ABSTRACT

YANG, MIN. Local Unitary Equivalence In Quantum Computation . (Under the direction of Naihuan Jing.)

Determining the local unitary equivalence in quantum systems plays an important role in distinguishing quantum states with different level of entanglement. In this dissertation, this problem is studied through several approaches involving matrix foldings and Gel-Mann basis etc. We find a special normal form for two partite mixed states and provide a new method to solve general local unitary problems based on matrix foldings.

Local Unitary Equivalence In Quantum Computation

by
Min Yang

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Mathematics

Raleigh, North Carolina

2014

APPROVED BY:

Ernest Stitzinger	Kailash Misra
Kimberly Weems	Naihuan Jing Chair of Advisory Committee

DEDICATION

To my parents and my advisor. Your support is my strength.

BIOGRAPHY

Min Yang was born in February 1985 in Wuhan, P.R. China, where he enjoyed all his childhood and finished all his nine years compulsory education and high school. In the same city, Huazhong University of Science and Technology accepted him to study towards his bachelor's degree in optical information science and technology department in 2003. He got B.S. in 2007 co-majored in computer science. After this, he was accepted by another national key university, Wuhan University, to study for his master's degree in the physics department in the same year.

In 2009, he was granted the degree, finished all his study in China and got the chance to study in North Carolina State University with financial support. He was expected to graduate with a Ph. D. degree in mathematics in July 2014.

ACKNOWLEDGEMENTS

My sincerest thanks goes to my advisor, Dr. Jing for his guidance, encourage, and continuos support though out all my graduate studies. I can not forget all the moments that he spend teaching me the latest knowledge in my study area, solving my problems encountered in the study, and giving advices on my research directions. I would not think of going into quantum information theory which best matches my knowledge structure without his help.

I also want to thank all my committee members, Dr. Naihuan Jing, Dr. Kailash Misra, Dr. Ernest Stitzinger, and Dr. Kim Weems, they are always there when I need help in all the processes working out this dissertation.

At last, I want to thank my parents. I can feel their love and support even if they are at the other side of the earth.

TABLE OF CONTENTS

Chapter 1

Introduction

Entanglement is one of the important phenomena in quantum information and computation theory. The problem on how to determine and classify the level of entanglement in each quantum state can be formulated as a mathematical problem. In this thesis, we develop new techniques to determine the local unitary equivalence of quantum states.

1.1 Quantum information and computation theory

Information theory is a study on the qualification of information in all applicable areas, say applied mathematics and engineering. It is well known as the fundamental theory for classic computer [1]. The fundamental results of classical information theory are Shannon's noiseless channel coding theorem and Shannon's noisy channel coding theorem, which give the limit for information storage and communication in classic computer [2]. Quantum mechanics, as one of the most amazing discoveries in modern science, has affect all the aspects of the microscopic world, which include the devices related to the storage, encryption, and teleportation of classic information and thus starts a new chapter for the information theory.

Specifically, the theory of quantum information is a result of the effort to generalize classical information theory to the quantum world.

1.1.1 Quantum mechanics

What is quantum mechanics? Quantum mechanics is the most accurate and complete description of the physical world, and it is the theoretic basis for quantum information and quantum computation [1]. In the early twentieth century, it is discovered that any object has both particle-like and wave-like behaviors, which is shown in the Photoelectric Effect experiment by Albert Einstein [3] and in matter wave experiment by de Broglie [4].

This phenomenon was not well-known in the classic world before, as the wave-like behavior of objects in the macro scale world were so subtle that one would not even notice. However, as the structure of atoms and the technique of electronic device miniaturization had drawn people's attention, more and more objects in nanoscale were analyzed in the laboratory, like laser, atom, electron, micro semiconductor [5]. These discoveries and technological inventions operate at a scale where quantum effects are significant. It was realized that we could no longer treat these objects as pure matter following the common sense, as the wave-like effect was no longer negligible in this magnitude.

The central idea of quantum mechanics is to set up an energy equation from both particle aspect and wave aspect for any object, then an object would be totally described in this differential equation, the Schrödinger's equation. The physical nature of wave-matter duality effort is not intuitive and hard to explain. Fortunately, quantum mechanics provides a mathematical and conceptual framework for the laws that a quantum system must obey. With the development of linear algebra and the effort of Born and Heisenberg, we could set up a matrix representation of this differential equation and consider these physical observations in the equations as linear operators, therefore the quantum state, the solution of this differential equation, would be a linear vector. We can use mathematical tools to analyze and compute quantum information.

