# Quantum Computing

Gunjan

A Thesis Submitted to

Department of Mathematics

as part of M.Sc. Project part-1

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Department of Mathematics

April 2015

# DECLARATION

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented any idea in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the source which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Signature of the supervisor)

G. Ramesh

(Name of the supervisor)

(Signature of the student)

GUNJAN

(Name of the student)

MA13M1002

(Roll no)

Date: 16/06/2015

Place: IIT Hyderabad

# APPROVAL SHEET

This thesis entitled "Quantum Computing" by GUNJAN SAPRA is approved for the degree of MASTER OF SCIENCE.

(Signature of the supervisor)

G. Ramesh

(Name of the supervisor)

Date: 16/06/2015

Place: IIT Hyderabad

# Acknowledgements

I would like to express my high regard to my guide Dr. G. Ramesh for his unhitching support constant visit while I set about the project. I am ever so thankful to you sir for your co-operation suggestions without which this project would not have seen the light of day.

Gunjan Sapra.

# Dedication

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents whose words of encouragement and push for tenacity ring in my ears. My Sister Ritu Sapra has never left my side and are very special.

# Contents

# Chapter 1

# Introductory Mathematics for Quantum computing

## 1.1 Introduction

In this chapter we will study topics of Linear algebra that will be needed for the rest of thesis. We begin by defining linear operators on vector spaces. we define physics Bra-Ket notation that will be used throughout the thesis. The next few sections deal with topics related to matrices like Trace,Unitary, Hermitian and Positive and Positive semi definite matrices. We define vector spaces with some additional structures which includes inner product space, Outer product, Hilbert space. we study how to make new spaces from the given spaces which includes direct sum of vector spaces, Tensor product. Tensor product of spaces plays an important role in various area of Quantum mechanics (we will study in next few chapters). we close this chapters with some applications of Tensor product.

## 1.2 Bra-Ket Notation

Let $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n) \in \mathbb{C}^n$. We write,
$|x\rangle = \Big(x_1 x_2 \dots x_n\Big)^T$ and $\langle x| = (|x\rangle)^* = \Big(\bar{x_1}\bar{x_2} \dots \bar{x_n}\Big)$

**Definition 1.2.1.** *A vector space V endowed with an inner product is called inner product space.*

**Example 1.2.2.** $\mathbb{C}^n$ *has an inner product defined by*

$$\Big((y_1 y_2 \dots y_n), (z_1 z_2 \dots z_n)\Big) = \sum_{i=1}^{n} y_i^* z_i. \textit{ for all } y_i, z_i \in \mathbb{C}, 1 \le i \le n.$$

### 1.2.1 Hilbert Space

**Definition 1.2.3.** *A complex inner product space is called Hilbert space if it is complete with respect to the norm* $\|x\| = \sqrt{\langle x, x\rangle}$.

*Throughout this thesis, we will be dealing with operators defined on the finite dimensional complex Hilbert space.*

## 1.3 Linear Operators

**Definition 1.3.1.** *Let $\mathbb{V}$ and $\mathbb{W}$ be vector spaces over a field $K$, either real or complex. A map $T : \mathbb{V} \to \mathbb{W}$ is linear if it satisfy following condition:*

$$T(ax + by) = aT(x) + bT(y) \text{ for all } x, y \in \mathbb{V} \text{ and } a, b \in K. \tag{1.1}$$

**Definition 1.3.2.** *Let $T : \mathbb{V} \to \mathbb{W}$ be a linear operator. Then, **Range(T)** and **Null(T)** is defined as:*

$$Range(T) = \{T(x) | x \in \mathbb{V}\}.$$

$$Null(T) = \{x \in \mathbb{V} | T(x) = 0\}.$$

**Remark 1.3.3.**

1. *We denote the space of all linear maps from $\mathbb{V}$ to $\mathbb{W}$ by $L(\mathbb{V}, \mathbb{W})$ and $L(\mathbb{V}, \mathbb{V}) = L(\mathbb{V})$.*
2. *Every $m \times n$ matrix defines a linear operator from $\mathbb{V}$ to $\mathbb{W}$ where $\mathbb{V}$ is $n$ dimensional and $\mathbb{W}$ is $m$ dimensional.*
3. *The set of all $n \times n$ matrices with entries from $K$ is denoted by $M_n(K)$.*

**Definition 1.3.4.** *Let $\mathbb{V}$ be a vector space. **Dual** of $\mathbb{V}$, denoted by $\mathbb{V}^*$, is the space defined by:*

$$V^* = \{f : \mathbb{V} \to \mathbb{C} | f \text{ is linear}\}.$$

## 1.4 Eigenvectors and eigenvalues

**Definition 1.4.1.** *Let $T$ be a linear operator on a vector space $\mathbb{V}$ then a nonzero vector $|v\rangle \in \mathbb{V}$ is said to be an **eigenvector** if there exists a complex number $\lambda$ such that*

$$T|v\rangle = \lambda|v\rangle,$$

*and complex number $\lambda$ is called eigenvalue of $T$ associated to $\lambda$.*

*The eigen space corresponding to an eigenvalue $\lambda$ is given by :*

$$ker(T - \lambda I) = \{|v\rangle \in V : T|v\rangle = \lambda|v\rangle \text{ for some } \lambda \in \mathbb{C}\}.$$

**Definition 1.4.2.** *An operator $T$ on a vector space $\mathbb{V}$ is said to be **diagonalizable** if there exists a basis $\beta$ of $\mathbb{V}$ such that $[T]_\beta$ is a diagonal matrix.*

**Remark 1.4.3.** *If $T$ is diagonalizable then $T$ can be represented as*

$$T = \sum_i \lambda_i |v_i\rangle\langle v_i|$$

*where $\{v_1, v_2, ..., v_n\}$ is an orthonormal basis of $\mathbb{V}$ with corresponding eigenvalue $\{\lambda_1, \lambda_2, ..., \lambda_n\}$. This representation is known as diagonal representation for $T$.*

**Spectral decomposition theorem:**

**Theorem 1.4.4.** *Let $T$ be a linear operator on a complex inner product space $\mathbb{V}$ then $\mathbb{V}$ has an orthonormal basis consisting of eigenvectors of $T$ if and only if $T$ is normal.*

### 1.4.1 Adjoint of a linear operator

**Definition 1.4.5.** *Let $T$ be a linear operator on an Hilbert space $H$. Then there exists a unique linear operator $T^*$ on $H$ such that*

$$(|v\rangle, T|w\rangle) = (T^*|v\rangle, |w\rangle).$$

*This linear operator is known as the adjoint of the operator $T$, for all vectors $|v\rangle, |w\rangle \in H$*

### 1.4.2 Outer Product

*There is a way to represent linear operators defined on inner product spaces which make use of inner product and it is known as outer product.*

**Definition 1.4.6.** *Let $|v\rangle \in \mathbb{V}$ and $|w\rangle \in \mathbb{W}$, where $\mathbb{V}$ and $\mathbb{W}$ be two inner product spaces over a field $K$. Define $|w\rangle\langle v| : \mathbb{V} \to \mathbb{W}$ by,*

$$(|w\rangle\langle v|)|v_1\rangle = |w\rangle\langle v|v_1\rangle = \langle v|v_1\rangle|w\rangle, \ \forall\ v \in \mathbb{V}. \tag{1.2}$$

### 1.4.3 Completeness relation

*Let $\{v_1, v_2, ...v_n\}$ be an orthonormal basis for an inner product space $\mathbb{V}$. Then $|v\rangle \in \mathbb{V}$ can be written as $v = \sum\limits_{i=1}^{n} c_i|v_i\rangle$ for some complex numbers $c_1, c_2, ...c_n \in \mathbb{C}$, Where $c_i = \langle v_i|v\rangle$, for $i = 1, 2, ..., n$.*

$$(\sum_{i=1}^{n} |v_i\rangle\langle v_i|)|v\rangle = \sum_{i=1}^{n} |v_i\rangle\langle v_i|v\rangle = \sum_{i=1}^{n} c_i|v_i\rangle = |v\rangle.$$

*since the last equality is true for all $|v\rangle \in \mathbb{V}$, it follows that*

$$\sum_{i=1}^{n} |v_i\rangle\langle v_i| = I. \tag{1.3}$$

*This equation is known as **completeness relation.***

**Remark 1.4.7.** *Every operator can be written in its outer product representation. Suppose $A : \mathbb{V} \to \mathbb{W}$ where $\mathbb{V}$ and $\mathbb{W}$ are two inner product spaces. Let $|v_i\rangle$ and $|w_j\rangle$ be orthonormal basis of $\mathbb{V}$ and $\mathbb{W}$ respectively. Then $A$ can be written as $A = I_{\mathbb{W}} A I_{\mathbb{V}}$.*

## 1.5 Unitary and Hermitian matrices

**Definition 1.5.1.** *$U \in M_n(\mathbb{C})$ is Unitary if $U^*U = I$*

**Proposition 1.5.2.** *For $U \in M_n(\mathbb{C})$, Following statements are equivalent:*

*(i) $U$ is unitary.*

*(ii) $U$ is invertible and $U^{-1} = U^*$.*

*(iii) $UU^* = I$.*

*(iv) $U^*$ is unitary.*

*(v) The columns of $U$ are orthogonal.*

*(vi) The rows of $U$ are orthogonal.*

*(vii) (Isometry) $\|Ux\| = \|x\|$ for all $x \in \mathbb{C}^n$.*

*(viii) (Inner product preserving) $\langle Ux|Uy\rangle = \langle x|y\rangle$ for all $x, y \in \mathbb{C}^n$.*

**Theorem 1.5.3.** *Let $A \in M_n(\mathbb{C})$. Then there exists a unitary matrix $U$ such that $U^*AU$ is upper triangular.*

**Definition 1.5.4.** *$H \in M_n(\mathbb{C})$ is called **Hermition** matrix if $H = H^*$.*

**Proposition 1.5.5.** *For $H \in M_n(\mathbb{C})$,the following statements are equivalent:*

*(i) $H$ is hermition.*

*(ii) There exists a unitary matrix $U$ such that $U^*AU = D$ where $D$ is diagonal matrix with real entries.*

*(iii) $H$ has orthonormal basis with real eigenvectors that is $H$ is diagonalizable.*

*(iv) $\langle x, Hx\rangle$ is real, for all $x \in \mathbb{C}^n$.*

## 1.6 Positive definite and Semi definite matrices

**Definition 1.6.1.** *Let $P \in M_n$.Then $P$ is called positive semi definite, denoted by, $P \geq 0$ if $\langle x|Px\rangle \geq 0\,\forall x \in \mathbb{C}^n$. It is called positive definite,denoted $P > 0$,if $\langle x|Px\rangle > 0\,\forall x \in \mathbb{C}^n$.*

**Remark 1.6.2.** *Every positive semi definite (positive definite) matrix is symmetric. It follows From Proposition 1.5.5(iv)*

**Proposition 1.6.3.** *For $P \in M_n$,the following statements are equivalent:*

1. *$P \geq 0\,(P > 0)$.*
2. *$P = P^*$ and all eigenvalues of $P$ are non negative (positive).*
3. *$P = B^*B$ for some matrix $B$ (in case of positive definite $B$ is invertible).*

**Theorem 1.6.4.** *$P \geq 0$ if and only if $P = \sum\limits_{i=1}^{m} |v_i\rangle\langle v_i|$ for some set of vectors $\{v_1, v_2, ..., v_n\}$.*

**Theorem 1.6.5.** *Let $P \in M_n$ and $P = \sum\limits_{i=1}^{m} |v_i\rangle\langle v_i|$,then $p > 0$ if and only if span$\{v_1 \ldots v_m\} = \mathbb{C}^n$.*

**Theorem 1.6.6.** *Let $P \in M_n$ be a Hermitian matrix.Then $P \geq 0$ if and only if determinant of its all principal minors are positive.*

## 1.7 Trace

**Definition 1.7.1.** *Let $A \in M_n(K)$ then trace of A, denoted by, Tr(A) is the sum of all diagonal entries of A*

$$Tr(A) = \sum_{i=1}^{n} a_{ii}.$$

**Proposition 1.7.2.** *Let $A, B \in M_n$. Following statements hold true:*

*(i) Tr(AB)=Tr(BA).*

*(ii) Tr(A+B)=Tr(B+A).*

*(iii) Tr(zA)=zTr(A) for any $z \in \mathbb{C}$.*

*(iv) Trace of a matrix is invariant under unitary similarity transformation.*

$$Tr(UAU^*) = Tr(A).$$

### 1.7.1 Trace of an operator

**Definition 1.7.3.** *Let $V$ be an $n$ dimensional vector space and $T \in L(V)$ ,then Trace of $T$, denoted by, $Tr(T)$, is the trace of $[T]_\beta$ where $\beta$ is any basis of $\mathbb{V}$.*

**Remark 1.7.4.** *If $\beta_1$ and $\beta_2$ are two basis of $\mathbb{V}$. Then there exists $P \in M_n$ such that $[T]_{\beta_1} = P[T]_{\beta_2}P^{-1}$.*

**Note 1.7.5.** *$Tr(T)$ does not depend upon the basis. If $\beta_1$ and $\beta_2$ are two basis of $H$ then $Tr[T]_{\beta_1} = Tr[T]_{\beta_2}$ as it is very clear from the above remark.*

**Remark 1.7.6.** *Let $T \in L(V)$ and $\psi \in \mathbb{V}$.Suppose that $\psi$ is a unit vector in $\mathbb{V}$. Then*

$$Tr(T|\psi\rangle\langle\psi|) = \langle\psi|T|\psi\rangle. \tag{1.4}$$

### 1.7.2 Properties of Trace

*(i) **Cyclic property of trace:** Let $A$ and $B$ be two linear operators defined on n dimensional vector spaces. Then,*

$$Tr(AB) = Tr(BA).$$

*(ii) **Linearity of Trace:** Let $A$ and $B$ be two linear operators. Then,*

$$Tr(A + B) = Tr(B + A).$$

$$Tr(zA) = zTr(A) \textit{ for all } z \in \mathbb{C}.$$

## 1.8 Direct sum of vector spaces

**Definition 1.8.1.** *Given vector spaces $V$ and $W$ their direct sum is defined as*

$$V \oplus W = \{(v, w)|v \in V, w \in W\},$$

*such that every element of this space has unique representation. It is a vector space with operations:*

$$(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2), v_1, v_2 \in V \text{ and } w_1, w_2 \in W.$$

$$a(v, w) = (av, aw); a \in K, v \in V, w \in W$$

**Note 1.8.2.** *It is a Hilbert space with respect to the inner product*

$$\langle (v_1, w_1)|(v_2, w_2)\rangle = \langle (v_1, v_2)\rangle_V + \langle (w_1, w_2)\rangle_W \, \forall \, v_1, v_2 \in V; w_1, w_2 \in W.$$

*Where $(.,.)_V$ and $(.,.)_W$ denote inner products on $V$ and $W$, respectively.*

**Proposition 1.8.3.** *If $\{v_1, v_2, ..., v_n\}$ is a basis for $V$ and $\{w_1, w_2, ..., w_k\}$ is a basis for $W$, then $\{(v_1, 0), (v_2, 0), ..., (v_n, 0), (0, w_1), (0, w_2), ..., (0, w_k)\}$ is a basis for $(V \oplus W)$ and hence, dim $(V \oplus W)$=dim(V)+dim(W).*

**Theorem 1.8.4.** *Let $U$ be a subspace of a vector space $V$. Then there always exist a subspace $W$ of $V$ such that $V = U \oplus W$.*

### 1.8.1 Orthogonal Projection

**Definition 1.8.5.** *Let $M$ be a subset of an inner product space $V$. Then the **orthogonal complement** of $M$ denoted as, $M^{\perp}$, is the set of all vectors in $V$ which are orthogonal to every vector in $M$.*

$$M^{\perp} = \{v \in V | \langle u, v\rangle = 0 \forall u \in U\}.$$

**Theorem 1.8.6.** *Let $M$ be a subspace of an inner product space $V$. Then $V = U \oplus U^{\perp}$.*

**Definition 1.8.7.** *Let $U$ be a subspace of an inner product space $V$ and $T : V \to U$.*

$$T(v) = T(u + w) = u$$

*where $u \in U, w \in U^{\perp}$. Then $T$ is called **orthogonal projection** of V onto U.*

