- For a scalar  $z$ ,  $z |v\rangle \otimes |w\rangle = (z |v\rangle) \otimes |w\rangle = |v\rangle \otimes (z |w\rangle)$
- $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
- $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$

## Tensor products for linear operators

**Definition 11**

Let  $A$  and  $B$  be linear operators on  $V$  and  $W$  respectively.

$$A \otimes B(|v\rangle \otimes |w\rangle) \equiv (A |v\rangle) \otimes (B |w\rangle)$$

Linearity:

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

Inner Product:

$$\left( \sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle \right) = \sum_{ij} a_i^* b_j \langle v_i | v'_j \rangle \langle w_i | w'_j \rangle$$

## Kronecker Product

Let  $A$  be  $m \times n$  matrix and  $B$  be  $p \times q$  matrix.

$$A \otimes B \equiv \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}$$

Notation:  $|v\rangle^{\otimes k}$  Implies  $|v\rangle$  tensored with itself  $k$  times

SUBSECTION 1.6

# Operator Functions

Functions like exp, log, square root, etc defined for normal matrices.

Let  $A = \sum_a a |a\rangle\langle a|$  be its spectral decomposition. Then,

$$f(A) = \sum_a f(a) |a\rangle\langle a|$$

## Trace of Matrix

$$\text{tr}(A) = \sum_i A_{ii}$$

Useful identity for calculating Trace of Operator:  
 $\text{tr}(A | \psi \rangle \langle \psi |) = \langle \psi | A | \psi \rangle$



Remark

$$\text{tr}(UAU^\dagger) = \text{tr}(A)$$

Hence trace remains same on unitary transformation of matrix.

So, trace of operator is defined as trace of any of its matrix representation.

SUBSECTION 1.7

## Commutator and Anticommutator

Definition 12

Commutator:  $[A, B] \equiv AB - BA$

If  $[A, B] = 0$ , we say  $A$  and  $B$  commute.

Anticommutator:  $\{A, B\} \equiv AB + BA$

If  $\{A, B\} = 0$ , we say  $A$  and  $B$  anti-commute.

Theorem 3

**Simultaneous Diagonalization Theorem:**

Given two Hermitian Matrices  $A$  and  $B$ . Then  $[A, B] = 0$  iff  $A$  and  $B$  are diagonalisable wrt a common orthonormal basis.

PROOF

Let  $A$  and  $B$  commute. Let  $|a, j\rangle$  be an orthonormal basis for the eigenstate  $V_a$  of  $A$  with eigenvalue  $a$  and degeneracy  $j$ . Then,

$$AB|a, j\rangle = BA|a, j\rangle = aB|a, j\rangle$$

Implying  $B|a, j\rangle$  is in eigenspace of  $V_a$ .

Let  $P_a$  be projector onto  $V_a$ . Define  $B_a \equiv P_a B P_a$ . Since  $B_a$  is Hermitian, it has a spectral decomposition wrt an orthogonal set of eigenvectors  $|a, b, k\rangle$ , where  $a$  labels to eigenvector of  $A$ ,  $b$  to eigenvectors of  $B_a$ , and  $k$  degeneracy of  $B_a$ .

$B|a, b, k\rangle \in V_a \implies B|a, b, k\rangle = P_a B|a, b, k\rangle$  and  $P_a B|a, b, k\rangle = |a, b, k\rangle$ . Hence,

$$B|a, b, k\rangle = P_a B P_a|a, b, k\rangle = b|a, b, k\rangle$$

Hence,  $|a, b, k\rangle$  is an eigenvector of  $B$ . Hence, it is orthonormal set of eigenvalues for both  $A$  and  $B$ , implying  $A$  and  $B$  are both simultaneously diagonalisable.  $\square$

SUBSECTION 1.8

## Polar and Singular Value Decompositions

Theorem 4

**Polar Decomposition**

Given a linear operator  $A$  on  $V$ , there exists a unitary  $U$  and positive operators  $J \equiv \sqrt{A^\dagger A}$  and  $K \equiv \sqrt{A A^\dagger}$  such that,

$$A = UJ = KU$$

If  $A$  is invertible,  $U = AJ^{-1}$  is uniquely determined.