1.1.2 Quantum effects in information theory

Following the technology development of twentieth century, the size of all kinds of laboratory facilities and electronic devices becomes smaller and smaller. It gradually enters the domain of quantum mechanics, which impedes the development of classic information technology.

Quantum effort becomes the dominant factor when it goes into very small size, say less than 10 nanometre. Like the semiconductor industry, which is the critical part of classic computer industry and developing speedily in the last fifty years according to the Moore's law, it had to eventually face this technical challenge; While, on the other hand, quantum computers [6] are expected to offer substantial speed-ups over their classical counterparts and to solve problems intractable for classical computers [7]. Besides, there are a lot of other discoveries and applications based on this important theory, for instance, instantaneous communication, teleportation, quantum cryptography [8], et al.

Different from classic information theory, quantum information theory is the study of the information processing tasks that can be accomplished through quantum mechanical systems. It is a result of the effort to generalize classical information theory to the quantum world. For example, classic information technology are based on classic information and computation with basic unit, bit, which is implemented by semiconductors. Quantum information on the other hand are built upon an analogue concept, quantum bits, also known as qubits, which can be implemented by quantum units with smaller size like quantum dots.

Unlike bit, whose status is either "0" or "1", the corresponding qubit could be in infinite many middle statuses inclusively between "0" and "1". Such statuses would be described as a linear combination of state "0" and "1", often called superposition. These properties allow a quantum system to carry more information in a single unit and more difficult to be detected for teleportation or preservation purpose.

1.2 Quantum entanglement

Quantum entanglement is the most extraordinary phenomenon in quantum mechanics compared with the classic physics occurrences.

This concept was in a weird sense in physics that they could not be accepted at the early stage when it was discovered. In 1935, Albert Einstein, Boris Podolsky and Nathan Rosen (collectively "EPR") posted the famous paradox about quantum entanglement in their paper [1]. During the same year, Schrödinger, the founder of the wave equation, also posted the cat paradox to fight against this nonclassic and unrealistic phenomenon.

The turnover took place in 1964's, Bell first demonstrated and distinct quantum mechanics from the classic physics world based on an experiment analog to the "EPR" paper, and the fellow results from other physicists also fitted perfectly with the quantum mechanics theory. Therefore, the entanglement of quantum states, known as the unique feature of this theory, was gradually accepted and became well-known. Nowadays, there are plenty of practical applications like quantum computing, quantum cryptography, quantum teleportation , which are impossible in the classic world, are based on this phenomenon.

Thus, having a better understanding of the entanglement of quantum states would help us to utilize quantum information in a more efficient way.

A lot of effort has already been put in this direction. Based on a series of Bell inequalities, some important criterions has been posted to determine the entanglement of quantum states. In 1997, Asher Peres and Michal Horodecki gave the first necessary condition to determine if a joint system of two sub systems is separable, which is known as partial positive transpose criterion(short for PPT) [9]. And in 1999, Michal Horodecki found out another important necessary condition for a mixed state to be separable, which is known as the reduction criterion [10, 11]. This is the first approach to deal with the quantum entanglement problems and a lot of following research has been done based on these important results.

So far, it is still a difficult task to determine the level of entanglement of quantum states, or equivalently speaking, it can not be easily determined if two quantum states could be transformed into each other using a series of quantum gates in practice. Classifying the local unitary(LU) equivalences of quantum states is a very important approach to deal with such problems and is chosen as the main topic in this thesis.

1.3 Outlines of the thesis

In this thesis, a lot of discussions and explorations have been carried out and some useful algorithms have been deducted on the topic of determining the local unitary equivalence of quantum states.

Our thesis is structured in the following way: in the second chapter, we introduce the basic techniques and notations in linear algebra that will be commonly applied in this thesis; and in the third chapter, the mathematical framework of quantum mechanics would be setup and all the problems will be translated into matrix forms for further discussion. In the last two chapters, we first analyze general local unitary problems based on the idea of matrix foldings for pure states, and discussed how to pass the criteria from pure states to mixed states. Then we provide a special normal form based on the Gel-Mann basis and give a series of invariant polynomials based on this normal form to help solving LU equivalence problems in two partite mixed states.