**Proposition 1.8.8.** *Let $T : V \to U$ be orthogonal projection of $V$ onto U. Then, following properties hold true.*

*(i)* Range(T)=U

*(ii)* Null(T)=$U^{\perp}$

*(iii)* $T^2 = T$

*(iv)* $T = T^*$

## 1.9 Bilinear mappings

**Definition 1.9.1.** *Let $X, Y$ and $Z$ be vector spaces over a field $K$.Then mapping $B : X \times Y \to Z$ is called Bilinear if the following conditions are satisfied.*

*(i)* $B(x_1 + x_2, y) = B(x_1, y) + B(x_2, y)$ *for all* $x_1, x_2 \in X$ *and* $y \in Y$

*(ii)* $B(cx, y) = cB(x, y),\ B(x, cy) = cB(x, y)$ *for all* $x \in X$ *and* $y \in Y, c \in K$

**Note 1.9.2.** *When $Z = K$,bilinear mapping is called a bilinear form.*
*We denote the set of all bilinear forms as $B(X \times Y, Z)$. This is a linear subspace of space of all maps from $X \times Y$ to $Z$ and dimension of this subspace is dim$(X)$.dim$(Y)$.dim$(Z)$.*

**Example 1.9.3.** *Let $V$ be an inner product space over a field $K$. Then an inner product is a bilinear map from $V \times V$ to $K$.*

**Example 1.9.4.** *Let $V$ and $W$ be two inner product spaces over a field $K$. Let $\phi \in V^*$ and $\psi \in W^*$. Then the mapping $B : V \times W \to K$ defined as $B(v, w) = \phi(v).\psi(w)$ is a bilinear from.*

**Remark 1.9.5.** *Let $V$ be a vector space over a field $K$. Then bilinear map from $V \times V$ to $K$ is same as bilinear form $V \times V$ to $K$.*

## 1.10 Tensor Product

***Motivation:*** *Tensor product gives a way of putting vector spaces together to form a large vector space. This construction is crucial to understand the Quantum mechanics of two or more physical system which we will define in next chapter.*

**Definition 1.10.1.** *Given two vector spaces $X$ and $Y$, then tensor product of $X$ and $Y$ is given by:*
*$X \otimes Y :=$ span $\{x \otimes y | x \in X, y \in Y\}$, where $x \otimes y$ is called elementary tensor which is a linear mapping acting on the space of all bilinear maps.*

$$x \otimes y : B(X \times Y) \to K \text{ given by}$$

$$x \otimes y(A) = \langle A, x \otimes y \rangle = A(x, y).$$

*Elements of tensor product are called tensors.*

**Remark 1.10.2.** *For every $x_1, x_2 \in X, y_1, y_2 \in Y$ and $\lambda \in K$. Following statements are true.*

*(i)* $(x_1 + x_2) \otimes y = x_1 \otimes y + x_2 \otimes y.$

*(ii)* $x \otimes (y_1 + y_2) = x \otimes y_1 + x \otimes y_2.$

*(iii)* $\lambda(x \otimes y) = (\lambda x) \otimes y = x \otimes (\lambda y).$

**Definition 1.10.3.** *Given a nonzero tensor $u \in X \otimes Y$, then there exists $n \in \mathbb{N}$ such that $u = \sum\limits_{i=1}^{n} x_i \otimes y_i$. The smallest nonzero $n$ such that the set $\{x_1, x_2, ..., x_n\}$ and $\{y_1, y_2, ..., y_n\}$ are linearly independent is known as **Schmidt rank or rank** of $u$. Tensors of rank $1$ are called elementary tensors.*

**Proposition 1.10.4.** *Let $X$ and $Y$ be vector spaces.*

*(i) Let $E$ and $F$ be linearly independent subsets of $X$ and $Y$ respectively. Then $\{x \otimes y | x \in E, y \in F\}$ is a linearly independent subset of $X \otimes Y$.*

*(ii) If $\{e_i|i \in I\}$ and $\{f_j|j \in J\}$ are bases for $X, Y$ respectively then $\{e_i \otimes f_j|(i,j) \in I \times J\}$ is a basis of $X \otimes Y$.Hence, If $X$ and $Y$ are finite dimensional then dim$(X \otimes Y) =$ dim $X$.dim $Y$.*

**Proposition 1.10.5.** *If $\{e_1, e_2, ..., e_n\}$ and $\{f_1, f_2, ..., f_m\}$ are bases for $X, Y$ respectively and $u \in X \otimes Y$.Then,*

*(i) There exists unique $x_1, ...x_m \in X$ such that $u = x_1 \otimes f_1 + x_2 \otimes f_2 + ... + x_m \otimes f_m$.*

*(ii) There exists unique $y_1, ..., y_n \in Y$ such that $u = e_1 \otimes y_1 + e_2 \otimes y_2 + ... + e_n \otimes y_n$.*

**Remark 1.10.6.** *It follows from proposition (1.10.5) that if dim$(X) = n$ and dim$(Y) = m$ then*

*(i) $X \otimes Y \cong X \oplus ... \oplus X$ ($m$ copies).*

*(ii) $X \otimes Y \cong Y \oplus ... \oplus Y$ ($n$ copies).*

*Moreover,the above isomorphism preserves linear structure of spaces.*

**Example 1.10.7.** *Consider the vector space $\mathbb{C}^2$ over $\mathbb{C}$. we will calculate $\mathbb{C}^2 \otimes \mathbb{C}^2$. here, dim $\mathbb{C}^2 = 2$ and standard ordered basis is $\{(1,0),(0,1)\}$. we will use the Bra-Ket notation to define the basis of this vector space. write $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$. Then dim $(\mathbb{C}^2 \otimes \mathbb{C}^2) = 4$ and*

$$\begin{aligned}\mathbb{C}^2 \otimes \mathbb{C}^2 &= span\{|0 \otimes 0\rangle, |0 \otimes 1\rangle, |1 \otimes 0\rangle, |1 \otimes 1\rangle\} \\ &= span\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.\end{aligned}$$

## 1.11 Tensor product and Linearization

*The primary purpose of tensor product is to linearize a bilinear mapping. Let $X, Y$ and $Z$ be vector spaces over a field $K$. We will show that the space of all bilinear mapping on $X \times Y$ is in one to one correspondence with the space of all linear mappings on $X \otimes Y$.*
*Let $A \in B(X \times Y, Z)$. We define a linear mapping*

$$\tilde{A} : X \otimes Y \to Z$$

*by*

$$\tilde{A}(\sum_{i=1}^{n} x_i \otimes y_i) = \sum_{i=1}^{n} A(x_i, y_i).$$

*To show that above mapping is well defined. It is enough to prove that if*
$\sum_i (x_i \otimes y_i) = 0$, *then* $\tilde{A}(\sum_i x_i \otimes y_i) = 0$.
*Suppose that $\sum_i x_i \otimes y_i = 0$ then for each $\phi \in Z^*$, the composition $\phi \circ A$ is a bilinear functional on $X \times Y$. So,*

$$\phi(\sum_i A(x_i, y_i)) = \sum_i \phi \circ A(x_i, y_i) = \langle \sum_i x_i \otimes y_i, \phi \circ A\rangle = 0$$

*and hence, $\sum_i A(x_i, y_i) = 0$. Therefore,$\tilde{A}$ is well defined.*
*Thus, Bilinear mapping $A$ is associated with linear mapping $\tilde{A}$. This situation is described in following diagram:*

$$\begin{tikzcd}
X \times Y \arrow[r, "T"] \arrow[d, "A"'] & X \bigotimes Y \\
Z \arrow[ur, "\tilde{A}"'] &
\end{tikzcd}$$

**The Universal property**

**Proposition 1.11.1.** *For every bilinear mapping $A : X \times Y \to Z$ there exists a unique linear mapping $\tilde{A} : X \otimes Y \to Z$ such that $A(x, y) = \tilde{A}(x \otimes y)\, \forall x \in X, y \in Y$.*

**Uniqueness of Tensor product**

**Proposition 1.11.2.** *Let $X$ and $Y$ be two vector spaces. Suppose there exists a vector space $W$ and a bilinear mapping $B : X \times Y \to Z$ with the property that, for every vector space $Z$ and for every bilinear mapping $A : X \times Y \to Z$ there is a unique linear mapping $L : W \to Z$ such that $A = L \circ B$.Then,there is an isomorphism $J : X \otimes Y \to W$ such that $J(x \otimes y) = B(x, y) \forall\ x \in X, y \in Y$.*

## 1.12 Tensor product of Linear mappings

**Definition 1.12.1.** *Let $S : X \to E$ and $T : Y \to F$ be two linear mappings. Then define a map $B : X \times Y \to E \otimes F$ by*

$$B(x, y) = (Sx) \otimes (Ty).$$

*Then, $B$ is clearly a bilnear map. So, by proposition (1.11.2) , linearization gives a mapping*

$$S \otimes T : X \otimes T \to E \otimes F$$

*given by*

$$S \otimes T(x \otimes y) = (Sx) \otimes (Ty) \text{ for all } x \in X, y \in Y.$$

**Remark 1.12.2.** *If $S$ and $T$ are both injective (respectively, surjective) then $S \otimes T$ is also injective (respectively, surjective).*

### 1.12.1 Tensor product of matrices

*Let*

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

*and*

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

*Then the tensor product $A \otimes B$ is:*

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

## 1.13 Tensor Product of Hilbert Spaces

**Definition 1.13.1.** *Let $H_1$ and $H_2$ be two Hilbert spaces with the inner product $\langle .,. \rangle_{H_1}$ and $\langle .,. \rangle_{H_2}$ respectively.Then tensor product of $H_1$ and $H_2$ is given by:*

$$H_1 \otimes H_2 = \ span\{h_1 \otimes h_2 | h_1 \in H_1, h_2 \in H_2\},$$

*where $h_1 \otimes h_2$ are elementary tensors act on the space of all bilinear mappings on $H_1 \times H_2$.*

*Let $h_1 \otimes h_2$ be an elementary tensor. Then $h_1 \otimes h_2 : B(H_1 \times H_2, \mathbb{C}) \to \mathbb{C}$ defined as:*

$$h_1 \otimes h_2(T) = T(h_1, h_2).$$

**Remark 1.13.2.** *Tensor product of finite dimensional Hilbert spaces is a Hilbert space. For this, define a function*

$$\langle .,. \rangle : (H_1 \otimes H_2) \times (H_1 \otimes H_2) \to \mathbb{C}$$

*by*

$$\langle h_1 \otimes k_1 | h_2 \otimes k_2 \rangle = \langle h_1 | h_2 \rangle_{H_1} . \langle k_1 | k_2 \rangle_{H_2}.$$

*Then $\langle .,. \rangle$ defines an inner product on $H_1 \otimes H_2$. We call this inner product the* ***Hilbert space tensor product****.*

**Note 1.13.3.** *If $H_1$ and $H_2$ are infinite dimensional, then $H_1 \otimes H_2$ is not complete with respect to the norm coming from inner product.*

**Theorem 1.13.4.** *Let $H_1$ and $H_2$ be two Hilbert spaces with orthonormal basis $\{\phi_i\}_{i \in I}$ and $\{\eta_j\}_{j \in J}$ respectively. Then $\{\phi_i \otimes \eta_j : i \in I, j \in J\}$ is an orthonormal basis for $H_1 \otimes H_2$.*

**Proposition 1.13.5.** *Let $K$ be a field. Suppose $A \in M_m(K)$ and $B \in M_n(K)$ have eigenvalues $\lambda$ and $\mu$ in $K$. Then, $A \otimes I_n + I_m \otimes B$ has eigenvalue $\lambda + \mu$.*

*Proof.* Let $v$ be an eigenvector of $A$ corresponding to eigenvalue $\lambda$ and let $w$ be an eigenvector of $B$ corresponding to eigenvalue $\mu$. Consider,

$$\begin{aligned}
(A \otimes I_n + I_m \otimes B)(v \otimes w) &= (A \otimes I_n)(v \otimes w) + (I_m \otimes B)(v \otimes w) \\
&= Av \otimes I_n w + I_m v \otimes Bw \\
&= \lambda v \otimes w + v \otimes \mu w \\
&= \lambda(v \otimes w) + \mu(v \otimes w) \\
&= (\lambda + \mu)(v \otimes w)
\end{aligned}$$

Hence, $(\lambda + \mu)$ is an eigenvalue of $(A \otimes I_n + I_m \otimes B)$.

## 1.14 Applications of Tensor Product

(i) Tensor product of two spaces is useful in studying the Quantum mechanics properties of more than two physical system.

(ii) Tensor product is used to linearize the bilinear mappings.

# Chapter 2

# Introductory Quantum Mechanics

## 2.1 Introduction

This chapter gives a very brief introduction to Quantum mechanics. we begin with basic definitions that will be useful in rest of the thesis. we study four postulates of Quantum mechanics. Then we move to problem of distinguishable quantum system that gives a condition to determine the state of the quantum system. We then turn to composite quantum system which makes use of tensor product to define the state of such system. Here, we have a beautiful property of composite system called Entanglement (where the joint state can not be written as a product of states of its component system) which we will study in next chapter. We define Quantum gates and Quantum cloning. we close this chapter with some applications of Quantum mechanics.

### Definitions

(i) **Physical system:** A physical system is a portion of universe chosen for analysis. Everything outside the system is known as environment.

(ii) **Quantum system:** A theoretical or actual system based on Quantum physics.

(iii) **State:** A unit vector in complex Hilbert space is called state of system.

(iv) **Observable:** The operators are called observables.In Quantum mechanics, observables are unitary matrices.

(v) **Closed system:** A system that does not interact with outside world.

(vi) **Composite System:** A Physical system is said to be composite, if it is made up of two or more quantum systems.

(vii) **Qubit:** In classic computer,a bit can be either $0$ or $1$. A Quantum bit or qubit is smallest unit for information in Quantum mechanics. A qubit is a vector in two dimensional complex vector space. The main difference between a qubit and a classic bit is that a qubit can stay in the superposition of basis states. Suppose $|0\rangle$ and $|1\rangle$ forms an orthonormal basis of state space. Then an arbitrary state vector in the state space can be written as

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

for some complex numbers $a$ and $b$ are called amplitudes.

The condition that $\psi$ should be a unit vector is equivalent to $\langle\psi|\psi\rangle = 1$ which is same as $a^2 + b^2 = 1$.

## 2.2 Postulates of Quantum Mechanics

- The first postulate of Quantum mechanics describes the space in which Quantum mechanics takes place.

**Postulate 1.** Associated to any physical system there corresponds a complex Hilbert space known as state space of the system. The system is completely described by its space which is a unit vector in the system state space.

- How does the state of a closed Quantum mechanical system changes with time? The following postulate gives a description.

**Postulate 2.**The time evolution from $t_1$ to $t_2$ where $t_1 < t_2$ of a closed quantum system is described by a unitary operator $U : H \to H$. on state space. If system is in state $\psi$ at time $t_1$. Then system would be in state $U(\psi)$ at time $t_2$.

- The evolution of the system which does not interact with rest of the world is given by measurement operators.

**Postulate 3.**The evolution of an open Quantum system is described by collection of operators called measurement operator. It is denoted by $M_m$ where $m$ denotes the outcomes that may occur in the system. If the state of the quantum system is $|\psi\rangle$ immediately before the experiment, then the probability that outcome will be $m$ is given by

$$p_m(\psi) = \langle\psi|MM^*|\psi\rangle = \langle\psi|MM^*\psi\rangle = ||M_m\psi||^2. \tag{2.1}$$

And the state of the system after the measurement is given by $M_m\psi/||M_m\psi||$. The measurement operators satisfy the completeness equation

$$\sum_m M_m^* M_m = I.$$

- The following postulate describes that how the state space of a composite system is build up from the state space of component systems.

**Postulate 4.** The state of a composite physical system is the tensor product of the state spaces of component physical systems.

