QUANTUM COMPUTING AND INFORMATION

Summer of Science 2022

Prerak Contractor

Mentors: Aditya Sriram and Aryaman Mihir Seth

preerakcontractor@gmail.com

Contents

PART

I

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.

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

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 $|v\rangle = \sum_{i=0}^{n} a_i |v_i\rangle$

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 $\sum_{i=1}^{n} a_i |v_i\rangle = 0$

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

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 $V \to W$ which is linear in inputs:

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

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

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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

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

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 diagonisable 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 eigenvectors λ_i

SUBSECTION 1.4

Adjoints and Hermition 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

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

Definition 9 Consider a k-dimensional vector subspace W of d- dimensional vector space V. We can construct an orthonormal basis $|1\rangle, \ldots, |d\rangle$ of V and its subset $|1\rangle, \ldots, |k\rangle$ 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 $|k+1\rangle, \ldots, |d\rangle$.

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

Theorem 1 **Sprectral Theorem**
Every Normal Operator M has a diagonal representation wrt some orthonormal basis. Conversely, any diagonisable 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 λ. Let P be projector onto eigenspace of λ, and Q be the orthogonal complement. Then,

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

Using $MP = \lambda$, $PMP = \lambda P^2 = \lambda P$ (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 λ. 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,

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

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

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,

$$(|v\rangle, A|v\rangle) = ((|v\rangle, B|v\rangle)) + i(|v\rangle, C|v\rangle) = k \in \mathbb{R}$$

Taking adjoint on both sides, and using the fact that B and C are Hermitian,

$$\langle v| (B - iC) |v\rangle = k = \langle v| (B + iC) |v\rangle$$

$$\implies C = 0$$

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

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 $|v\rangle |w\rangle, \quad |v, w\rangle, \quad |vw\rangle$)

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:

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

Kronecker Product

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

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

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

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

Remark

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

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

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 diagonisable 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 $P_s\,|a, b, k\rangle = |a, b, k\rangle$. 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 diagonisable. □

Subsection 1.8

Polar and Singular Value Decompositions

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

Theorem 4 **Polar Decomposition**
Given a linear operator A on V, there exists an unitary U and positive operators $J \equiv \sqrt{A^\dagger A}$ and $K \equiv \sqrt{AA^\dagger}$ such that,

$$A = UJ = KU$$

Proof $J \equiv \sqrt{A^\dagger A}$ is positive operator, and hence its spectral decomposition $J = \sum_i \lambda_i\,|i\rangle$. Define $|\psi_i\rangle = A\,|i\rangle \implies \langle\psi_i|\psi_i\rangle = \lambda_i^2$. For non-zero λ_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 $|i\rangle$ □

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. □

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 supperposition of states $|\psi_i\rangle$ with **amplitudes** α_i

Subsection 2.2

Psotulate 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**:

$$i\hbar\frac{\mathrm{d}\,|\psi\rangle}{\mathrm{d}t} = H\,|\psi\rangle$$

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,

$$U = \sum_a e^{ia}\,|a\rangle\langle a|$$

$$U^\dagger = \sum_a e^{-ia}\,|a\rangle\langle a|$$

$$\implies UU^\dagger = \sum_{i,j} \delta_{ij}\,|i\rangle\langle j| = I$$

$\square$

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:

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

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 $M = \sum_m mP_m$ 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 $E = \sum mp(m) = \langle\psi|\, M\,|\psi\rangle = \langle M\rangle$
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 $1, 2, \ldots, n$ with states $|\psi_i\rangle$, then joint state of total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$

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:**

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$\frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$\frac{|10\rangle + |01\rangle}{\sqrt{2}}$$
$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

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 interchangebly density matrix) is defined as:

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

Time evolution of density operator: $\{p_i, |\psi_i\rangle\} \to \{p_i, U|\psi_i\rangle\}$.
Hence, $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \to \sum_i p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U\rho U^\dagger$

Probability of measurement:

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

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

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

The density operator just after becomes:

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

Definition 14

Pure State: The quantum system is exactly known to be in state $|\psi\rangle$. ($\mathrm{tr}(\rho^2) = 1$)
Mixed State: The quantum system has many states with different probabilities. ($\mathrm{tr}(\rho^2) < 1$)

Properties

An operator ρ is density operator associated with an ensemble of states $\{p_i, |\psi_i\rangle\}$ iff it satisfies:

- $\mathrm{tr}(\rho) = 1$
- It is positive operator.

The first part can be directly checked from definition. For converse, any positive operator has a spectral decomposition $\rho = \sum_i \lambda_i |i\rangle\langle i|$ with $\lambda_i > 0$. Trace condition gives $\sum_i \lambda_i = 1$. Hence $\{\lambda_i, |i\rangle\langle i|\}$ is an ensemble with ρ as density operator

Postulate 1

Any isolated system is completely described by its *density operator* ρ acting on the state space of the system.