Chapter 2

Linear algebra

In this chapter, we will go through some concepts and notations that would be applied in this thesis. These definitions are very important and commonly used, when we analyze quantum mechanics theory and quantum information in mathematics perspective.

2.1 Hilbert Space

A Hilbert space is both an inner product space and a complete metric space, which ensures the concept of distance and angle. In physics, it is analogue to the real world, and is used as the basic space for any physics state, like quantum states.

2.1.1 Vector spaces

A vector space over some field $\mathcal{F}$, commonly denoted as $\mathcal{V}$, is a set of elements, known as vectors, that are closed under addition and scalar multiplcation. The ten axioms that a vector space must follow are introduced in [12]. For any subspace $\mathcal{W}$ of a vector space $\mathcal{V}$, we can always decompose the vector space $\mathcal{V}$ into a direct sum of these two subspaces, $\mathcal{V} = \mathcal{W} \oplus \mathcal{W}^{\perp}$, such that $\mathcal{W} \cap \mathcal{W}^{\perp} = \emptyset$, it is known that any vector $\mathbf{v}$ in the vector space $\mathcal{V}$ can also be decomposed as $\mathbf{v} = x + y$, such that $x \in \mathcal{W}, y \in \mathcal{W}^{\perp}$.

The typical vector space that is used in our thesis is $\mathbb{C}^n$, it is the space of all n-tuples of complex numbers. In quantum mechanics, $|\psi\rangle$, the bra ket notation, is used as the standard notation to describe a vector in some vector space.

2.1.2 Inner product

Definition 2.1. Inner product is a binary operation, $\langle .,. \rangle$, defined in a vector space $\mathcal{V}$ over the field $\mathcal{F}$:

$$\langle .,. \rangle : V \times V \rightarrow F$$

that satisfies the following three axioms for any vectors $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{V}$, $\alpha \in \mathcal{F}$:

1. Conjugate symmetry: $\langle \mathbf{x}, \mathbf{y} \rangle = \overline{\langle \mathbf{y}, \mathbf{x} \rangle}$.

2. Linearity in the first argument: $\alpha \langle \mathbf{x}, \mathbf{y} \rangle = \langle \alpha \mathbf{x}, \mathbf{y} \rangle, \langle \mathbf{x}, \mathbf{z} \rangle + \langle \mathbf{y}, \mathbf{z} \rangle = \langle \mathbf{x} + \mathbf{y}, \mathbf{z} \rangle$.

3. Positive-definite: $\langle \mathbf{x}, \mathbf{x} \rangle \geq \mathbf{0}, \langle \mathbf{x}, \mathbf{x} \rangle = \mathbf{0} \Rightarrow \mathbf{x} = \mathbf{0}$.

A vector space is called an inner product space if an inner product operation is defined. Since inner product is a positive definite bilinear form, it introduces a norm, which is generally realized as "length" or "distance", for the vectors in the inner product space. The induced norm (length) of a vector $\mathbf{v}$ in the vector space $\mathcal{V}$ is defined as $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$. Inner product also introduces the idea of "angle" θ between two vectors by $\mathbf{cos}(\theta) = \langle \mathbf{x}, \mathbf{y} \rangle / (\|\mathbf{x}\| \|\mathbf{y}\|)$ and the idea of "perpendicular", if $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{0}$, $\mathbf{x}$ and $\mathbf{y}$ are said to be orthogonal, i.e. perpendicular, to each other.

A *Hilbert space* is a vector space where an inner product and its induced norm for "length" are well defined. For our vector space $\mathbb{C}^n$, a standard inner product is defined to extend it into a Hilbert space: Let $\mathbf{v_1}, \mathbf{v_2}$ be any two vectors in $\mathbb{C}^n$, the inner product of $\mathbf{v_1}, \mathbf{v_2}$ in the matrix form is defined as $\langle \mathbf{v_1}, \mathbf{v_2} \rangle = \mathbf{v_1^\dagger v_2}$ and the induced norm of $\mathbf{v_1}$ would be $\|\mathbf{v_1}\| = \sqrt{\mathbf{v_1^\dagger v_1}}$. In quantum computation, or in any physics system to say, the Hilbert space is the basic space to start with, more discussion would be made in the next chapter.