**Example 2.2.1.** *We give an example of measurement of qubit on computational basis. This is a measurement on a single qubit with two outcomes defined by two measurements operators $M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|$. Each measurement is Hermitian and*

$$M_0^2 = M_0$$
$$M_1^2 = M_1.$$

*And*

$$I = M_0^* M_0 + M_1^* M_1 = M_0 + M_1. \tag{2.2}$$

*Hence, I satisfies the complete relation.*
*Suppose that the state being measured is $\psi = a|0\rangle + b|1\rangle$.*
*Then the probability of obtaining measurement $0$ is given by:*

$$p(0) = \langle\psi|M_0^* M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2. \tag{2.3}$$

*Similarly,the probability of obtaining measurement $1$ is $p(1) = |b|^2$.*
*The state after the measurement in two cases are:*

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle, \; \frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle. \tag{2.4}$$

### 2.2.1 Problem of distinguish Quantum state OR Quantum Game

*In the classical world ,distinct states of an object is distinguishable. But in Quantum mechanics, this situation is a bit complicated. Given distinct states of a quantum system, we can not always distinguish the states. This situation is described by the following example.*

**Example 2.2.2.** *Let $H$ be state space of quantum system. Suppose Alice has two states $\{\psi, \phi\}$ and Bob knows that quantum system takes these two states. Alice picks one and sends to Bob. Then,can Bob create a measurement system $M_m$ to describe which one he is given.*
*We want $M_1$ and $M_2$ such that*
$\|M_1\psi_2\| = 0, \|M_1\psi_1\|^2 = p_1(\psi_1) = 1, \; \|M_2\psi_1\| = 0, \|M_2\psi_2\|^2 = p_2(\psi_2) = 1.$
***case 1.*** $(\psi_1) \perp (\psi_2)$*:Let $H_1 =$ span$(|\psi_1\rangle)$.*
*Then $H$ can be written as $H = H_1 \oplus$ span$(|\psi_1\rangle).^{\perp}$*
*Let $M_1 = |\psi_1\rangle\langle\psi_1|$. Then $M_1$ is the orthogonal projection onto the span of $\psi_1$.*
*let $M_2 = |\psi_2\rangle\langle\psi_2|$. Then $M_2$ is the orthogonal projection onto the span of $\psi_2$. Note that*

$$M_1^2 = M_1^* M_1 = M_1 \, and M_2^2 = M_2^* M_2 = M_2. \tag{2.5}$$

*Let $M_3 = I - M_1 - M_2$. which is the projection onto the span of $\{\psi_1, \psi_2\}.^{\perp}$ note that*

$$M_3^2 = M_3^* M_3 = M_3. \tag{2.6}$$

*Hence,*

$$\begin{aligned}
\|M_1\psi_1\|^2 &= \langle M_1\psi_1|M_1\psi_1\rangle \\
&= \langle \psi_1|\psi_1\rangle \\
&= 1. \\
\|M_1\psi_2\| &= \langle M_1\psi_2|M_1\psi_2\rangle = 0. \\
\|M_2\psi_1\| &= 0.\ \textit{and} \\
\|M_2\psi_2\| &= 1.
\end{aligned}$$

*Therefore, we can distinguish with certainty.*
***case 2.*** *If states $\psi_1$ and $\psi_2$ are not orthogonal to each other then there is no Quantum measurements capable of distinguish the states.*
*Consider the Quantum states $|\psi_1\rangle = |0\rangle,\ |\psi_2\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta$ both are not equal to zero.*
*If a measurement is performed then $\psi_1$ is projected to $|0\rangle$ with probability $1$ and $\psi_2$ is also projected to $|0\rangle$ with the probability $\alpha \neq 0$.*
*So,If the outcome is $|0\rangle$, then it is impossible to say whether state is $|\psi_1\rangle$ or $|\psi_2\rangle$.*
*Hence non orthogonal states can not be distinguished with certainty.*

**Remark 2.2.3.** *Given states $\{\psi_1, ..., \psi_n\}$ which are linearly independent,there exists a measurement systems $M_1, ..., M_n$ such that if $i^{th}$ occurs, then state $\psi_i$ is received.*

## 2.3 Composite system

*As described in Postulate 4 that the state of a composite system is tensor product of the state space of component system. If the state space of composite systems are $H_1, H_2, .., H_n$ and let $i^{th}$ component be in state $\psi_i$, then state of composite system is $\psi_1 \otimes ... \otimes \psi_n$.*

**Example 2.3.1.** *Suppose we have two systems.State of the first system is given by $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and the second is given by $\frac{1}{\sqrt{2}}|0\rangle + \iota\frac{1}{\sqrt{2}}|1\rangle$.Then state space of the composite system is $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ and state is given by:*

$$\begin{aligned}
\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes \frac{1}{\sqrt{2}}|0\rangle + \iota\frac{1}{\sqrt{2}}|1\rangle &= \frac{|0\rangle \otimes |0\rangle + |0\rangle \otimes \iota|1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes \iota|1\rangle}{2} \\
&= \frac{|00\rangle + \iota|01\rangle + |10\rangle + \iota|11\rangle}{2}.
\end{aligned}$$

*where* $|00\rangle = |0\rangle \otimes |0\rangle, |01\rangle = |0\rangle \otimes |1\rangle, |10\rangle = |1\rangle \otimes |0\rangle, |11\rangle = |1\rangle \otimes |1\rangle$

### 2.3.1 Measurements in Composite systems

## Tensor product of operators:

*Given $R : H \to H, T : K \to K$, there exists a unique operator*

$$R \otimes T : H \otimes K \to H \otimes K$$

*given by*

$$R \otimes T(\sum_{i=1}^{n} h_i \otimes k_i) = \sum_{i=1}^{n} (Rh_i) \otimes (Tk_i), \text{ where } h_i \in H, k_i \in K \text{ for } 1 \leq i \leq n.$$

## Properties of tensor product of operators.

**Theorem 2.3.2.** *(i) If $R_i : H \to H,\ T_i : K \to K,$ for $i = 1, 2.$ then*

$$(R_1 \otimes T_1)(R_2 \otimes T_2) = (R_1R_2) \otimes (T_1T_2.)$$

*(ii)* $(R \otimes T)^* = R^* \otimes T^*.$

*Proof.* (i) let $h_i \in H, k_i \in K$.Then
$(R_1 \otimes T_1)(R_2 \otimes T_2)(\sum_{i=1}^{n} h_i \otimes k_i) = (R_1R_2 \otimes T_1T_2)(\sum_{i=1}^{n} h_i \otimes k_i).$
$R_i \otimes T_i : H \otimes K \to H \otimes K$ ,for $i = 1, 2$ then,

$$(R_1 \otimes T_1)(R_2 \otimes T_2) : H \otimes K \to H \otimes K.$$

and

$$\begin{aligned}(R_1 \otimes T_1)(R_2 \otimes T_2)(\sum_{i=1}^{n} h_i \otimes k_i) &= (R_1 \otimes T_1)(\sum_{i=1}^{n} R_2h_i \otimes \sum_{i=1}^{n} T_2k_i) \\ &= \sum_{i=1}^{n} (R_1R_2h_i \otimes T_1T_2k_i) \\ &= (R_1R_2 \otimes T_1T_2)(\sum_{i=1}^{n} h_i \otimes k_i).\end{aligned}$$

*Proof.* (ii) Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then,

$$\begin{aligned}\langle h_1 \otimes k_1 | (R \otimes T)^*(h_2 \otimes k_2)\rangle &= \langle (R \otimes T)(h_1 \otimes k_1) | h_2 \otimes k_2)\rangle \\ &= \langle Rh_1 \otimes Tk_1 | h_2 \otimes k_2\rangle \\ &= \langle Rh_1 | h_2\rangle_H . \langle Tk_1 | k_2\rangle_K \\ &= \langle h_1 | R^*h_2\rangle_H . \langle k_1 | T^*k_2\rangle_K \\ &= \langle h_1 \otimes k_1 | (R^* \otimes T^*)(h_2 \otimes k_2)\rangle.\end{aligned}$$

Hence, $(R \otimes T)^* = R^* \otimes T^*.$

## 2.4 Quantum gates

Classical Computer circuit consists of Logic gates. Logic gates perform manipulation of information converting it from one to another. Quantum analog of logic gates are unitary operator which is represented by matrices. quantum gates in the form of linear operator interacts with qubit or multiple qubits through tensor product operation.

**Note 2.4.1.** *Firstly we will describe quantum gates which acts on single qubit and then we move to the quantum gates which act on multiple qubits/Quantum register.*

### 2.4.1 Quantum gates

- ***Pauli X gate:*** *It is Quantum equivalent of 'NOT'gate.It maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. It is represented by Pauli X matrix.*

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

- ***Pauli Y gate:*** *It maps $|0\rangle$ to $\iota|1\rangle$ and $|1\rangle$ to $-\iota|0\rangle$. It is represented by Pauli Y matrix:*

$$Y = \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix}.$$

- ***Pauli Z gate:*** *It leaves the basis state $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$. It is represented by Pauli Z matrix:*

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

- ***Hadamard gate:*** *It maps $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. It is represented by Hadamard matrix.*

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

- ***Swap gate:*** *It acts on two or more qubits. Multiple qubits are obtained by taking tensor product of single qubits. Swap gate maps*

$$\begin{aligned}
|0\rangle \otimes |0\rangle &= |00\rangle \mapsto |00\rangle \\
|0\rangle \otimes |1\rangle &= |01\rangle \mapsto |10\rangle \\
|1\rangle \otimes |0\rangle &= |10\rangle \mapsto |01\rangle \\
|1\rangle \otimes |1\rangle &= |11\rangle \mapsto |11\rangle.
\end{aligned}$$

*If we consider above as standard ordered basis then swap gate can be represented by the matrix.*

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

- ***Controlled Gate:*** *It acts on two or more qubits where one or more qubit acts as a control for some operation.*

**Example 2.4.2.** *Controlled NOT gate: It performs the 'NOT'operation on second qubit only when first qubit is 1 otherwise it leaves it as it is. It maps*

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |11\rangle \\ |11\rangle &\mapsto |10\rangle. \end{aligned}$$

*This is represented by the matrix.*

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

***Taffoli gate:*** *It acts on 3-qubits. It is also called 'CCNOT'gate. It performs the NOT operation on third qubit if first two qubits are 1. It maps*

$$\begin{aligned} |000\rangle &\mapsto |000\rangle \\ |010\rangle &\mapsto |010\rangle \\ |100\rangle &\mapsto |100\rangle \\ |110\rangle &\mapsto |111\rangle \\ |001\rangle &\mapsto |001\rangle \\ |011\rangle &\mapsto |011\rangle \\ |101\rangle &\mapsto |101\rangle \\ |111\rangle &\mapsto |110\rangle \end{aligned}$$

*It is represented by the matrix.*

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

## 2.5 Quantum cloning

**Definition 2.5.1.** *Quantum cloning is a process that takes an arbitrary unknown quantum state and make a copy of it without altering the original state.*

**Example 2.5.2.** *Consider the CNOT gate. Let this gate be represented by unitary operator $U$ .Then $U : \mathbb{C}^2 \to \mathbb{C}^2$ is given by*

$$U(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$$

$$U(|0\rangle \otimes |1\rangle) = |0\rangle \otimes |1\rangle$$

$$U(|1\rangle \otimes |1\rangle) = |\rangle \otimes |0\rangle$$

$$U(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle$$

*From the last equation, It follows that CNOT can clone.Note that states given in last equation are orthogonal to each other.*

### No cloning:

*It prevents in producing further copies of an arbitrary Quantum state.*

**Example 2.5.3.** *Let $\psi = \alpha e_0 + \beta e_1 = \alpha|0\rangle + \beta|1\rangle$. Let CNOT be represented by unitary operator U.Apply $U$ to $\psi \otimes e_0$, we get*

$$U(\psi \otimes e_0) = U(\alpha e_0 + \beta e_1) \otimes e_0 = U(\alpha e_0 \otimes e_0) + U(\beta e_1 \otimes e_0.) \tag{2.7}$$

*Suppose U can clone $\psi$. Then Eq. (2.7) should be equal to $\psi \otimes \psi$.*
*But Eq. (2.7) turns out to be $\alpha^2 e_0 \otimes e_0 + \alpha\beta(e_o \otimes e_1 + e_1 \otimes e_0) + \beta^2 e_1 \otimes e_1$. If $\alpha\beta \neq 0$, then U can not clone $\psi$. The only case when U can clone $\psi$ is either $\psi = e_0$ or $\psi = e_1$.*
*Hence, In general it is impossible to have a universal unitary operator that can clone any arbitrary quantum state. This gives a motivation for 'No cloning theorem'.*

### No cloning Theorem:

**Theorem 2.5.4.** *An arbitrary Quantum state can not be cloned.*

*Proof.* Let $\psi \in H$ be any arbitrary state and $U$ be a unitary operator that can clone $\psi$. Then for all $\psi \in H$.we have,

$$U(\psi \otimes \phi) = (\psi \otimes \psi).$$

Also,

$$U((-\psi) \otimes \phi) = U(-\psi) \otimes (-\psi) = \psi \otimes \psi \tag{2.8}$$

Then,

$$\begin{aligned} U((-\psi) \otimes \phi) &= U(-(\psi \otimes \phi)) \\ &= -U(\psi \otimes \phi) \\ &= -(\psi \otimes \psi). \end{aligned}$$

which is a contradiction.

## 2.6 Quantum Parallelism

Consider the Hadamard gate which is represented by

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

Let $e_0$ and $e_1$ be orthonormal basis for $H$..Then,

$$He_0 = \frac{e_0 + e_1}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

We write

$$\underbrace{He_0 \otimes He_0 \otimes ... \otimes He_0}_{\text{n times}}$$

as

$$\begin{aligned} H^n(e_0 \otimes e_0 ... \otimes e_0) &= \underbrace{(He_0) \otimes (He_0) \otimes ... \otimes (He_0)}_{\text{n times}} \\ &= \underbrace{\frac{e_0 + e_1}{\sqrt{2}} \otimes \frac{e_0 + e_1}{\sqrt{2}} \otimes ... \otimes \frac{e_0 + e_1}{\sqrt{2}}}_{\text{n times}}. \end{aligned}$$

When $n = 2$, we have,

$$\frac{e_0 + e_1}{\sqrt{2}} \otimes \frac{e_0 + e_1}{\sqrt{2}} = \frac{e_0 \otimes e_0 + e_0 \otimes e_1 + e_1 \otimes e_0 + e_1 \otimes e_1}{(\sqrt{2})^2} = (\frac{1}{(\sqrt{2}})^2 \sum_{i,j \in \mathbb{Z}_2} (e_i \otimes e_j) \tag{2.9}$$

In general,
$H^n(e_0 \otimes e_0 ... \otimes e_0) = (\frac{1}{\sqrt{2}})^n \sum_{i,j \in \mathbb{Z}_2^n} (e_i \otimes e_j)$

## 2.7 Applications of Quantum Mechanics

(i) The biggest application of a quantum computer is its ability to factorize a very large number into product of two prime numbers. Most of the popular public key ciphers are based on the difficulty of factoring integers or the discrete logarithm problem, which can both be solved by Shor's algorithm

(ii) Atomic clocks are the most accurate time and frequency standards known and are used as primary standards for International distribution services. Inaccuracy of Atomic clock is due to Quantum noise.

(iii) Quantum cryptography describes the use of quantum computation and quantum communication to perform cryptographic tasks or to break cryptographic systems.

# Chapter 3

# Mathematical approach to Quantum mechanics

## 3.1 Introduction

This chapter deals with mathematical analogy of quantum mechanics. It accomplishes two tasks, firstly, it gives information about quantum system using density operator, even if state of the system is not known. Secondly, it provides information about component system using the definition of partial trace. We start with defining density operator. We will see that every idea of quantum mechanics can be studied in terms of density operator. Based on this formulation, we will reformulate the postulates of quantum mechanics. We study about partial trace and reduced density operator. We close this chapter with some applications of density operator.