PROOF

$J \equiv \sqrt{A^\dagger A}$  is positive operator, and hence its spectral decomposition  $J = \sum_i \lambda_i |i\rangle\langle i|$ . Define  $|\psi_i\rangle = A|i\rangle \implies \langle \psi_i | \psi_i \rangle = \lambda_i^2$ . For non-zero  $\lambda_i$ , define  $|e_i\rangle = |\psi_i\rangle / \lambda_i$  and use Gram-Schmidt process to extend this to make an orthonormal basis of  $V$ . Then the unitary  $U = |e_i\rangle\langle i|$  satisfies  $A = UJ$  for basis  $|i\rangle$   $\square$

**Theorem 5 Singular Value Decomposition**

For a square matrix  $A$ , there exists unitary matrices  $U$  and  $V$  and diagonal matrix  $D$  with non-negative entries such that

$$A = UDV$$

The diagonal entries of  $D$  are called *Singular Values* of  $A$

**PROOF** By polar decomposition  $A = SJ$ , with  $J$  having spectral decomposition  $J = TDT^\dagger$ . Hence  $U = ST$  and  $V = T^\dagger$  completes the proof.  $\square$

## SECTION 2

## Postulates of Quantum Mechanics

## SUBSECTION 2.1

### Postulate 1

Associated to any isolated physical system is a complex vector space with inner product (Hilbert Space), known as **state space**. The state of physical system is completely defined by its **state vector**, which is a *unit vector* in the system's state space.

**Example** The simplest quantum mechanical system is the *qubit*, with a two dimensional state space.

If  $|0\rangle$  and  $|1\rangle$  form an orthonormal basis for this system, any state vector can be represented as:

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

with normalisation condition  $\langle\psi|\psi\rangle = 1 \implies |a|^2 + |b|^2 = 1$

In general,  $|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$  is called superposition of states  $|\psi_i\rangle$  with **amplitudes**  $\alpha_i$

## SUBSECTION 2.2

### Postulate 2

The evolution of **closed** systems is described by **unitary transformations**, i.e, if  $|\psi\rangle$  and  $|\psi'\rangle$  are state vectors at time  $t_1$  and  $t_2$ , then,

$$|\psi'\rangle = U|\psi\rangle$$

with  $U$  being unitary operator.

**Example** Hadamard Gate:

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  and  $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ .

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

#### 2.2.1 Postulate 2'

Time Evolution of closed systems is described by **Schrödinger equation**:

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

$H$  here is not the Hadamard Operator, but the *Hamiltonian* of the system, which is a Hermitian operator

Spectral decomposition of Hermitian  $H = \sum_E E |E\rangle\langle E|$ , where  $|E\rangle$  are energy eigenstates or stationary states with *energy*  $E$

State with lowest energy is called ground state

General Solution:

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right] |\psi(t_1)\rangle = U(t_1, t_2) |\psi(t_1)\rangle$$

Proof that any operator  $U = e^{iK}$  for Hermitian operator  $K$  is unitary.

PROOF

Since  $K$  is Hermitian,  $K = \sum_a a |a\rangle\langle a|$  with  $a \in \mathbb{R}$   
Hence,

$$\begin{aligned} U &= \sum_a e^{ia} |a\rangle\langle a| \\ U^\dagger &= \sum_a e^{-ia} |a\rangle\langle a| \\ \implies UU^\dagger &= \sum_{i,j} \delta_{ij} |i\rangle\langle j| = I \end{aligned}$$

□

SUBSECTION 2.3

### Postulate 3

Quantum measurements are described by a collection  $\{M_m\}$  of measurement operators acting on the state space of the system being observed. Given a state  $|\psi\rangle$ , the probability that result  $m$  occurs is