2.1.3 Bases

A *basis* $\mathfrak{B}$ of a vector space $\mathcal{V}$ over a field F is a linearly independent subset of $\mathcal{V}$ that spans $\mathcal{V}$, the vector number N of a basis B of is the *dimension* of the vector space $\mathcal{V}$.

In a Hilbert space $\mathcal{H}$, an *orthogonal* basis will be a set of orthonormal vectors $\{v_i, 1 \leq i \leq n\}$, such that $\langle v_i, v_j \rangle = 0$, for any i, j that $i \neq j$. And a *normalized* orthogonal basis $\{w_i, 1 \leq i \leq n\}$ based on $\{v_i, 1 \leq i \leq n\}$ would be the orthogonal basis all of whose elements are of norm one: $\{w_i = \frac{v_1}{\|v_i\|}, 1 \leq i \leq n\}$, such that $\langle w_i, w_j \rangle = \delta_{i,j}, \forall 1 \leq i, j \leq n$, where, δ_{ij} denote the Kronecker delta function.

The *standard basis* for the Hilbert space $\mathbb{C}^n$ is an orthogonal basis that contains a series of column vectors such that for each vector, one of their entry, say the i-th entity, is one while all the other entries are zero, denoted as $\{e_i, 1 \leq i \leq n\}$:

$$\mathbf{e_1} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \mathbf{e_2} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \cdots, \mathbf{e_i} = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \text{ : i-th entry }, \cdots, \mathbf{e_n} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

2.1.4 Tensor product spaces

Tensor product, denoted as $\otimes$, is an important method to form a composite vector space from several vector spaces.

Let $\mathcal{V}$ and $\mathcal{W}$ be two F-vector spaces of dimension m and n respectively. The tensor product $\mathcal{W} \otimes_F \mathcal{V}$ consists of all linear combinations $\sum_{\mathbf{i,j,k}} \mathbf{c_i v_j} \otimes \mathbf{w_k}$, where $\mathbf{v_1}, \mathbf{v_2}, \cdots \in \mathcal{V}$, $\mathbf{w_1}, \mathbf{w_2}, \cdots \in \mathcal{W}$, $c_1, c_2, \cdots \in F$. The tensor product $\mathcal{W} \otimes_F \mathcal{V}$ is of dimension mn and satisfies the following properties:

1.
$$c(\mathbf{v_1} \otimes \mathbf{w_1}) = (c\mathbf{v_1}) \otimes \mathbf{w_1} = \mathbf{v_1} \otimes c\mathbf{w_1}$$

2.
$$(\mathbf{v_1} + \mathbf{v_2}) \otimes \mathbf{w_1} = \mathbf{v_1} \otimes \mathbf{w_1} + \mathbf{v_2} \otimes \mathbf{w_1}$$

3.
$$\mathbf{v_1} \otimes (\mathbf{w_1} + \mathbf{w_2}) = \mathbf{v_1} \otimes \mathbf{w_1} + \mathbf{v_1} \otimes \mathbf{w_2}$$

In matrix from, the tensor product will behave in the following way, let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$ be two two by two matrices, the tensor product of them would be:

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

Tensor products of Hilbert spaces are also Hilbert spaces. In fact, the inner product can be extended to the resulted space, for example, if the two vector spaces in last example are Hilbert spaces associated with $\langle , \rangle_1$ and $\langle , \rangle_2$, respectively. Then the inner product in the resulted Hilbert space $\mathcal{V} \otimes \mathcal{W}$ would be $\langle , \rangle$, such that $\langle v_1 \otimes w_1, v_2 \otimes w_2 \rangle = \langle v_1, v_2 \rangle_1 \otimes \langle v_2, w_2 \rangle_2$. In quantum computation, the tensor product of several Hilbert spaces is used to describe the state space that consists of more than one quantum subsystems.

2.2 Linear operators

Linear operators, also known as linear transformations or linear maps, are certain vector space homomorphisms between two vector spaces over the same field, which preserves the addition and scalar multiplication operations.