**Definition 3.1.1.** *Consider a composite system made up of two component system. Let $\psi$ be the state of the composite system such that $\psi$ can not be written as tensor product of states of component systems. Then this phenomenon is called* ***entanglement*** *and state of the system is called* ***entangled state****.*

**Example 3.1.2.** *Consider the two qubit state and $\psi = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. We will prove that $\psi$ is an entengled state that is $\psi$ can not be written as tensor product of states of component system. There does not exist single qubit $|a\rangle$ and $|b\rangle$ such that $\psi = |a\rangle \otimes |b\rangle = |ab\rangle$. On the contrary, assume that there exists two single qubit $|a\rangle = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix}$ and $|b\rangle = \begin{bmatrix} b_{11} \\ b_{21} \end{bmatrix}$. then*

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \begin{pmatrix} a_{11}b_{11} \\ a_{11}b_{21} \\ a_{21}b_{11} \\ a_{21}b_{21} \end{pmatrix}$$

*After equating the corresponding entries of above two matrices, we get*

$$a_{11}b_{11} = 1$$

$\Rightarrow a_{11}$ *and* $b_{11}$ *are both nonzero.*

$$a_{11}b_{21} = 0$$

$$\Rightarrow b_{21} = 0$$

$$a_{21}b_{11} = 0$$

$$\Rightarrow a_{21} = 0$$

$$a_{21}b_{21} = 1$$

$\Rightarrow a_{21}$ *and* $b_{21}$ *are both nonzero.*

*First two equations give* $a_{21}b_{21} = 0$*. This is a contradiction.*
*Hence, state* $\psi$ *is in entangled state.*

## 3.2 Density operator

**Definition 3.2.1.** *An ensemble denoted by,* $\{p_i, \psi_i\}$ *is a set of states* $\psi_i$ *together with the probabilities* $p_i \geq 0$ *and* $\sum\limits_{i=1}^{l} p_i = 1$.

**Note 3.2.2.** *Given a measurement system* $\{M_\alpha\}$*, the probability of outcome* $\alpha$ *given this ensemble is,*

$$p_\alpha(\{p_i, \psi_i\}) = \sum_{i=1}^{l} p_i \|M_\alpha(\psi_i)\|^2. \quad (See\,Sec(1.2)) \tag{3.1}$$

**Definition 3.2.3.** *Consider an ensemble of states* $\{p_i, \psi_i\}$*, then*
***density operator*** *for this ensemble is defined as*

$$\rho = \sum_{i=1}^{l} p_i |\psi_i\rangle\langle\psi_i| \tag{3.2}$$

**Remark 3.2.4.** *Let* $\rho$ *be the density operator arises from ensembles* $\{\psi_i, p_i\}$*. Let* $e_n$ *denote an orthonormal basis of* $H$*. Then the matrix representation of density operator with respect to given orthonormal basis is:*

$$\rho_{mn} = \sum_i p_i(\langle e_m|\psi_i\rangle)(\langle\psi_i|e_n\rangle).$$

*This matrix is called* ***density matrix****.*

**Example 3.2.5.** ***Evolution of density operator for a closed quantum system:*** *Suppose the evolution of a closed system is described by a unitary operator U. Let* $\{p_i, \psi_i\}$ *be the ensemble of states. Density operator corresponding to this ensemble is:*

$$\rho = \sum_{i=1}^{l} p_i |\psi_i\rangle\langle\psi_i|. \tag{3.3}$$

*After evolution,state of the system is $U(|\psi_i\rangle)$. Then the corresponding density operator is given as*

$$\begin{aligned}
\rho' &= \sum_{i=1}^{l} p_i(U|\psi_i\rangle)(U|\psi_i\rangle)^* && (3.4)\\
&= \sum_{i=1}^{l} p_i U|\psi_i\rangle\langle\psi_i|U^* && (3.5)\\
&= U(\sum_{i=1}^{l} p_i|\psi_i\rangle\langle\psi_i|)U^* && (3.6)\\
&= U\rho U^*. && (3.7)
\end{aligned}$$

***Measurement in terms of Density operator:*** *Suppose we perform a measurement described by a measurement operator $M_m$.Let $\psi_i$ be the initial state of the system. Let $p(i)$ denotes the probability of getting state $|\psi_i\rangle$. Then probability of getting result $m$ when initial state is $\psi_i$ is*

$$\begin{aligned}
p(m/i) &= \langle\psi_i|M_m^* M_m|\psi_i\rangle && (3.8)\\
&= tr(M_m^* M_m|\psi_i\rangle\langle\psi_i|). && (3.9)
\end{aligned}$$

*It follows from equation* (1.4)
*By the law of total probability, probability of getting result $m$ is*

$$\begin{aligned}
p(m) &= \sum_i p(|\psi_i\rangle)p(m|i) && (3.10)\\
&= \sum_i p(i)p(m|i) && (3.11)\\
&= \sum_i p(i)tr(M_m^* M_m|\psi_i\rangle\langle\psi_i|) && (3.12)\\
&= tr(\sum_i p(i)(M_m^* M_m|\psi_i\rangle\langle\psi_i|)) && (3.13)\\
&= tr(M_m^* M_m \sum_i p(i)|\psi_i\rangle\langle\psi_i|) && (3.14)\\
&= tr(M_m^* M_m \rho). && (3.15)
\end{aligned}$$

*We will calculate the density operator of the system after obtaining the measurement result $m$. This formula gives an elegant expression to calculate the density operator of the system if outcome $m$ and the density operator corresponding to the ensemble of state before measurement is known.*
*If the initial state of the system is $|\psi_i\rangle$, then the state after obtaining the result $m$ is*

$$\begin{aligned}
|\psi_m\rangle &= \frac{M_m|\psi_i\rangle}{\| M_m|\psi_i\rangle\|} && (3.16)\\
&= \frac{M_m|\psi_i\rangle}{\sqrt{tr(M_m^* M_m|\psi_i\rangle\langle\psi_i|}}. && (3.17)
\end{aligned}$$

*Let $\rho_m$ be the density operator after the measurement $m$.Then,*

$$\rho_m = \sum_i p(i/m)|\psi_m\rangle\langle\psi_m|. \tag{3.18}$$

*By the law of probability*

$$p(i/m) = p(i,m)/p(m) \tag{3.19}$$
$$p(i,m) = p(m/i)p(i) \tag{3.20}$$
$$= tr(M_m^* M_m|\psi_i\rangle\langle\psi_i|)p(i). \tag{3.21}$$

*Substitute the value of $p(i,m)$ (Refer equation*(3.20)*) and value of $p(m)$ (Refer equation* (3.15)*) in equation* (3.19), *we get,*

$$p(i/m) = \frac{tr(M_m^* M_m|\psi_i\rangle\langle\psi_i|)p(i)}{tr(M_m^* M_m\rho)}. \tag{3.22}$$

*Substituting the value of $|\psi_m\rangle, \langle\psi_m|, p(i/m)$ in equation* (3.18) *we get,*

$$\rho_m = \sum_i \frac{(M_m|\psi_i\rangle\langle\psi_i|M_m^*)tr(M_m^* M_m|\psi_i\rangle\langle\psi_i|)p(i)}{tr(M_m^* M_m|\psi_i\rangle\langle\psi_i|)tr(M_m^* M_m\rho)}. \tag{3.23}$$
$$= \frac{M_m\rho M_m^*}{tr(M_m^* M_m\rho)}. \tag{3.24}$$

**Note 3.2.6.** *A quantum system whose state is exactly known is called* ***pure state****. Density operator for such system is, $\rho = |\psi\rangle\langle\psi|$. Otherwise, $\rho$ is in mixed state of ensembles.*

**Note 3.2.7.** *Consider a quantum system is prepared in the state $\rho_i$ with probability $p_i$. Then this system may be described by density matrix*

$$\rho = \sum_i p_i\rho_i.$$

***Justification:*** *Suppose that $\rho_i$ arises from ensembles $\{p_{ij}, \psi_{ij}\}$ ($i$ is fixed). Let $p_i$ denotes the probability that system is in state $\psi_i$. Then the probability that the state of the system is $\psi_{ij}$ is $p_i p_{ij}$. Then,*

$$\begin{aligned}\rho &= \sum_i\sum_j p_i p_{ij}|\psi_{ij}\rangle\langle\psi_{ij}\rangle \\ &= \sum_i p_i \sum_j p_{ij}|\psi_{ij}\rangle\langle\psi_{ij}\rangle \\ &= \sum_i p_i\rho_i\end{aligned}$$

### 3.2.1 Properties of Density operator

***Characterization of Density operator:*** *An operator $\rho$ is the density operator associated to some ensembles $\{p_i, \psi_i\}$ iff it satisfies the following conditions:*

1. ***(Trace condition)*** *$\rho$ has trace equal to 1.*
2. ***(Positivity condition)*** *$\rho$ is a positive operator.*

*Proof.* Assume that $\rho = \sum\limits_i p_i|\psi_i\rangle\langle\psi_i|$ be the density operator associated to ensembles $\{p_i, \psi_i\}$.

$$\begin{aligned} tr(\rho) &= tr(\sum_i p_i|\psi_i\rangle\langle\psi_i|) \\ &= \sum p_i tr(|\psi_i\rangle\langle\psi_i|) \\ &= \sum p_i = 1. \end{aligned}$$

Hence, $Tr(\rho) = 1$.
We will prove that $\rho$ is a positive operator. let $\psi$ be any state vector. Consider,

$$\begin{aligned} \langle\psi|\rho|\psi\rangle &= \langle\psi|(\sum_i p_i|\psi_i\rangle\langle\psi_i|)|\psi\rangle \\ &= \langle\psi|\sum_i p_i|\psi_i\rangle\langle\psi_i|\psi\rangle \quad \text{(It follows from the definition of outer product.)} \\ &= \sum_i p_i\langle\psi||\psi_i\rangle\langle\psi_i|\psi\rangle \\ &= \sum_i p_i|\langle\psi|\psi_i\rangle|^2 \geq 0. \end{aligned}$$

Hence $\rho$ is a positive operator.
Conversely, Suppose that $\rho$ is any operator satisfying Trace and positivity condition. We will show that $\rho$ is a density operator.
By hypothesis $\rho$ positive. By Spectral decomposition theorem , $\rho$ can be written as

$$\rho = \sum_j \lambda_j|e_j\rangle\langle e_j|$$

where $|j\rangle$ are orthogonal to each other. Since $\rho$ is positive so $\lambda_j \geq 0 \forall j$. From trace condition, $\sum\limits_j \lambda_j = 1$. Therefore a system in state $|j\rangle$ with probability $\lambda_j$ will have density operator $\rho$. that is ensemble $\{\lambda_j, e_j\}$ gives rise to density operator $\rho$.

### 3.2.2 Density operator for composite ensembles

Consider two physical system $A$ and $B$ with state space $H_A$ and $H_B$ respectively. Let $\{p_i, \psi_i\}$ be an ensemble in system $A$ and $\{q_j, \phi_j\}$ be an ensemble in system $B$. Then composite system is represented by a density operator on $H_A \otimes H_B$.
Suppose that systems $A$ and $B$ are in state $\psi_i$ and $\phi_j$ with probability $p_i, q_j$ respectively. Then

Postulate 4 says that $\{p_i q_j, \psi_i \otimes \phi_j\}$ is an ensemble in composite system. Then density operator for composite system is given by:

$$\rho_{composite} = \sum_{i,j} p_i q_j |\psi_i \otimes \phi_j\rangle\langle\psi_i \otimes \phi_j| \tag{3.25}$$

$$= \sum_{i,j} p_i q_j (|\psi_i\rangle\langle\psi_i|) \otimes (|\phi_j\rangle\langle\psi_j|). \tag{3.26}$$

**Note 3.2.8.** *Above theorem characterizes the density operator. We can define a density operator to be a positive operator whose trace is equal to* $1$*. This characterization allows us to rephrased the Basic postulates of Quantum mechanics in terms of density operator. It has nothing to do with state of the system. Here Basic unit is density operator.*

### 3.2.3 Reformulation of postulates:

***Postulate 1.*** *Associated to any physical system is a complex Hilbert space known as state space of the system. State of the system is completely described in terms of density operator, which is a positive operator with trace* $1$ *acting on the state of the system. If a Quantum system is in state* $\rho_i$ *with probability* $p_i$ *then density operator for this system is* $\sum\limits_i p_i\rho_i$*.* ***Postulate 2:*** *The evolution of closed Quantum system is described by Unitary transformation. That the density operator* $\rho$ *of the system at time* $t_1$ *is related to density operator* $\rho'$ *of the system at time* $t_2$ *where* $t_1{<}t_2$ *by*

$$\rho' = U\rho U^*.$$

***Postulate 3:*** *Quantum measurements are described by a collection* $M_m$ *of Measurement operators. These are the operators acting on the state space of the system being measured. The index* $m$ *refers to the outcome. If the state of the Quantum system is* $\rho$ *immediately before the experiment then probability that outcome will be* $m$ *is given by:*

$$p(m) = tr(M_m^* M_m \rho).$$

*and the state of the system after the measurement is*

$$\frac{M_m \rho M_m^*}{tr(M_m^* M_m \rho)}.$$

*The measurement operator satisfy the completeness relation*

$$\sum M_m^* M_m = I.$$

***Postulate 4:*** *The state space of the composite physical system is the tensor product of state space of the component physical systems. Further, If we have system numbered* $1$ *through* $n$ *and state of the system number* $i$ *is* $\psi_i$ *then state of the composite system is* $\psi_1 \otimes \psi_2 \otimes ... \otimes \psi_n$*.*

**Example 3.2.9.** ***Criterion to decide if a state is mixed or pure:*** *Let* $\rho$ *be a density operator then show that* $tr(\rho^2) \leq 1$ *and it is an equality if* $\rho$ *is a pure state.*
***justification:*** *If system is in mixed state:*

*we will prove that* $tr(\rho_2) \leq 1$.
$\rho$ *is a diagonalizable operator So, it is similar to a diagonal matrix D say* $= diag(p_1, p_2, ...p_n)$ *and each* $p_i > 0$ *then* $\rho^2$ *is similar to* $D^2$. *Hence,*$tr(\rho^2) = \sum\limits_{i=1}^{n} p_i^2$.

$$\sum_{i=1}^{n} p_i = 1, \textit{ Square both sides,we get}$$
$$(\sum_{i=1}^{n} p_i^2) = \sum_{i=1}^{n} p_i^2 + (\textit{ some positive terms}) = 1$$
$$\sum_{i=1}^{n} p_i^2 = 1 - (\textit{ some positive terms}) < 1.$$

*Hence,*$tr(\rho^2) \leq 1$
*If system is in pure state* $\psi$ *say, then* $\rho = |\psi\rangle\langle\psi|$
*Hence,* $Tr(\rho^2) = \|\rho\|^2 = 1$.