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

and the state right after measurement is

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

Completeness relation:

$$\sum_m M_m^\dagger M_m = I$$

**An important result from this postulate is that non-orthogonal states cannot be distinguished, i.e., we cannot distinguish between two such states by any using any measurement operator.**

#### Projective Measurements

Observable  $M$ , which is a Hermitian operator with a spectral decomposition  $M = \sum_m m P_m$  with  $P_m$  being projector onto eigenspace of  $M$  with eigenvalue  $m$ . Upon measuring state  $|\psi\rangle$ , probability of getting result  $m$  is

$$p(m) = \langle\psi| P_m |\psi\rangle$$

The state just after is

$$\frac{P_m |\psi\rangle}{\|P_m |\psi\rangle\|}$$

The average value  $E = \sum m p(m) = \langle\psi| M |\psi\rangle = \langle M \rangle$

The standard deviation for the observable  $[\Delta M]^2 = \langle (M - \langle M \rangle)^2 \rangle = \langle M^2 \rangle - \langle M \rangle^2$

### Heisenberg Uncertainty Relationship

$$\Delta C \Delta D \geq \frac{|\langle \psi | [C, D] | \psi \rangle|}{2}$$

### POVM Measurements:

Formalism for analysis of only probabilities of measurements and not of the state after measurement. Define, for a measurement operator  $M_m$ , a positive operator:

$$E_m \equiv M_m^\dagger M_m$$

Hence,  $p(m) = \langle \psi | E_m | \psi \rangle$ .

The operators  $E_m$  are called POVM *elements* and the set  $\{E_m\}$  is called POVM (Positive Operator Value Measure)

#### SUBSECTION 2.4

### Postulate 4

The state space of composite system is the tensor product of the state spaces of composite systems.

Moreover, if we have states  $1, 2, \dots, n$  with states  $|\psi_i\rangle$ , then joint state of total system is  $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$

#### 2.4.1 Entangled States

States of composite system which cannot be expressed as product of its constituent states are called entangled states.

*Example*

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq |a\rangle |b\rangle \quad \text{for all } a, b \text{ as states of individual qubits}$$

*Remark*

### Bell States/Bell Basis:

$$\begin{aligned} & \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ & \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ & \frac{|10\rangle + |01\rangle}{\sqrt{2}} \\ & \frac{|01\rangle - |10\rangle}{\sqrt{2}} \end{aligned}$$

#### SUBSECTION 2.5

### Density Operator

#### Ensembles of Quantum States

**Definition 13**

Given a quantum system which is in one of the states  $|\psi_i\rangle$  with probabilities  $p_i$ , we call  $\{p_i, |\psi_i\rangle\}$  ensemble of pure states. The density operator (or interchangeably density matrix) is defined as:

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Time evolution of density operator:  $\{p_i, |\psi_i\rangle\} \rightarrow \{p_i, U |\psi_i\rangle\}$ .

Hence,  $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \rightarrow \sum_i p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U \rho U^\dagger$

**Probability of measurement:**

$$\begin{aligned} p(m|i) &= \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle \\ &= \text{tr}(M_m^\dagger M |\psi_i\rangle\langle\psi_i|) \quad (\text{Identity in sidenotes from trace section}) \end{aligned}$$

Hence,  $p(m) = \sum p(m|i)p_i$

$$\begin{aligned} p(m) &= p_i \text{tr}(M_m^\dagger M |\psi_i\rangle\langle\psi_i|) \\ &= \text{tr}(M_m^\dagger M \rho) \end{aligned}$$

The density operator just after becomes:

$$\rho' = \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}$$

**Definition 14**

**Pure State:** The quantum system is exactly known to be in state  $|\psi\rangle$ . ( $\text{tr}(\rho^2) = 1$ )

**Mixed State:** The quantum system has many states with different probabilities. ( $\text{tr}(\rho^2) < 1$ )