There exists two special linear operators for any non-empty vector space $\mathcal{V}$ to map it into itself, one is identity operator, I_V, from $\mathcal{V}$ to itself, by mapping $I_V\mathbf{v} = \mathbf{v}$, $\forall \mathbf{v} \in \mathcal{V}$; and the other is zero operator, 0, from $\mathcal{V}$ to zero vector space, by mapping $0\mathbf{v} = \mathbf{0}$, $\forall \mathbf{v} \in \mathcal{V}$. For two linear operators $T_1 : \mathcal{V}_1 \to \mathcal{V}_2$ and $T_2 : \mathcal{V}_2 \to: \mathcal{V}_3$, a combined linear operator $T_3 = T_2 \circ T_1 : \mathcal{V}_1 \to \mathcal{V}_3$ can be composed from these two, defined by $T_3(\mathbf{v_1}) = T_2 \circ T_1(\mathbf{v_1}) = T_2(T_1(\mathbf{v_1})), \forall \mathbf{v_1} \in \mathcal{V}_1$.

Definition 2.2. There are several useful types of linear operators between two Hilbert spaces:

- A linear operator $U : \mathcal{H} \to \mathcal{H}$ is a unitary operator, if it satisfies $U^\dagger U(x) = x, UU^\dagger(y) = y, \forall x, y \in \mathcal{H}$, which leads to $\langle x, y\rangle = \langle U(x), U(y)\rangle, \forall x, y \in \mathcal{H}$.

- There is a unique adjoint linear operator $T^\dagger : \mathcal{H}_1 \to \mathcal{H}_2$ for $T : \mathcal{H}_2 \to \mathcal{H}_1$, such that $\langle T(x), y\rangle = \langle x, T^\dagger(y)\rangle, \forall x \in \mathcal{H}_1, y \in \mathcal{H}_2$.

- A linear operator maps from a Hilbert space into itself, $T : \mathcal{H} \to \mathcal{H}$, is a hermitian operator, or self-adjoint operator, if it satisfies $\langle T(x), y\rangle = \langle x, T^\dagger(y)\rangle, \forall x, y \in \mathcal{H}$.

2.2.1 Projection operators

Definition 2.3. A projection operator is a linear operator that maps a vector space $\mathcal{V}$ into itself, $P : \mathcal{V} \to \mathcal{V}$, such that $P \circ P = P$. The image space of a projection operator $P : \mathcal{V} \to \mathcal{V}$ is a subspace of the vector space $\mathcal{V}$. Let $x + y$ be a general vector in $\mathcal{V}$, where $x \in P(\mathcal{V}), y \in P(\mathcal{V})^\perp$, then P(x+y)=x.

There are two main types of projection operators: orthogonal projection operators and oblique projection operators, where orthogonal projection operator can be formulated in a simple way but oblique projection may not. In our thesis, we only concern with the orthogonal projection operators, which will be introduced in the following sections.

2.2.2 Matrix representations of linear operators

The matrix representations of a linear operator are not unique and depend on the choice of bases for each vector space during this map. For example, let $T : \mathcal{V} \to \mathcal{W}$ be a linear operator, with $\mathfrak{B}_v = \{v_i, 1 \le i \le n\}$ be the basis for $\mathcal{V}$, and $\mathfrak{B}_w = \{w_i, 1 \le i \le m\}$ be a basis for $\mathcal{W}$, then the relations from this linear map, $T(v_j) = \sum T_{ij} w_i, 1 \le j \le n, 1 \le i \le m$, would form the matrix representation of T, $[T]_{\{\mathfrak{B}_v, \mathfrak{B}_w\}} = \{T_{i,j}\}_{m \times n}$, which is a m by n matrix, with respect to the basis $\mathfrak{B}_v$ for V, and $\mathfrak{B}_w$ for W.

- A unitary linear operator $U : \mathcal{H} \to \mathcal{H}$ will have a unitary matrix representation no matter which bases are chosen, i.e. $UU^\dagger = U^\dagger U = I_{\mathcal{H}}$.
- A Hermitian linear operator $T : \mathcal{H} \to \mathcal{H}$ will have a Hermitian matrix representation no matter which bases are chosen, i.e. $U = U^\dagger$.
- The orthogonal projection operator will have a semi-positive definite Hermitian matrix representation no matter which bases are chosen, and it can be formulated based on the selection of the basis for the projection space. Let $\{v_i, 1 \le i \le k\}$ be basis elements for the projection space for $P : \mathcal{V} \to \mathcal{V}$, then an orthogonal projection operator can be formed as $P = \sum_{i=1}^{k} v_i v_i^\dagger$.