**Note 3.2.10.** *Two different ensembles of Quantum states can give rise to same density operator as shown in following example:*

**Example 3.2.11.** *Suppose that a Quantum system with density operator is*

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|.$$

*Then system is in state* $|0\rangle$ *with probability 3/4 and it is in state* $|1\rangle$ *with probability 1/4. Define*

$$|a\rangle = \sqrt{\frac{3}{4}}|0\rangle\langle 0| + \sqrt{\frac{1}{4}}|1\rangle\langle 1|$$

*and*

$$|b\rangle = \sqrt{\frac{3}{4}}|0\rangle\langle 0| - \sqrt{\frac{1}{4}}|1\rangle\langle 1|.$$

*A Quantum system is prepared in the state* $|a\rangle$ *with probability 1/2 and in state* $|b\rangle$ *with probability 1/2. Then corresponding density operator is*

$$\rho = \frac{1}{2}|a\rangle\langle a| + 12|b\rangle\langle b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|.$$

*that is these two different ensembles give rise to same density operator. Above discussion leads to a Question that which class of ensembles give rise to same density matrix. it motivates the following theorem*

**Remark 3.2.12.** *The sets* $|\tilde{\psi_i}\rangle$ *and* $|\tilde{\phi_j}\rangle$ *gives the same density operator if and only if*

$$|\tilde{\psi_i}\rangle = \sum_j u_{ij}|\tilde{\psi_i}\rangle.$$

## 3.3 Trace

*Identify $L(\mathbb{C}^n)$ as $M_n$.Let $A(a_{ij}) \in M_n$. Then*

$$tr(A) = \sum_{i=1}^{n} a_{ii} = \sum_{i=1}^{n} \langle e_i | Ae_i \rangle.$$

**Proposition 3.3.1.** *Let $\{u_1, u_2, ..., u_n\}$ be an orthonormal basis for $\mathbb{C}^n$. Then,*

$$tr(A) = \sum_{i=1}^{n} \langle u_i | Au_i \rangle.$$

**Remark 3.3.2.** *Let $R \in H_A, T \in H_B$ then $R \otimes T \in H_A \otimes H_B$. defined as*

$$R \otimes T(\sum_i h_i \otimes k_i) = \sum_i (Rh_i \otimes Tk_i).$$

**Proposition 3.3.3.** *Let $R \in H_A, T \in H_B$ then $tr(R \otimes T) = tr(R)tr(T)$.*

*Proof.* Let $\{e_1, e_2, ..., e_n\}$ and $\{f_1, f_2, ..., f_m\}$ be orthonormal basis for $H_A$ and $H_B$ respectively. Then

$$\{e_i \otimes f_j : 1 \leq i \leq n, 1 \leq j \leq m\}$$

is an orthonormal basis for $R \otimes T$. Therefore,

$$\begin{aligned} tr(R \otimes T) &= \sum_{i=1}^{n} \sum_{j=1}^{m} \langle (e_i \otimes f_j) | (R \otimes T)(e_i \otimes f_j) \rangle \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} \langle (e_i \otimes f_j) | (Re_i) \otimes (Tf_j) \rangle \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} \langle e_i | Re_i \rangle_{H_A} \langle f_j | Tf_j \rangle_{H_B} \\ &= (\sum_{i=1}^{n} \langle e_i | Re_i \rangle)_{H_A} (\sum_{j=1}^{m} \langle f_j | Tf_j \rangle)_{H_B} \\ &= tr(R)tr(T). \end{aligned}$$

**Proposition 3.3.4.** *Let $H_A$ and $H_B$ be two finite dimensional Hilbert spaces then $\tau : L(H_A) \otimes L(H_B) \rightarrow L(H_A \otimes H_B)$is an isomorphism.*

*Proof.* Let $\dim(H_A) = m$ and $\dim(H_B) = n$ then
$\dim L(H_A) = m^2$, $\dim L(H_B) = n^2$ Hence, $\dim(L(H_A) \otimes L(H_B)) = m^2 n^2$.
$\dim(L(H_A \otimes H_B)) = m^2 n^2$. Hence dimensions of both spaces are equal.

To show that $\tau$ is an isomorphism, it is enough to show that $\tau$ is injective.
we will show that $ker(\tau) = \{0\}$.
Identify $L(H_B)$ as $M_n$ which has a basis $\{E_{ij} : 1 \leq i, j \leq n.\}$

Chose an orthonormal basis $\{f_1, f_2, ..., f_n\}$ for $H_B$ such that

$$E_{ij} f_l = \begin{cases} f_i, & j = l \\ 0, & j \neq l \end{cases}$$

Given $X \in ker(\tau)$. Then from proposition (1.10.5) there exists unique $X_{ij} \in L(H_A)$ such that

$$X = \sum_{i,j=1}^{m} X_{ij} \otimes E_{ij}.$$

**claim:** $X = 0$.
$X = 0$ if and only if $X_{ij} = 0 \forall 1 \leq i, j \leq m$.
It is enough to prove that $X_{ij} = 0 \forall 1 \leq i, j \leq m$
$\tau(X) : H_A \otimes H_B \to H_A \otimes H_B$

$$\begin{aligned} \tau(X)(h \otimes l) &= \sum_{i,j=1}^{m} (X_{ij} \otimes E_{ij})(h \otimes l) \\ &= \sum_{i,j=1}^{m} (X_{ij} h) \otimes (E_{ij} l) \end{aligned}$$

Above equation is true for all $h \in H_A, l \in H_B$.
pick $l = f_l$. Then,

$$\begin{aligned} 0 &= \tau(X)(h \otimes f_l) \\ &= \sum_{i,j=1}^{n} (X_{ij} h) \otimes (E_{ij} f_l) \\ &= \sum_{i=1}^{n} (X_{il} h) \otimes (f_i) \end{aligned}$$

that is $X_{il} h = 0 \forall 1 \leq i \leq n$ and $\forall h \in H$. This implies $X_{il} = 0 \, \forall i$. Repeat this process for all $l$ and get $X_{il} = 0$ for all $l$. Therefore,$X = 0$.

**Note 3.3.5.** *Above theorem is useful in defining partial trace.*

**Note 3.3.6.** *Recall from chapter* 1*.Let $H_A$ and $H_B$ be two finite dimensional Hilbert spaces with dimensions $m$ and $n$. Then*

$$\begin{aligned} &H_A \otimes H_B \cong H_A \oplus ... \oplus H_A (n \text{ copies}). \\ &H_A \otimes H_B \cong H_B \oplus ... \oplus H_B (m \text{ copies}). \end{aligned}$$

**Proposition 3.3.7.** *Let $H_A$ and $H_B$ be two finite dimensional Hilbert spaces with dimensions $m$ and $n$.Then*

$$\begin{aligned} &L(H_A \otimes H_B) \cong L(H_A \oplus ... \oplus H_A)(n \text{ copies}). \\ &L(H_A \otimes H_B) \cong L(H_B \oplus ... \oplus H_B)(m \text{ copies}). \end{aligned}$$

## 3.4 Partial Trace

*We will use proposition* (3.3.4) *in defining Partial trace.*

**Definition 3.4.1.** *Suppose we have Physical systems $A$ and $B$ with corresponding state spaces are $H_A$ and $H_B$. Then Partial trace over system $B$, denoted as $tr_B$ is defined by*

$$tr_B : L(H_A \otimes H_B) \to L(H_A)$$

*We define this map as follows:*
*Identify* $L(H_A \otimes H_B) \cong L(H_A) \otimes L(H_B)$.
*Given*

$$X = \sum_i R_i \otimes T_i. \textit{ Then,}$$

$$tr_B(X) = \sum_i tr(T_i)R_i.$$

*Define,*

$$A : L(H_A) \times L(H_B) \to L(H_A)$$

*such that*

$$(R, T) \mapsto tr(T)R$$

*Then,* $A$ *is a bilinear mapping.By universal property of Tensor product,there exists a linear mapping* $\tilde{A} : L(H_A) \otimes L(H_B) \to L(H_A)$ *such that*

$$\tilde{A}(R \otimes T) = A(R, T).$$

*map* $\tilde{A}$ *coincides with the map* $tr_B(X)$. *Hence it is well defined. Given* $X \in L(H_A \otimes H_B)$. *We write* $X^B = tr_A(X) \in L(H_A)$.

*Similarly,*

$$tr_B : L(H_A) \times L(H_B) \to L(H_A)$$

*such that*

$$(R, T) \mapsto tr(R)T$$

*Given* $X \in L(H_A \otimes H_B)$. *We write* $X^A = tr_B(X) \in L(H_B)$.

### 3.4.1 Another way to define partial trace

*We will give an explicit formula to calculate the partial trace* $tr_B$ *and* $tr_A$ *with the assumption that* $H_A$ *and* $H_B$ *are finite dimensional Hilbert space. Let dim*$(H_A) = m$ *and dim*$(H_A) = n$.
*Identify* $L(H_B) \cong M_n$ *which has a basis* $\{E_{ij} : 1 \leq i, j \leq n.\}$
*Chose an orthonormal basis* $\{f_1, f_2, ..., f_n\}$ *for* $H_B$ *such that*

$$E_{ij} f_l = \begin{cases} f_i, & j = l \\ 0, & j \neq l \end{cases}$$

*Given* $X \in ker(\tau)$. *Then from* **??** *there exists unique* $X_{ij} \in L(H_A)$ *such that*

$$X = \sum_{i,j=1}^{m} X_{ij} \otimes E_{ij}$$

*Then,Partial traces are given by:*

$$\begin{aligned}
tr_B(X) &= tr_B(\sum_{i,j=1}^{m} X_{ij} \otimes E_{ij}) \\
&= \sum_{i,j}^{n} X_{ij} tr(E_{ij}) \\
&= \sum_{i}^{n} X_{ii} \in L(H_A) \\
tr_A(X) &= tr_A(\sum_{i,j=1}^{m} X_{ij} \otimes E_{ij}) \\
&= \sum_{i,j}^{n} E_{ij} tr(X_{ij}) \\
&= \sum_{i,j}^{n} E_{ij} tr(X_{ij}) \in L(H_B)
\end{aligned}$$

### 3.4.2 Reduced density operator

*The biggest application of density operator is to provide a tool to get information about subsystems of composite system.*

**Definition 3.4.2.** *Suppose A and B be two physical system and $\rho_{AB}$ be the density operator for composite system. Then reduced density operator for system A is denoted by,$\rho_A$ is:*

$$\rho_A = tr_B(\rho_{AB})$$

*where $tr_B$ is the partial trace over system $B$. Reduced density operator $\rho_A$ describes completely all properties of component system A when system B is left unobserved.*

## 3.5 Applications

*(i) Superdense coding is surprising application of Quantum Information theory. This technique is used to send two bits of classical information using only one qubit. Entanglement is used to accomplishes this task.*

*(ii) A Quantum Computer is a device that makes direct use of Quantum mechanics Phenomenon such as superpositions, entanglement and Quantum Parallelism, to perform operations on data.*

# Chapter 4

# Positive matrices

## 4.1 Introduction

*Chapter 4 focuses on basic definitions and crucial results regarding positive definite matrices. It includes some equivalent conditions of a positive definite matrix. We study about block matrices and contractions. This section includes equivalent conditions for a block matrix to be positive in terms of contraction maps. These result will be used very frequently in later chapters.*

*Throughout, we assume the scalar field is $\mathbb{C}$. Let $M_n(\mathbb{C})$ denotes the space of all $n \times n$ matrices over $\mathbb{C}$. We consider finite dimensional Hilbert space throughout the chapter. we denote them by $\mathcal{H}, \mathcal{H}_1$ and $\mathcal{H}_2$ etc. Let $\mathcal{L}(\mathcal{H})$ denotes the space of all linear operators on Hilbert space $\mathcal{H}$. If $\mathcal{H} = \mathbb{C}^n$, then $M_n(\mathbb{C})$ can be identified with $B(\mathcal{H})$.*

**Definition 4.1.1.** *A matrix $A \in B(\mathcal{H})$ is called*

1. ***positive** if $\langle Ax, x\rangle \geq 0 \;\; for all\, x \in \mathcal{H}$.*
2. ***strictly positive** if $\langle Ax, x\rangle > 0 \;\; for all\, x \in \mathcal{H}, x \neq 0$.*

**Note 4.1.2.** *If $A$ is a positive matrix, then we denote it by $A \geq 0$ and if $A$ is strictly positive matrix, then we denote it by $A > 0$.*

**Theorem 4.1.3.** *Let $A \in M_n(\mathbb{C})$. Then,*

1. *(a) $A \geq 0 \Leftrightarrow A = A^*$ and all its eigenvalues are non-negative.*

   *(b) $A > 0 \Leftrightarrow A = A^*$ and all its eigenvalues are positive .*
2. *(a) $A \geq 0 \Leftrightarrow A = A^*$ and all its principal minors are non negative.*

   *(b) $A > 0 \Leftrightarrow A = A^*$ and all its principal minors are positive.*
3. *(a) $A \geq 0 \Leftrightarrow A = B^*B$ for some matrix $B \in M_n(\mathbb{C})$.*

   *(b) $A > 0 \Leftrightarrow A = B^*B$ where $B \in M_n(\mathbb{C})$ is non-singular.*
4. *(a) $A \geq 0 \Leftrightarrow A = T^*T$ for some upper triangular matrix $T$.*

   *(b) $A > 0 \Leftrightarrow A = T^*T$ for a unique upper triangular matrix $T$.*

5. *(a.)* $A \geq 0 \Leftrightarrow$ *there exists* $x_1, x_2, ..., x_n \in \mathbb{C}^n$ *such that*

$$a_{ij} = \langle x_i, x_j \rangle.$$

*(b.)* $A > 0 \Leftrightarrow$ *there exists linearly independent vectors* $x_1, x_2, ..., x_n \in \mathcal{H}$ *such that*

$$a_{ij} = \langle x_i, x_j \rangle.$$

## 4.2 Examples

1. *If* $A$ *is a diagonal matrix with all its entries are positive, then* $A$ *is a positive matrix.*

2. *Let* $A \in M_n(\mathbb{C})$ *be a positive matrix. Then,* $X^*AX$ *is positive for any* $X \in M_n(\mathbb{C})$*.*

3. *Let* $\lambda_1, \lambda_2, ..., \lambda_m$ *be positive real numbers. Then, the matrix* $A = a_{ij}$*, where,*

$$a_{ij} = \frac{1}{\lambda_i + \lambda j}$$

*is positive matrix and is called Cauchy matrix. Since,*

$$a_{ij} = \int_0^\infty e^{-(\lambda_i + \lambda_j)t} dt$$

*if we define* $f_i(t) = e^{-\lambda_i t}, 1 \leq i \leq m.$ *then,* $a_{ij} = \langle f_i, f_j \rangle$*.*
*By axiom* $(5)(a)$ *of theorem (4.1.3) above, A is positive.*

*If* $\lambda_1, \lambda_2, ..., \lambda_m$ *are complex numbers with positive real parts, then the matrix* $A = (a_{ij})$ *where,*

$$a_{ij} = \frac{1}{\bar{\lambda}_i + \lambda j}$$

*is positive.*

**Definition 4.2.1.** 1. *Let* $A = (a_{ij})$ *and* $B = (b_{ij}) \in M_n(\mathbb{C})$*. Then, the* ***Schur product*** *of A and B is defined by* $(A \circ B)_{ij} = (a_{ij}b_{ij})$*.*

2. *The* ***symmetrized product*** *of A and B is the matrix* $S = AB + BA$*.*

**Definition 4.2.2.** *Let* $\mathcal{K}$ *be a subspace of a Hilbert space* $\mathcal{H}$ *and* $P$ *be an orthogonal projection onto* $\mathcal{K}$*. Define an operator* $V : \mathcal{K} \to \mathcal{H}$ *such that* $V$ *is the injection of* $\mathcal{K}$ *into* $\mathcal{H}$*. Then, an operator* $A \in \mathcal{B}(\mathcal{H})$ *can be written in block matrix form*

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$

*the operator,* $V^*AV = A_{11}$ *is called compression of A onto* $\mathcal{K}$*. Similarly, Other Block matrices* $A_{ij}$ *can be obtained by defining the operator V accordingly.*

**Proposition 4.2.3.** *A matrix $A$ is positive if and only if all its compressions are positive.*

*Proof.* Every compression of $A$ is of the form $V^*AV$ for some $V \in \mathcal{B}(\mathcal{K})$. Hence, result follows by (2) of example (4.2). Thus, all principal submatrices are positive.
Conversely, let all principal submatrices are positive. Clearly $A$ is hermitian and one calculation shows that coefficients of characteristic polynomial alternate in signs. Hence, By Descartes rule all roots of $A$ are non-negative. Therefore, $A$ is positive, by 1(a) of theorem (4.1.3).