Postulate 2

Time evolution of a system is described by unitary transformations:

$$\rho' = U\rho U^\dagger$$

Postulate 3

Collection $\{M_m\}$ describes measurements on a system.

$$\begin{aligned} p(m) &= \mathrm{tr}\left(M_m^\dagger M_m \rho\right) \\ |\psi\rangle' &= \frac{M_m \rho M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)} \end{aligned}$$

Postulate 4

State of a composite system is given by:

$$\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$$

Remark Many **different** ensembles can give rise to same density operator

Theorem 6 **Unitary freedom in the ensemble for density matrices**
Consider $\rho = \sum |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$ where $|\tilde{\psi}_i\rangle = \sqrt{p_i}\,|\psi_i\rangle$. Then the sets $|\tilde{\psi}_i\rangle$ and $|\tilde{\varphi}_i\rangle$ give same density operator iff

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij}|\tilde{\varphi}_j\rangle$$

Where u_{ij} is a unitary matrix, and we 'pad' the smaller set with 0 as elements ($p_i = 0$).

Proof Let $|\tilde{\psi}_i\rangle = \sum_j u_{ij}|\tilde{\varphi}_j\rangle$. Then,

$$\begin{aligned}\sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| &= \sum_{ijk} u_{ij}u_{ik}^* \,|\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \\ &= \sum_{jk}\left(\sum_i u_{ki}^\dagger u_{ij}\right)|\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \\ &= \sum_{jk}\delta_{kj}\,|\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \\ &= \sum_j |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j|\end{aligned}$$

For converse, assume $A = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_j |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j|$
Let $A = \sum \lambda_k \,|k\rangle\langle k|$ be the spectral decomposition, and let $|\tilde{k}\rangle = \sqrt{\lambda_k}\,|k\rangle$. Let $|\psi\rangle$ be any vector orthonormal to space spanned by $|\tilde{k}\rangle$. Then,

$$\langle\psi|\,A\,|\psi\rangle = 0 = \sum_i \langle\psi|\tilde{\psi}_i\rangle\,\langle\tilde{\psi}_i|\psi\rangle = \sum_i \left|\langle\tilde{\psi}_i|\psi\rangle\right|^2$$

Implying $|\tilde{\psi}_i\rangle$ is orthonormal to $|\psi\rangle$. Hence it can be written as linear combination of $|\tilde{k}\rangle \implies |\tilde{\psi}_i\rangle = \sum_k c_{ik}|\tilde{k}\rangle$

Using $A = \sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$,

$$\sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_{kl}\left(\sum_i c_{ik}c_{il}^*\right)|\tilde{k}\rangle\langle\tilde{l}|$$

Since $|\tilde{k}\rangle$ and $|\tilde{l}\rangle$ are linearly independent, $\sum_i c_{ik}c_{il}^* = \delta_{kl}$. Hence by adding extra columns if needed and appending 0 to set of $|\tilde{k}\rangle$, we can make c a unitary matrix v such that $|\tilde{\psi}_i\rangle = \sum_k v_{ik}|\tilde{k}\rangle$. Similary, we can obtain $|\tilde{\varphi}_j\rangle$ in same form (let unitary matrix in this case be u). And hence, $|\tilde{\psi}_i\rangle = \sum_j w_{ij}|\tilde{\varphi}_j\rangle$, where $w = vu^\dagger$ □

2.5.1 Reduced Density Operator

Definition 15 Consider two systems A and B, whose state is described by density operator ρ^{AB}. The reduced density operator for A is defined as

$$\rho^A \equiv \mathrm{tr}_B\left(\rho^{AB}\right)$$

Where, tr_B is a map of operators

$$\mathrm{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \,\mathrm{tr}(|b_1\rangle\langle b_2|)$$

Quantum Entanglement: It is possible that the joint state be a pure state, but the state of individual systems be a mixed state.

SUBSECTION 2.6
Schmidt Decomposition

Theorem 7 Given a pure state $|\psi\rangle$ of composite system AB, there exists orthonormal states $|i_A\rangle$ and $|i_B\rangle$ for systems A and B such that:

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

Where λ_i are non negative with $\sum_i \lambda_i^2 = 1$, called **Schmidt coefficients**.

The bases i_A and i_B are called **Schmidt Bases** and number of non-zero λ_i is called **Schmidt number**.

Schmidt number quantifies 'amount' of entanglement between systems A and B. It remains invariant under unitary transformations.

SUBSECTION 2.7
Purification

Given a state ρ^A of a quantum system A, it is possible to introduce another system R (called *reference system*) and define a pure state $|AR\rangle$ for the joint system AR such that $\rho^A = \mathrm{tr}_R(|AR\rangle\langle AR|)$. This procedure is called **purification** and allows us to associate pure states with mixed states.

Procedure to obtain reference system

Suppose $\rho^A = \sum_i p_i \left|i^A\right\rangle\left\langle i^A\right|$ (orthonormal decomposition). Now consider system R which has same state space as system A with orthonormal basis states $\left|i^R\right\rangle$. Then we define a pure state for the combined system as:

$$|AR\rangle = \sum_i \sqrt{p_i} \left|i^A\right\rangle \left|i^R\right\rangle$$

PART

II

Quantum Circuits