Where † denotes transpose conjugate operation on matrix.

2.3 Singular value decomposition

Singular value decomposition is an important matrix decomposition in a rotation perspective compared with the eigendecomposition. The standard singular value decomposition of an $m \times n$ real or complex matrix M is a factorization of the form $M = U\Sigma V^\dagger$, where U is an $m \times m$ real or complex unitary matrix, Σ is an $m \times n$ rectangular diagonal matrix with non-negative real numbers on the diagonal, and V is an $n \times n$ real or complex unitary matrix. The diagonal entries $\Sigma_{i,i} = \sigma_i$ are known as the singular values of M.

The m columns of U and the n columns of V are called the left-singular vectors and right-singular vectors of M, respectively. Moreover, the left-singular vectors of M are eigenvectors of $MM^\dagger$; the right-singular vectors of M are eigenvectors of $M^\dagger M$; the non-zero singular values of M are the square roots of the non-zero eigenvalues of both $M^\dagger M$ and $MM^\dagger$.

It worths to mention that the singular value decomposition is not unique.

2.4 Smith normal form

The Smith normal form is a normal form that can be defined for a matrix of any shape with entries in a principal ideal domain (P.I.D.).

Definition 2.4. Let matrix A be nonzero m by n matrix over a principal ideal domain R, then there exists some invertible matrices $P \in R^{m\times m}, Q \in R^{n\times n}$ that PAQ be a m by n matrix such that all its nonzero elements are on its diagonal and they divides each other from top to bottom and all its zero elements stay at the bottom.

$$\text{i.e. } PAQ = \begin{bmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots \\ 0 & d_2 & \cdots & 0 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_m & 0 & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}_{n\times m}$$

Here, $d_i \in \mathbb{C}[\lambda]$ such that $d_i | d_{i+1}$, $\forall 1 \leq i \leq r$ and $r \leq n, r \leq m$.

Existence and Uniqueness: The Smith normal form can be deduced step by step though some invertible row and column operations similarly defined as the elementary operations for the Gauss elimination:

1. add one row/column by another row/column multiplied by $f(\lambda)$.
2. Multiply one row/column by a nonzero scale.
3. switch two row/column.

As all the elementary operations could be equivalently carried out though left and right multiplication of some corresponding invertible matrices (elementary operation matrices), existence of the Smith normal form is garanteed. The proof of the uniqueness of such normal form is complicated and is shown in [13].

The common P.I.D. include the integer domain $\mathbb{Z}$, and $F[\lambda]$, which is a P.I.D. extended from a field F by adding a new variable λ. We will use the smith normal form over the P.I.D. $\mathbb{C}[\lambda]$ over field $\mathbb{C}$ in the later chapter to get our results.

Chapter 3

States in quantum system

Some basic concepts and latest developments in quantum information and quantum computation are introduced in this chapter. Instead of a comprehensive discussion in the physics nature of quantum mechanics, we will introduce the mathematics framework and explain all the rules and restrictions satisfied by a quantum system with only the critical reasoning. After this chapter, we will focus on the mathematics essence of these quantum information problems, and use the mathematics tools introduced in the last chapter to complete the further discussion.

3.1 Quantum state and its state space

In quantum information or any quantum mechanics related area, a quantum system could be quantitively described just as the other physical system, and we named the description as quantum state. Rather than the exact amount in classic information, it describes the chance of happening for each state of the quantum system. From the statistic perspective, it is a random variable, rather than a fact. The magnitude of each value in quantum state gives the corresponding probability that the object will be in that state at a given time, while the phase of each value gives the relative phase difference of all its states in a superposition. It is important for us to figure out if two quantum states are equivalent with each other through different states.

This description varies when it comes to different types of quantum systems. The most common quantum system is an isolated quantum system, but some composite quantum system may also be considered and be described in a different manner.

3.1.1 Pure quantum state

Postulation 1: Associated to any isolated physical system is a complex Hilbert space known as the *state space* of the system.The system is completely described by its state vector, which is a unit vector in the system 's state space [1].