## 4.3 Properties

1. Sum of two positive definite matrices is again positive definite.

   *Proof.* Let $A, B \in M_n(\mathbb{C})$ be two positive matrices. Consider $x \in \mathbb{C}^n$.
   Then, we have,
   $$\langle (A+B)x, x\rangle = \langle Ax, x\rangle + \langle Bx, x\rangle \geq 0.$$
   Hence, $A+B$ is positive. □

2. Tensor product of two positive matrices is positive.

   *Proof.* Let $A, B \in M_n(\mathbb{C})$ be two positive matrices. Consider
   $x \otimes y \in \mathbb{C}^n \otimes \mathbb{C}^n$. Then,
   $$\langle (A \otimes B)x \otimes y, x \otimes y\rangle = \langle Ax, x\rangle . \langle By, y\rangle \geq 0.$$
   Hence, $A \otimes B$ is positive. □

3. Hadamard product of two positive matrices is positive.

   *Proof.* It directly follows from proposition 4.2. Since, $A \circ B$ is compression of $A \otimes B$, which is positive. Hence, $A \circ B$ is positive. □

**Remark 4.3.1.** *1. Multiplication of two positive matrices need not be positive.*

2. *Symmetrized product of two positive matrices need not be positive.*

   *Let*
   $$A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$
   *and*
   $$B = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

*Then, It can be seen that their Symmetrized product is not positive but A and B are positive.*

**Proposition 4.3.2.** *Let $A$ and $B$ be hermitian and suppose $A$ is strictly positive. If the symmetrized product $S = AB + BA$ is positive (strictly positive) then $B$ is positive (strictly positive).*

*Proof.* Since, $B$ is hermitian So, there exists an orthonormal basis such that $B = diag(\lambda_1, \lambda_2..., \lambda_n)$, the diagonal matrix with diagonal entries $(\lambda_1, \lambda_2..., \lambda_n)$. Then, $s_{ii} = 2\lambda_i a_{ii}$. Since, all the diagonal entries of a positive matrix are positive and $S^* = S$ Hence, $\lambda_i \geq 0$. Therefore, $B$ is positive. □

**Proposition 4.3.3.** *If $A$ and $B$ are positive and $A > B$, then $A^{1/2} > B^{1/2}$.*

*Proof.* We have the identity

$$X^2 - Y^2 = \frac{(X+Y)(X-Y) + (X-Y)(X+Y)}{2}$$

If $X$ and $Y$ are strictly positive then $X + Y$ is strictly positive. So, if $X^2 - Y^2$ is strictly positive then, $X - Y$ is positive by proposition (4.3.2). □

**Definition 4.3.4.** *Let $A$ and $B \in B(\mathcal{H})$. We say that $A$ is congruent to $B$ and write $A \sim B$, if there exists an invertible operator $X \in B(\mathcal{H})$ such that $B = X^*AX$. If $X$ is unitary, we say that $A$ is unitarily equivalent to $B$.*

**Definition 4.3.5.** *Let $A = A^*$, then inertia of $A$ is the triples of non-negative integers*

$$In(A) = (\pi(A), \psi(A), \nu(A))$$

*where $\pi(A), \psi(A), \nu(A)$ denote the number of positive, zero and negative eigenvalues of $A$.*

**Remark 4.3.6.** *Two hermitian matrices are congruent if and only if they have the same inertia.*

**Remark 4.3.7.** *Two hermitian matrices are unitarily equivalent if and only if they have same eigenvalues (counted the multiplicity).*

## 4.4 Block Matrices

*A $2n \times 2n$ matrix of the form*

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

*is called* ***block matrix*** *where $A, B, C, D \in M_n(\mathbb{C})$.*
*Before proceeding, we will fix some notations for Block matrices.*

**Theorem 4.4.1.** *Let $A \in B(\mathcal{H})$. Then, $\exists$ a unitary operator $U \in B(\mathcal{H})$ and a positive operator $P$ such that $A = UP$*

**Theorem 4.4.2.** *Let $A \in B(\mathcal{H})$. Then, $\exists$ unitary operators $U, V \in B(\mathcal{H})$ and a diagonal operator $S$ which consists all singular values of $A$ such that $A = USV$.*

**Definition 4.4.3.** *Let $A \in B(\mathcal{H})$. Then, norm of $A$, denoted as $||A||$ and is defined as:*

$$||A|| = \sup_{||x||=1} ||Ax||$$

**Remark 4.4.4.** *Let $A, B \in B(\mathcal{H})$. Then,*

1. $||AB|| \leq ||A||.||B||$.
2. $||A|| = ||A^*||$.
3. $||A|| = ||UAV||$ *for all unitaries $U$ and $V$.*
4. $||A^*A|| = ||A||^2$.

**Definition 4.4.5.** *An operator $A$ is said to be* ***contractive*** *if $||A|| \leq 1$.*

**Proposition 4.4.6.** *The operator $A$ is contractive if and only if the operator*

$$\begin{bmatrix} I & A \\ A^* & I \end{bmatrix}$$

*is positive.*

*Proof.* We will prove it by induction on $dim\mathcal{H}$. If $dim\mathcal{H} = 1$ then theorem says that if $a \in \mathbb{C}$ if and only if the matrix

$$\begin{bmatrix} 1 & a \\ \bar{a} & 1 \end{bmatrix}$$

is positive. To prove the theorem for general case, we will use singular value decomposition of matrix $A$. Let $A = USV$ Then,

$$\begin{bmatrix} I & A \\ A^* & I \end{bmatrix} = \begin{bmatrix} I & USV \\ V^*SU^* & I \end{bmatrix}$$

$$\begin{bmatrix} U & 0 \\ 0 & V^* \end{bmatrix} \times \begin{bmatrix} I & S \\ S & I \end{bmatrix} \times \begin{bmatrix} U^* & 0 \\ 0 & V \end{bmatrix}$$

This matrix is unitarily equivalent to

$$\begin{bmatrix} I & S \\ S & I \end{bmatrix}$$

which in turn is unitarily equivalent to the direct sum

$$\begin{bmatrix} 1 & s_1 \\ s_1 & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & s_2 \\ s_2 & 1 \end{bmatrix} \oplus ... \oplus \begin{bmatrix} 1 & s_n \\ s_n & 1 \end{bmatrix}$$

These $2 \times 2$ matrices are all positive if and only if $s_1 \leq 1$ that is $||A|| \leq 1$.

□

**Proposition 4.4.7.** *Let $A, B \in \mathcal{M}_n(\mathcal{C})$ be positive. Then*

$$\begin{bmatrix} A & X \\ X^* & B \end{bmatrix}$$

*is positive if and only if $X = A^{1/2}KB^{1/2}$ for some contraction $K$.*

*Proof.* Assume that $A$ and $B$ are strictly positive. Then,

$$\left[\begin{array}{cc} A & X \\ X^* & B \end{array}\right] \sim \left[\begin{array}{cc} A^{-1/2} & 0 \\ 0 & B^{-1/2} \end{array}\right] \times \left[\begin{array}{cc} A & X \\ X^* & B \end{array}\right] \times \left[\begin{array}{cc} A^{-1/2} & 0 \\ 0 & B^{-1/2} \end{array}\right] = \left[\begin{array}{cc} A^{-1/2}XB^{-1/2} & 0 \\ B^{-1/2}X^*A^{-1/2} & I \end{array}\right]$$

Let $K = A^{-1/2}B^{-1/2}$. Then by proposition (4.4.6 ), above block matrix is positive if and only if $K$ is a contraction.

□

**Proposition 4.4.8.** *Let $A$ and $B$ be two $n \times n$ strictly positive matrices then*

$$\begin{bmatrix} A & X \\ X^* & B \end{bmatrix}$$

*is positive if and only if $A \geq XB^{-1}X^*$.*

*Proof.* We have,

$$\left[\begin{array}{cc} A & X \\ X^* & B \end{array}\right] \sim \left[\begin{array}{cc} I & -XB^{-1} \\ 0 & I \end{array}\right] \times \left[\begin{array}{cc} A & X \\ X^* & B \end{array}\right] \times \left[\begin{array}{cc} I & 0 \\ -B^{-1}X^* & 0 \end{array}\right] = \left[\begin{array}{cc} A - XB^{-1}X^* & 0 \\ 0 & B \end{array}\right]$$

Clearly, above block matrix is positive if and only if $A \geq XB^{-1}X^*$.

□

**Proposition 4.4.9.** *An $n \times n$ matrix $A$ is positive if and only if*

$$\begin{bmatrix} A & A \\ A & A \end{bmatrix}$$

*is positive.*

*Proof.* Above block matrix can be written as:

$$\left[\begin{array}{cc} A & A \\ A & A \end{array}\right] = \left[\begin{array}{cc} A^{1/2} & 0 \\ A^{1/2} & 0 \end{array}\right] \times \left[\begin{array}{cc} A^{1/2} & A^{1/2} \\ 0 & 0 \end{array}\right]$$

Now, proof directly follows from axiom (3) of theorem (4.1.3) by taking

$$B = \begin{bmatrix} A^{1/2} & A^{1/2} \\ 0 & 0 \end{bmatrix}.$$

□

**Corollary 4.4.1.** *Let $A$ be any $n \times n$ matrix. Then,*

$$\begin{bmatrix} |A| & A^* \\ A & |A^*| \end{bmatrix}$$

*is positive.*

*Proof.* We will use the polar decomposition of $A$. Write $A = UP$ . Then,

$$\begin{bmatrix} |A| & A^* \\ A & |A^*| \end{bmatrix} = \begin{bmatrix} P & PU^* \\ UP & UPU^* \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} \times \begin{bmatrix} P & P \\ P & P \end{bmatrix} \times \begin{bmatrix} I & 0 \\ 0 & U^* \end{bmatrix}$$

Now, proof directly follows from proposition (4.4.9) and example 4.2(ii).

□

**Corollary 4.4.2.** *Let $A \in M_n$ be a normal matrix. Then,*

$$\begin{bmatrix} |A| & A^* \\ A & |A| \end{bmatrix}$$

*is positive.*

*Proof.* If $A$ is normal then, $|A| = |A^*|$. Proof directly follows from corollary (4.4.1) □

## 4.5 Norm on the Schur Product

*Let $A, B \in \mathbb{M}_n(\mathbb{C})$ Define $S_A : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ by*

$$S_A(X) = A \circ X \textit{ for all } X \in M_n(\mathbb{C}).$$

*where $A \circ X$ denotes the schur product of $A$ and $X$. Then,*

$$||S_A|| = \sup_{||X||=1} ||S_A(X)|| = \sup_{||X||\leq 1} ||S_A(X)||.$$

**Theorem 4.5.1.** *(Schur) Let $A = a_{ij}$ be a positive matrix. Then,*

$$||S_A|| = max \ \ a_{ii}$$

.

*Proof.* Let $||X|| \leq 1$. Then, by proposition (4.4.6)

$$\begin{bmatrix} I & X \\ X^* & I \end{bmatrix}$$

is positive and by proposition (4.4.9)

$$\begin{bmatrix} A & A \\ A & A \end{bmatrix}$$

is positive. Hence, Schur product of above two block matrices is positive that is

$$\begin{bmatrix} A \circ I & A \circ X \\ (A \circ X)^* & A \circ I \end{bmatrix}$$

is positive. So, by proposition (4.4.7) , $A \circ X = (A \circ I)^{1/2} K (A \circ I)^{1/2}$ for some contraction $K$. Hence, $||(A \circ X)|| \leq ||(A \circ I)|| = max\ a_{ii}$.
Therefore, $||S_A|| = max\ \ a_{ii}$. □

**Note 4.5.2.** *For each matrix $X$, Let $||X_c||$= maximum of Euclidean norms of columns of $X$. It defines a norm on $M_n(\mathbb{C})$ and $||X_c|| \leq ||X||$.*

**Theorem 4.5.3.** *Let $A \in M_n$ be any matrix. then,*

$$||S_A|| \leq \textit{inf}\ \{||X_C||||Y_C|| : A = X^*Y\}.$$

*Proof.* Let $A = X^*Y$. Then,

$$\begin{bmatrix} X^*X & X^*Y \\ Y^*X & Y^*Y \end{bmatrix} = \begin{bmatrix} X^* & 0 \\ Y^* & 0 \end{bmatrix} \times \begin{bmatrix} X & Y \\ 0 & 0 \end{bmatrix}$$

is positive. Let $Z \in M_n(\mathbb{C})$ such that $||Z|| \leq 1$. Then, by proposition (4.4.6)

$$\begin{bmatrix} I & Z \\ Z^* & I \end{bmatrix}$$

is positive. Hence, Schur product of above two block matrices is positive that is

$$\begin{bmatrix} (X^*X) \circ I & (X^*Y) \circ Z \\ (X^*Y \circ Z)^* & Y^*Y \circ I \end{bmatrix}$$

is positive . So, by proposition (4.4.7) , $X^*Y \circ Z = (X^*X \circ I)^{1/2} K (Y^*Y \circ I)^{1/2}$ for some contraction $K$. Thus,

$$||A \circ Z|| \leq ||X^*X \circ I||^{1/2} ||Y^*Y \circ I||^{1/2} = ||X||_c ||Y||_c.$$

Therefore,

$$||S_A|| \leq \text{ inf } \{||X_C||||Y_C|| : A = X^*Y.\}$$

□

# Chapter 5

# Positive Linear maps

## 5.1 Introduction

*Chapter 5 deals with the concept of positive linear maps. First few sections include the definition of positive linear maps, basic examples and properties.* ***Kadison's inequality*****, *****Choi's inequality*****, *****Choi's theorem*** *and* ***The Russo-Dye theorem*** *are the main results of this chapter.*

## 5.2 Representation

**Definition 5.2.1.** *A linear map $\Phi : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ is called representation if it satisfy the following properties:*

1. *preserves product that is $\Phi(AB) = \Phi(A)\Phi(B)$ for all $A, B \in M_n(\mathbb{C})$.*
2. *preserves adjoint that is $\Phi(A)^* = \Phi(A^*)$ for all $A \in M_n(\mathbb{C})$.*
3. *preserves the identity that is $\Phi(I) = (I)$.*

### 5.2.1 Examples

1. *Let $U \in M_n(\mathbb{C})$ be such that $UU^* = U^*U = I$. Define a map*

$$\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$$

*by*

$$\Phi(A) = U^*AU, \text{ for all } A \in M_n(\mathbb{C}).$$

*Then, $\Phi$ is a representation on $M_n(\mathbb{C})$*

**Definition 5.2.2.** *Let $A \in B(\mathcal{H})$ then spectral radius of $A$ denoted as $r(A)$ is*

$$r(A) = \sup\{|\lambda| : \lambda \in \sigma(A)\}.$$

*where $\sigma(A)$ denotes the spectrum of $A$.*

**Note 5.2.3.** *Let $A \in \mathcal{B}(\mathcal{H})$ be a self-adjoint operator. Then,*

1. $||A|| = r(A)$.
2. $||A^*A|| = ||A||^2$.
3. $r(\Phi(A)) \leq r(A)$ *where $\Phi$ is a representation.*

### 5.2.2 Properties

1. *Every representation has norm 1.*

   *Proof.* Let $\Phi : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ be a representation.
   Then,

   $$\begin{aligned} ||\Phi(A)||^2 &= ||\Phi(A)^*\Phi(A)|| \\ &= ||\Phi(A^*A) \\ &= r\Phi(A^*A) \\ &\leq r(A^*A) \\ &= ||A^*A|| \\ &= ||A^2|| \end{aligned}$$

   Thus, $||\Phi(A)|| \leq ||A||$ for all $A$. Since, $\Phi(I) = (I)$. It follows that , $||\Phi|| = 1$. □

2. *A representation carries orthogonal projection to orthogonal projection, unitaries to unitaries and it preserves unitary conjugation.*

## 5.3 Positive maps

**Definition 5.3.1.** *A linear map $\Phi : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ is called*

1. *positive if* $\Phi(A) \geq 0$ *for all* $A \geq 0$.
2. *strictly positive if* $\Phi(A) > 0$ *for all* $A > 0$.
3. *unital if* $\Phi(I) = I$.

**Remark 5.3.2.** *A positive linear map is strictly positive if and only if* $\Phi(I) > 0$.

### 5.3.1 Examples

1. *Every projection is positive.*

   *Proof.* Let $P$ be a projection. Then, $P = P^* = P^2$. Then, for all $x \in \mathcal{H}$ we have,
   $\langle Px, x\rangle = \langle P^2x, x\rangle = \langle Px, Px\rangle = ||Px||^2 \geq 0$. □

2. *Let $\Phi : M_n(\mathbb{C}) \to \mathbb{C}$ defined by*
$$\Phi(A) = tr(A)$$
*where $tr(A)$ denotes the trace of the matrix $A$.*

3. *Every representation is positive.*

   *Proof.* Let $\Phi : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ be a representation. Let $A \in M_n(\mathbb{C})$ be positive. Then, $A$ can be written as $A = B^*B$ for some $B \in M_n(\mathbb{C})$. Then,
$$\Phi(A) = \Phi(B^*B) = \Phi(B^*)\Phi(B) = \Phi(B)^*\Phi(B). \tag{5.1}$$
   Hence, by theorem (4.1.3), $\Phi(A)$ is positive. □

4. $\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ *defined by*
$$\Phi(A) = A^{tr}$$
*where $A^{tr}$ denotes the transpose of $A$.*

5. *Let $\Phi : M_n(\mathbb{C}) \to \mathbb{C}$ defined by*
$$\Phi(A) = \sum_{i,j} a_{ij}.$$
   *Proof.* Let $e = (1, 1, ...1) \in \mathbb{C}^n$ Then, $\Phi(A) = \langle e, Ae\rangle$. Since, $A \geq 0$, we have, $\Phi(A) \geq 0$. Hence, $\Phi$ is a positive linear functional. □

6. *Let $X \in M_{n\times k}(\mathbb{C})$. Then, the map $\Phi : M_n(\mathbb{C}) \to \mathbb{C}$ defined by*
$$\Phi(A) = X^*AX, \textit{for all } A \in M_n(\mathbb{C})$$
*is a positive linear map.*

7. *Let $B \in M_n(\mathbb{C})$ be a positive matrix. Then,the map defined by $\Phi : M_n(\mathbb{C}) \to M_{n^2}(\mathbb{C})$ defined by*
$$\Phi(A) = A \otimes B \textit{ for all } A \in M_n(\mathbb{C})$$
*is positive linear map. Hence,the map*
$$\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$$
*defined by*
$$\Phi(A) = A \circ B$$
*is positive.*

8. *we have proved that sum of two positive matrices is positive and space of positive matrices is closed under multiplication by a positive scalar. Hence, any positive linear combination of positive matrices is positive. Any convex combination of positive unital map is positive and unital.*

### 5.3.2 Properties

**Theorem 5.3.3.** *Let $\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ be a positive linear map. Then, $\Phi(A^*) = \Phi(A)^*$.*

**Theorem 5.3.4.** *(Kadison's inequality:) Let $\phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ be a positive and unital map. Then, for every hermitian matrix $A$, we have,*

$$\Phi(A)^2 \leq (\Phi(A^2)).$$

*Proof.* By the Spectral theorem,we have

$$A = \sum_{j=1}^{n} \lambda_j P_j \text{ and } \sum_{j=1}^{n} P_j = I. \tag{5.2}$$

where $\lambda_{j's}$ are eigenvalues of $A$ and $P_{j's}$ are mutually orthogonal projections. Therefore, $A^2 = \sum\limits_{j=1}^{n} \lambda_j^2 P_j$. Hence,
$\Phi(A) = \sum\limits_j \lambda_j \Phi(P_j)$, $\Phi(A^2) = \sum\limits_j \lambda_j^2 \Phi(P_j)$ and $\sum\limits_j \Phi(P_j) = I$.
Note that $\Phi(P_j)$ is positive. Consider,

$$\begin{bmatrix} \Phi(A^2) & \Phi(A) \\ \Phi(A) & I \end{bmatrix} = \begin{bmatrix} \sum\limits_j \lambda_j^2 \Phi(P_j) & \sum\limits_j \lambda_j \Phi(P_j) \\ \sum\limits_j \lambda_j \Phi(P_j) & \sum\limits_j \Phi(P_j) \end{bmatrix}$$

$$= \sum_j \begin{bmatrix} \lambda_j^2 \Phi(P_j) & \lambda_j \Phi(P_j) \\ \lambda_j \Phi(P_j) & \sum\limits_j \Phi(P_j) \end{bmatrix}$$

$$= \sum_j \begin{bmatrix} \lambda_j^2 & \lambda_j \\ \lambda_j & 1 \end{bmatrix} \otimes \Big( \ \Phi(P_j) \ \Big).$$

which is positive. Now, proof follows directly from proposition (4.4.8 ) by taking $X = \Phi(A)$. Hence, $\Phi(A)^2 \leq \Phi(A^2)$.

□

**Theorem 5.3.5.** *Let $\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ be positive and unital linear map. Then, for every normal matrix A. we have,*

$$\Phi(A)\Phi(A^*) \leq \Phi(A^*A) \quad \textit{and} \quad \Phi(A^*)\Phi(A) \leq \Phi(A^*A).$$

*Proof.* The proof follows in the similar lines of the proof of previous theorem. From equation 5.2, we have ,

$$A^* = \sum_{j=1}^{n} \bar{\lambda_j} P_j$$

and

$$A^*A = \sum_{j=1}^{n} \lambda_j^2 P_j, \quad \sum P_j = I.$$

Consider,

$$\begin{bmatrix} \Phi(A^2) & \Phi(A) \\ \Phi(A) & I \end{bmatrix} = \sum_{j=1}^{n} \begin{bmatrix} |\lambda_j|^2 & \lambda_j \\ \lambda_j & 1 \end{bmatrix} \otimes \left( \ \Phi(P_j) \ \right).$$

The above matrix is positive and rest of the proof directly follows by taking $X = \Phi(A)$ in theorem (4.4.8). Hence, $\Phi(A)\Phi(A^*) \leq \Phi(A^*A)$. □

**Remark 5.3.6.** *1. A positive linear map carries hermitian matrices to hermitian matrices and unitaries to contractions.*

*2. If A is normal, then $\Phi(A)$ need not be normal.*

**Example 5.3.7.** *Let $\Phi : M_2(\mathbb{C}) \to M_2(\mathbb{C})$ be defined by*

$$\Phi \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & b \\ c & a \end{bmatrix}$$

*where $a, b, c, d \in \mathbb{C}$.*

*Clearly, $\Phi$ is positive. Let*

$$A = \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix}$$

*Here, A is normal. But $\Phi(A)$ is not normal.*

**Theorem 5.3.8.** *Let $\Phi$ be strictly positive and unital. Then, for every strictly positive matrix A, we have*

$$\Phi(A)^{-1} \leq \phi(A^{-1}).$$

*Proof.* Proof follows by theorem (5.3.4). □

**Theorem 5.3.9.** *(The Russo- Dye Theorem:) If $\Phi$ is positive and unital,then $||\Phi|| = 1$.*

**Corollary 5.3.3.** *Let $\Phi$ be a positive linear map.Then, $||\Phi|| = ||\Phi(I)||$.*

*In the next section, we ask three questions regarding positive linear maps. They are:*

1. *corollary (5.3.3) of The Russo-Dye theorem says that every positive linear map attains its norm at identity. Is the converse true, that is if a Linear map attains its norm at identity, then must it be positive?*

2. *We restrict the linear map on a subspace of $M_n(\mathbb{C})$. Then, do we still have the theorem like Russo-Dye theorem?*

3. *By Hahn- Banach theorem, we can say that every linear functional on a linear subspace of $M_n(\mathbb{C})$ can be extended to a linear functional on $M_n(\mathbb{C})$. So, we may ask the similar question that whether a positive linear functional on an operator system $\mathcal{S}$ of $M_n(\mathbb{C})$ can be extended to a positive linear functional on $M_n(\mathbb{C})$ ?*

*In answer to question 1, we present some examples of linear maps which attain their norm at identity but they are not positive. We present a result which says that the converse of* ***The Russo-Dye theorem*** *is true for every linear functional.*

**Definition 5.3.10.** *A linear subspace $\mathcal{S}$ of $M_n(\mathbb{C})$ is called an operator system if it is closed under the operation $^*$ and it contains identity $I$.*

**Example 5.3.11.** *1. The space of all symmetric matrices*

2. *space of all skew-symmetric matrices and*

3. *space of all diagonal matrices are operator system of $M_n(\mathbb{C})$.*

**Note 5.3.12.** *1. Let $T : \mathcal{H} \to \mathcal{H}$ be a linear operator. Then $T$ can be written as $T = A + iB$ where $A$ and $B$ are self adjoint operators. This is called the cartesian decomposition of $T$.*

2. *Every hermitian matrix $A$ on an operator system can be written as difference of two positive definite matrices.*

**Lemma 5.3.13.** *Let $\mathcal{S}$ be an operator system of $M_n(\mathbb{C})$ and*

$$\Phi : \mathcal{S} \to M_k(\mathbb{C})$$

*be a positive linear map. Then, $\Phi(A^*) = (\Phi(A))^*$.*

**Theorem 5.3.14.** *Let $\Phi : \mathcal{S} \to M_k(\mathbb{C})$ be a positive linear map. Then,*

1. $||\Phi(A)|| \leq ||\Phi(I)||.||A||$ *for all* $A \in \mathcal{S}_{s.a}$ *where $\mathcal{S}_{s.a}$ is the space of all self-adjoint operators on $\mathcal{S}$.*

2. $||\phi(T)|| \leq 2||\Phi(I)||||T||$ *for all* $T \in \mathcal{S}$.

   *Moreover, If $\Phi$ is unital then,*

$||\Phi(A)|| \leq ||A||$ *for all $A \in \mathcal{S}_{s.a}$. and* $||\phi(T)|| \leq 2||T||$ *for all $T \in \mathcal{S}$.*

*Proof.* Note that if $P \in \mathcal{S}$ be positive. Then, $0 \leq P \leq ||P||I$ that is $||P||I - P \geq 0$.
Let $A$ be a hermitian matrix. Then, $A = P_+ - P_-$ where $P_+$ and $P_- \geq 0$.

Since, $||A|| \leq max\{||P_+||, ||P_-||\}$, we have,

$$\begin{aligned} ||\Phi(A)|| &\leq max\{||\Phi(P_+)||, ||\Phi(P_-)||\} \\ &= max\{||P_+||, ||P_-||\}||\Phi(I)||. \end{aligned}$$

Second part can be proved by using the Cartesian decomposition of $A$ and then part(I). □

**Theorem 5.3.15.** *Let $\phi$ be a positive linear functional on operator system $\mathcal{S}$. Then, $||\phi|| = ||\phi(I)||$.*

**Theorem 5.3.16.** *Let $\phi$ be a linear functional on operator system $\mathcal{S}$ such that $||\phi|| = \phi(I)$. Then, $\phi$ is positive.*

**Theorem 5.3.17.** *(The Krein extension Theorem:) Let $S$ be an operator system in $M_n(\mathbb{C})$. Then, every positive linear functional on $S$ can be extended to a positive linear functional on $M_n(\mathbb{C})$.*

**Theorem 5.3.18.** *Let $\Phi : \mathcal{S} \to M_k(\mathbb{C})$ be a unital linear map such that $||\Phi|| = 1$. Then, $\Phi$ is positive.*

# Chapter 6

# Completely Positive maps

## 6.1 Introduction

*Chapter 6 deals with the study of completely positive maps which are particular class of positive linear maps. We start with the definition and examples of completely positive maps.* ***Choi's Theorem the Stinespring dilation theorem*** *are the main results of this thesis. They give a characterization of all completely positive maps in various settings.*

**Definition 6.1.1.** *Let $M_m(M_n)$ be the space of all $m \times m$ block matrices $[[A_{ij}]]$ whose $(i,j)$ entry is an element of $M_n(\mathbb{C})$. Every linear map $\Phi : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ includes a linear map $\Phi_m : M_m(M_n(\mathbb{C})) \to M_m(M_k(\mathbb{C}))$ defined as*

$$\Phi_m[[A_{ij}]] = [[\Phi(A_{ij})]] \ , \ [[A_{ij}]] \in M_m(M_n(\mathbb{C})).$$

*we say that the map $\Phi$ is*

1. *m-positive if $\Phi_m$ is positive.*
2. *completely positive if $\Phi_m$ is positive for all $m \in \mathbb{N}$.*

**Example 6.1.2.** 1. *Every representation is completely positive.*

*Proof.* Let $\Phi : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ be a representation. Consider, $\Phi_m : M_m(M_n(\mathbb{C})) \to M_m(M_k(\mathbb{C}))$ defined as

$$\Phi_m[[A_{ij}]] = [[\Phi(A_{ij})]].$$

We will prove that $\Phi_m$ is positive. Since,$\Phi_m$ is unital and has norm 1. Hence, $\Phi_m$ is positive. Therefore, $\Phi$ is completely positive. □

2. *Let $V \in \mathbb{C}^{n\times k}$ and $\Phi : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ be defined by*

$$\Phi(A) = V^*AV \ \ , A \ \in M_n(\mathbb{C}).$$

*Then, $\Phi$ is completely positive.*

*Proof.* We will prove that $\Phi_m : M_m(M_n(\mathbb{C})) \to M_m(M_k(\mathbb{C}))$ defined by

$$\Phi_m[[A_{ij}]] = [[\Phi(A_{ij})]] = [[V^*A_{ij}V]] \geq 0.$$

It is enough to prove that

$$\langle [[\Phi(A_{ij})]]x_j, x_i\rangle \geq 0 \ \text{ for all } \ x_i \in \mathbb{C}^k.$$

Consider,

$$\begin{aligned}\langle [[\Phi(A_{ij})]]x_j, x_i\rangle &= \langle [[V^*(A_{ij})V]]x_j, x_i\rangle \\ &= \langle A_{ij}(V(x_j), (V(x_i))\rangle \geq 0.\end{aligned}$$

□

**Theorem 6.1.3.** *Let $\Phi : M_n(\mathbb{C}) \to M_m(\mathbb{C})$ be a linear map. Then, $\Phi$ is completely positive if and only if $\Phi$ is of the form $\Phi(A) = \sum_i V_i^* AV_i$ for all $A \in M_n(\mathbb{C})$ and $V_i \in M_{n\times m}(\mathbb{C})$.*

*In next section, we will consider linear maps whose domain is the linear subspace $\mathcal{S}$ of $M_n(\mathbb{C})$ and whose range is $M_k(\mathbb{C})$. we will give a bijective correspondence between $\mathcal{L}(M_k(\mathcal{S}), \mathbb{C})$ and $\mathcal{L}(\mathcal{S}, M_k(\mathbb{C}))$. We will establish this correspondence now.*

*Let $\Phi : \mathcal{S} \to M_k(\mathbb{C})$ is given. Then, define $\phi : M_k(\mathcal{S}) \to \mathbb{C}$ by*

$$\phi[[S_{ij}]] = \frac{1}{k}\sum_{i,j=1}^{k} [\Phi(S_{ij})]_{i,j}, \ \ S_{ij} \in \mathcal{S}. \tag{6.1}$$

*where $[A]_{i,j}$ denotes the $(i, j)$th entry of the matrix $A$.*

*Conversely, Let $\phi : M_k(\mathcal{S}) \to \mathbb{C}$ be given. Then, define $\Phi : \mathcal{S} \to M_k(\mathbb{C})$ by*

$$[\Phi(A)]_{i,j} = k\phi(E_{ij} \otimes A) \tag{6.2}$$

*where $E_{ij}, 1 \leq i, j \leq k$ are unit matrices in $M_k(C)$.*

**Theorem 6.1.4.** *Let $\mathcal{S}$ be an operator system in $M_n(\mathbb{C})$ and $\Phi : \mathcal{S} \to M_k(\mathbb{C})$ be a linear map. Then,the following conditions are equivalent:*

1. *$\Phi$ is completely positive.*

2. *$\Phi$ is k-positive.*

3. *the functional $\phi$ defined in (6.1) is positive.*

*Proof.* (1.) $\Rightarrow$ (2.) is clear. Since, a completely positive map is $m$-positive for all $m \in \mathbb{N}$.
(2.) $\Rightarrow$ (3.) Let $\{e_j : 1 \leq j \leq k\}$ be a basis for $\mathbb{C}^k$. Consider a vector $x = e_1 \oplus e_2 \oplus ...e_k \in \mathbb{C}^{k^2}$. Then,

$$\phi[[S_{ij}]] = \frac{1}{k}\sum_{i,j=1}^{k}[\Phi(S_{ij})]_{i,j} \tag{6.3}$$

$$= \frac{1}{k}\sum_{i,j=1}^{k}\langle e_i, [[\Phi(S_{ij})]]e_j\rangle \tag{6.4}$$

$$= \frac{1}{k}\langle x, [[\Phi(S_{ij})]]x\rangle \tag{6.5}$$

we will prove that $\phi : M_k(\mathcal{S}) \to \mathbb{C}$ is positive. Let $(S_{ij})$ be a positive element of $M_k(\mathcal{S})$ where $(S_{ij}) \in M_n(C)\ \forall\ 1 \leq i, j \leq k$. Then, It is clear from equation (6.3) that $\phi$ is positive.