If a quantum system is an isolated quantum system, say the energy spectrum of an electron, then the quantum state is recognized as a pure state inside its state space. To be more specific, it would be given as a column vector in a Hilbert Space $\mathcal{H}$, called the state vector, and the associated Hilbert space is known as the state space for such quantum states. Bra ket notation is used when it refers to a quantum system with associated properties. A state vector is denoted as $|\psi\rangle$, known as ket, over the field of complex number $\mathbb{C}$, rather than the mathematics notation, $\mathbf{v}$, associated with an inner product, $\langle|\psi\rangle, |\phi\rangle\rangle$ as $\langle\psi|\phi\rangle$, where $\langle\psi|$ denotes the dual vector of $|\psi\rangle$ in the dual Hilbert Space, $\mathcal{H}^*$, of $\mathcal{H}$, it is a linear functional $\langle|\psi\rangle, \rangle$ such that $\langle\psi|\psi\rangle = 1$, which is known as the *normalization condition.* In matrix representation, this dual vector $\langle\psi|$ is exactly the transpose conjugate of the state vector $|\psi\rangle$, denoted as $\langle\psi| = (\overline{|\psi\rangle})^T = (|\psi\rangle)^\dagger$.

There is a huge difference between classic states and quantum states in information theory, even through they have the similar forms . For example, the basic unit in classic information is bit, 1/0, which has two status, 0 and 1. Comparably, the basic unit in quantum information is qubit, which also has two status, $|0\rangle$ and $|1\rangle$. However, a state in a classic bit is either in status 0 or status 1, but a state in a qubit will have infinity many possible status including $|0\rangle$ and $|1\rangle$.Let $|\psi\rangle$ be a pure state in one qubit, it would be a vector in $\mathcal{H}_2$, such that $\langle\psi|\psi\rangle = 1$.It is equivalent to say that $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$. It is an intermedium status between $|0\rangle$ and $|1\rangle$ where the length of α and β contains the probability information for each status and the normalization condition $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$ comes from the probability nature of a quantum state.

Similar with the concept of multi bits, a quantum state described in an integral Hilbert space $\mathcal{H}$ is said to be of one *partite* and the one described in a composite Hilbert space as a tensor product of several component Hilbert subspaces is said to be of *multipartite.* For instance,

$$|\psi\rangle = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} \sum_{k=0}^{n_3-1} a_{ijk} |i\rangle^{(1)} \otimes |j\rangle^{(2)} \otimes |k\rangle^{(3)}$$

is a three partite pure state in a tensor Hilbert space with n_1, n_2, n_3 dimension for each component Hilbert subspace over the complex field, i.e. $\mathcal{H}_{n_1} \otimes \mathcal{H}_{n_2} \otimes \mathcal{H}_{n_3}(\mathbb{C})$, or $\mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \mathbb{C}^{n_3}$. Here, $\{|i\rangle^{(l)}, 0 \leq i \leq n_1 - 1\}$ is a set of orthonormal basis for the lth component Hilbert subspace and the superscript indicate to which partite does the basis element belongs.

A *multi-qubit* state refers to the quantum states on a tensor Hilbert subspace that each component Hilbert space is of dimensional two, with $|0\rangle^{(i)}$ and $|1\rangle^{(i)}$ as its basis for the ith partite of the state. For example, a bell state $1/\sqrt{2}(|00\rangle + |11\rangle) = 1/\sqrt{2}(|0\rangle^{(1)} \otimes |0\rangle^{(2)} + |1\rangle^{(1)} \otimes |1\rangle^{(2)})$ is a typical two qubit pure state in $\mathcal{H}_2 \otimes \mathcal{H}_2$.

The standard basis of a one partite N dimensional pure state $|\psi\rangle$ would be the same as that of a vector space in matrix form:

$$|0\rangle = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}, |1\rangle = \begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}, \cdots, |N-1\rangle = \begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}$$

Similarly, the standard basis of a multipartite pure state would be the tensors of the basis elements in each component subspace, take two qubit space as an example, the basis would be:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, |01\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix}, = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

This standard basis of a quantum state is also known as the *computational basis*.