(3.) $\Rightarrow$ (1.) Assume that the functional $\phi$ is positive. We will prove that the linear map $\Phi$ is completely positive. Since $\mathcal{S}$ is an operator system of $M_n(\mathbb{C})$. So, $M_k(\mathbb{S})$ is an operator system of $M_k(M_n\mathbb{C})$. Since $\phi : M_k(\mathcal{S}) \to \mathbb{C}$ be a linear functional. By The Krein Extension Theorem, $\phi$ can be extended to the entire space $M_k(M_n(\mathbb{C})$. Let $\tilde{\phi} : M_k(M_n(C)) \to (\mathbb{C})$ be the extended linear functional. Then, there exists a linear map $\tilde{\Phi} : M_n(\mathbb{C}) \to M_k(\mathbb{C})$. Clearly, $\tilde{\Phi}$ is an extension of $\Phi$. It is enough to prove that $\tilde{\Phi}$ is completely positive. Let $m$ be a positive integer. Consider,

$$\tilde{\Phi}_m : M_m(M_n(\mathbb{C})) \to M_m(M_k(\mathbb{C}))$$

. We will prove that $\tilde{\Phi}_m$ is positive. Every positive element of $M_m(M_n(\mathbb{C}))$ can be written as sum of matrices $[[A_i^*A_j]]$ where $A_j,\ 1 \leq j \leq m$ are elements of $M_n(\mathbb{C})$. It is enough to prove that $[[\tilde{\Phi}(A_i^*A_j)]] \in M_{mk}(\mathbb{C})$ is positive. Let $x \in \mathbb{C}^{mk\cdot}$. Then, $x$ can be written as $x = x_1 \oplus x_2 \oplus ...x_m$, $x_j \in \mathbb{C}^k$ and $x_j = \sum_{p=1}^{k}\psi_{jp}e_p$. Consider,

$$\langle x, [[\tilde{\Phi}(A_i^*A_j)]]x\rangle = \sum_{i,j=1}^{m} \tag{6.6}$$

$$= \langle x_i, \tilde{\Phi}(A_i^*A_j)x_j\rangle \tag{6.7}$$

$$= \sum_{i,j=1}^{m}\sum_{p,q=1}^{k}\bar{\psi_{ip}}\psi_{jq}k\tilde{\phi}(E_{pq} \otimes A_i^*A_j) \quad \text{(By Equation (6.2).)} \tag{6.8}$$

For $1 \leq i \leq m$, let $X_i \in M_k(\mathbb{C})$ such that

$$\begin{bmatrix} \psi_{i1} & \psi_{i2} & \dots & \psi_{ik} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}$$

Then

$$[X_i^* X_j]_{pq} = \bar{\psi_{ip}} \psi_{jq} \tag{6.9}$$

$$= \sum_{p,q=1}^{k} \bar{\psi_{ip}} \psi_{jq} E_{pq}. \tag{6.10}$$

So, equation (6.6) can be written as

$$\langle x, [[\tilde{\Phi}(A_i^* A_j)]]x\rangle = k \sum_{i,j=1}^{m} \tilde{\Phi}(X_i^* X_j \otimes A_i^* A_j)$$

$$= k\tilde{\Phi}\Big(\Big(\sum_{i=1}^{m} X_i \otimes A_i\Big)^* \Big(\Big(\sum_{i=1}^{m} X_i \otimes A_i\Big)\Big) \geq 0. \text{ Since } \tilde{\phi} \text{ is positive.}$$

Hence, $\Phi$ is positive.

□

## 6.2 Banach algebra

**Definition 6.2.1.** *Let $\mathcal{A}$ be a nonempty set then $\mathcal{A}$ is called an algebra if*

1. $(\mathcal{A}, +, .)$ *is a vector space over* $\mathbb{F}$.
2. $(\mathcal{A}, +, \circ)$ *is a ring.*
3. $(\alpha a) \circ b = \alpha(a \circ b) = a \circ (\alpha b)$. *for all* $\alpha \in \mathbb{F}$ *and* $a, b \in \mathcal{A}$

**Definition 6.2.2.** *An algebra $\mathcal{A}$ is said to be:*

1. *real or complex according to the field* $\mathbb{F} = \mathbb{R}$ *or* $\mathbb{F} = \mathbb{C}$ *respectively.*
2. *Commutative if* $(\mathcal{A}, +, \circ)$ *is commutative.*
3. *unital if* $(\mathcal{A}, +, \circ)$ *has a unit.*

**Definition 6.2.3.** *If $\mathcal{A}$ is an algebra and $||.||$ is a norm on $\mathcal{A}$ satisfying $||ab|| \leq ||a||.||b||$ for all $a, b \in \mathcal{A}$. Then, $(\mathcal{A}, ||.||)$ is called a normed algebra. A complete normed algebra is called Banach algebra.*

**Definition 6.2.4.** *Let $\mathcal{A}$ be a complex algebra. A map $a \mapsto a^*$ is called an involution map on $\mathcal{A}$ if it satisfies:*

1. $(a^*)^* = a$.
2. $(ab)^* = b^* a^*$.
3. $(\alpha a + \beta b)^* = \bar{\alpha} a + \bar{\beta} b \; \forall a, b \in \mathcal{A}$ *and* $\alpha, \beta \in \mathbb{C}$.

**Definition 6.2.5.** *A $C^*-$ algebra is a Banach algebra with an involution map $^*$ satisfying $||a^* a|| = ||a||^2$ for all $a \in \mathcal{A}$.*

**Definition 6.2.6.** *Let $\mathcal{A}$ be an algebra and $\mathcal{B} \subseteq \mathcal{A}$ then $\mathcal{B}$ is called a sub-algebra of $\mathcal{A}$ if $\mathcal{B}$ itself is an algebra with respect to operations of $\mathcal{A}$.*

**Example 6.2.7.** *1. Let $\mathcal{A} = \mathbb{C}$. Then, with respect to usual addition and multiplication and the modulus $\mathcal{A}$ is a commutative, unital Banach algebra.*

2. *Let $K$ be a compact hausdroff space and $\mathcal{A} = C(K)$ then with respect to point wise multiplication of functions, $\mathcal{A}$ is a commutative, unital algebra and with the norm $||f||_\infty = Sup_{t\in K}|f(t)|$ is a Banach algebra and with the involution map $f^*(x) = f(\bar{x})$, it is a $C^*-$ algebra.*

3. *Let $\mathcal{H}$ be a Hilbert space then $\mathcal{B}(\mathcal{H})$ is a $C^*-$ algebra with its usual operator norm and involution map is $T \mapsto T^*$.*

**The Gelfand Naimark Theorem 6.2.8.** *For every $C^*-$ algebra $\mathcal{A}$ there exists a Hilbert space $\mathcal{H}$ such that $\mathcal{A}$ is $C^*-$ isomorphic to a $C^*-$ subalgebra of $\mathcal{B}(\mathcal{H})$.*

**Stinespring Dilation theorem 6.2.9.** *Let $\mathcal{A}$ be a $C^*-$ algebra with a unit and $H$ be a Hilbert space. Let $\Phi : \mathcal{A} \to B(H)$ be a linear function.Then, a necessary and sufficient condition that $\Phi$ have the form*

$$\Phi(A) = V^*\pi(A)V \quad for\ all\ A \in \mathcal{A}.$$

*where $V : \mathcal{H} \to K$ be a bounded operator and $\pi : \mathcal{A} \to B(K)$ is a *- representation, is that $\Phi$ be completely positive.*

*Before discussing the proof of above theorem, we will recall some results that are needed to understand the proof completely.*

**Lemma 6.2.10.**

*(Cauchy Schwartz inequality:) Let $K$ be a sub field of $\mathbb{C}$ and $V$ be a semi inner product space over $K$.Then,*

$$|\langle x, y\rangle|^2 \leq \langle x, x\rangle.\langle y, y\rangle \ \ for \ \ all\ x, y \in V.$$

**Lemma 6.2.11.** *Let $\mathcal{A}$ be a $C^*$-algebra. Then, $a^*b^*ba \leq ||b||^2a^*a$ for all $a, b, c \in \mathcal{A}$.*

*Proof.* It is enough to show that

$$a^*||b||^2a - a^*b^*ba = a^*(||b||^2 - b^*b)a \geq 0.$$

We will use Gelfand Naimark Theorem, If $\mathcal{A}$ is a unital $C^*$ -algebra. Then, $\mathcal{A}$ is isometrically $^*-$ isomorphic to a concrete $C^*-$ algebra, that is $\mathcal{A}$ can be embedded in $\mathcal{B}(H)$ for some Hilbert space $\mathcal{H}$.
We know that if $T \in B(H)$. Then, $T^*T \leq ||T||^2I$.
Now, theorem follows directly from above result.

□

*Now, we are all set to give a proof of Stinespring Dilation theorem.*

*Proof.* Suppose that $\phi$ is a completely positive map. We need to show the existence of a Hilbert space $K$, a unital $^*-$ isomorphism $\pi : \mathcal{A} \to B(\mathcal{K})$ and a linear operator $V : \mathcal{H} \to \mathcal{K}$ such that

$$\Phi(A) = V^*\pi(A)V \quad for\ all\ A \in \mathcal{A}.$$

Consider the vector space $\mathcal{A} \otimes \mathcal{H}$, the algebraic tensor product of $\mathcal{A}$ and $\mathcal{H}$. For, $\xi = \sum\limits_i a_i \otimes x_i$ and $\eta = \sum\limits_i b_i \otimes y_i$ in $\mathcal{A} \otimes \mathcal{H}$ define a sesquilinear map $[.,.]$ on $\mathcal{A} \otimes \mathcal{H}$ by

$$[\xi, \eta] = \sum_i \langle \Phi(b_i^* a_i) x_i, y_i \rangle \tag{6.11}$$

Since, $\Phi$ is assumed to be completely positive. It follows that

$$\langle \xi, \xi \rangle = \sum_{i,j} \langle \Phi(A_j^* A_i) x_i, x_j \rangle \geq 0.$$

Hence, [.,.] is positive semi definite and positive semi definite form satisfy the Cauchy schwarz inequality. Define,

$$\mathcal{N} := \{u \in \mathcal{A} \otimes \mathcal{H} : [u, u] = 0\}.$$

By the Cauchy-schwarz inequality, we can show that

$$\mathcal{N} = \{u \in \mathcal{A} \otimes \mathcal{H} : [u, v] = 0 \text{ for all } v \in \mathcal{A} \otimes \mathcal{H}\}.$$

$\mathcal{N}$ is a subspace of semi inner product space $\mathcal{A} \otimes \mathcal{H}$. Define a map on quotient space $\mathcal{A} \otimes \mathcal{H}/\mathcal{N}$ by $\langle u + \mathcal{N}, v + \mathcal{N} \rangle = [u, v]$.
Then, [.,.] is an inner product on quotient space $\mathcal{A} \otimes \mathcal{H}/\mathcal{N}$. Let $\mathcal{K}$ be the completion of this space to Hilbert space. For any element $a$ in $\mathcal{A}$, define

$$\pi(a) : \mathcal{A} \otimes \mathcal{H} \to \mathcal{A} \otimes \mathcal{H}$$

by

$$\pi(a)\bigg(\sum_{i=1}^{l} a_i \otimes x_i\bigg) = \sum_{i=1}^{l} (a a_i) \otimes x_i.$$

Clearly, $\pi$ is linear and it satisfies the following inequality,

$$[\pi(a)u, \pi(a)u] \leq ||a||^2 [u, u]. \tag{6.12}$$

Observe that,

$$\begin{aligned} \left[\pi(a)\bigg(\sum_j a_j \otimes x_j\bigg), \pi(a)\left(\sum_i a_i \otimes x_i\right)\right] &= \sum_{i,j} \langle \Phi(a_i^* a^* a a_j) x_j, x_i \rangle \\ &\leq ||a||^2 \sum_{i,j} \langle \Phi(a_i^* a_j) x_j, x_i \rangle \\ &\leq ||a||^2 \left[\bigg(\sum_j A_j \otimes x_j\bigg), \bigg(\sum_i a_i \otimes x_i\bigg)\right]. \end{aligned}$$

It follows from inequality (6.12) that null space of $\Pi(a)$ contains $\mathcal{N}$. Hence, $\Pi(a)$ can be viewed as a linear operator on $\mathcal{A} \otimes \mathcal{H}/\mathcal{N}$, and we denote it by $\pi(a)$ again.
Inequality (6.12) shows that $\Pi(a)$ is a bounded linear operator on $\mathcal{K}$. Therefore, it extends a bounded linear operator on $\mathcal{K}$. We will denote it by $\pi(a)$.

Define a map, $\pi : \mathcal{A} \to B(\mathcal{K})$ by

$$a \mapsto \pi(a), \text{ for } \text{ all } a \in \mathcal{A}.$$

Then, $\pi$ is a unital $^*-$ homomorphism.

Define, $V : \mathcal{H} \to \mathcal{K}$ by $V(x) = 1 \otimes x + \mathcal{N}$.
Clearly, $V$ is linear. we have , for all $x \in \mathcal{H}$,

$$\begin{aligned} ||Vx||^2 &= \langle 1 \otimes x + \mathcal{N}, 1 \otimes x + \mathcal{N} \rangle \\ &= [1 \otimes x, 1 \otimes x] \\ &= \langle \Phi(1)x, x \rangle \\ &= \langle \Phi(1)^{1/2}x, \Phi(1)^{1/2}x \rangle \\ &= ||\Phi(1)^{1/2}x||^2. \end{aligned}$$

Hence, $||V||^2 = ||\Phi(1)^{1/2}||^2 = ||\Phi(1)||$. We need to show that $V^*\pi(a)V = \Phi(a)$.
For all $x, y \in \mathcal{H}$, we have

$$\begin{aligned} \langle V^*\pi(a)Vx, y \rangle_{\mathcal{H}} &= \langle \pi(a) 1 \otimes x, 1 \otimes y \rangle_{\mathcal{K}} \\ &= \langle \pi(a)x, y \rangle_{\mathcal{H}} \, for \ all \ x, y \in \mathcal{H}. \end{aligned}$$

Hence, $V^*\pi(A)V = \Phi(A.)$
Conversely, assume that $\Phi(A) = V^*\pi(A)V$. We will prove that $\Phi$ is completely positive.
It is enough to prove that,

$$\begin{aligned} \sum_{i,j} \langle \Phi_n[[(A_{ij})]]x_i, x_j \rangle &= \sum_{i,j} \langle [[\Phi(A_{ij})]]x_i, x_j \rangle \\ &= \sum_{i,j} \langle V^*\pi(A_{ij})Vx_i, x_j \rangle \\ &= \sum_{i,j} \langle \pi(A_{ij})(Vx_i), (Vx_j) \rangle \geq 0 \text{ for } \text{ all} x_i \in \mathcal{H}. \end{aligned}$$

Since $\pi$ is a $^{*-}$ and every representation is completely positive. Hence, above assertion follows directly.
Therefore, $\Phi$ is completely positive. □

# References

[1] *Nielsen and Chuang(2000), Quantum computation and Quantum information, Cape town,South Africa, Cambridge University press.*

[2] *Vern Paulsen, Brandon Lee (2011), Lectures on Quantum computing and completely positive maps, Department of Mathematics, University of Houston.*

[3] *Bhatia, Rajendra (2007), Positive Definite Matrices, Princeton University Press, 3 Market Place, Woodstock, Oxfordshire OX20 1SY.*

[4] *Fuzhen Zhang (1999), Matrix Theory, Springer Sciences and Business Media.*

[5] *W. Forrest Stinespring (1995), Positive Functions on C*-algebras, American Mathematical Society.*

[6] *Man-Duen Choi, Completely Positive linear maps on complex matrices, Department of Mathematics, University of California, Berkeley, California 94720.*