3.1.2 Phase of a state

It is mentioned in the previous section that the phase of the entries of a quantum state gives information about the relative phase of the states in a superposition, and we will give more details here. let $|\psi\rangle = a|\phi_1\rangle + b|\phi_2\rangle$ be a one partite pure state(superposition) with two states $|\phi_1\rangle$ and $|\phi_2\rangle$, where $a = |a|exp(i\theta_a), b = |b|exp(i\theta_b)$ and $|a|^2 + |b|^2 = 1$, then the state could also be expressed as $|\psi\rangle = exp(i\theta_a) \cdot (|a| \cdot |\phi_1\rangle + exp(i\theta_a - \theta_b) \cdot |b| \cdot |\phi_2\rangle)$, where $exp(i\theta_a)$ work as a global phase term and $exp(i\theta_a - \theta_b)$ work as the relative phase term between two state in this superposition.

In quantum system, the entries of the state vector refers to probability information, thus the global phase is meaningless, or unphysical, as it does not provide any information of a quantum state, whilst the relative phase term provides the phase difference, the interface information, between the two states in the superposition. For example, if two states share the same magnitudes for all their entries, then even if these two states are different by a the global phase, they would be treated as the same, i.e. $|\psi\rangle \equiv exp(i\theta)|\psi\rangle$, for any angle θ; while, if the relative phase is the different in these two states, then these two states are different, i.e. $|\phi_1\rangle + exp(i\theta_a)|\phi_2\rangle \neq |\phi_1\rangle + exp(i\theta_b)|\phi_2$, if $exp(i\theta_a) \neq exp(i\theta_b)$.

Therefore we are interested in the techniques that will not change the "relative position" between any partites in the quantum system, which will be discussed in the later passage.

3.1.3 Density operator and mixed state

We already know that there exists a unique projection operator for any nonzero vector in last chapter. Similarly in quantum mechanics, for any pure quantum state $|\psi\rangle$, there exists a unique linear operator $|\psi\rangle\langle\psi|$, known as a measurement operator in physics, which corresponds to that state and use the state as its unique eigenvector. A measurement on a pure state, $|\psi\rangle$, of any state vector, $|\phi\rangle$, in the same state space, can be obtained as the eigenvalue λ by applying the corresponding measurement operator to that vector, i.e. $(|\psi\rangle\langle\psi|)(|\phi\rangle) = \lambda|\phi\rangle$. The uniqueness of such operator allows us to use this operator as an alternative way to describe quantum states and this operator is known as the density operator for a quantum state.

Besides a pure state as some isolated quantum system, this operator could also be used to describe some complicate quantum system which is a mixture of several correlated systems with associated chance, known as a mixed state. For example if a quantum system will appear in n different states $|\psi_i\rangle, 1 \leq i \leq n$ with chance p_i, then its mixed state ρ is defined to be statistical ensemble of several pure quantum states, which share the same state space, in form of their density operator, $\rho = \sum_{i=1}^{n} p_i|\psi_i\rangle\langle\psi_i|$. In general, such mixed state could not be described as a column vector in a Hilbert space like pure state.

Mathematically speaking, the density operator for a quantum state, no matter pure or mixed, would be a linear operator acting on the common state space of all its component pure quantum states. Correspondingly, the operator space for density operators would be the Hilbert space of all the linear operators acting on its state vector space with a well defined inner product.

3.2 Density matrices and related features

Density matrix, on the other hand, refers to the matrix representation of the density operator with respect to certain basis. For example, a density matrix ρ for a two partite quantum state of dimensional two on both partite will be a linear operator acting on Hilbert Space $\mathcal{H}_2 \otimes \mathcal{H}_2$, and the inner product for any density operator ρ_1, ρ_2 on state space $\mathcal{H}_2 \otimes \mathcal{H}_2$ in matrix form would be $\langle\rho_1, \rho_2\rangle = tr(\rho_1^\dagger \rho_2)$.

3.2.1 Basis for density operator

A basis of a density operator could be induced from the basis for each partite of the quantum state. Let ρ be the density operator of a M partite quantum state with $n_1, n_2, \cdots, n_M$ dimension for each partite, i.e. ρ is a linear operator acting on the Hilbert space $\mathcal{H}_{n_1} \otimes \mathcal{H}_{n_2} \otimes \cdots \otimes \mathcal{H}_{n_M}$. Let $\{|i_1\rangle^{(1)}, 0 \leq i_1 \leq n_1 - 1\}$, $\{|i_2\rangle^{(2)}, 0 \leq i_2 \leq n_2 - 1\}$, ..., $\{|i_M\rangle^{(M)}, 0 \leq i_M \leq n_M - 1\}$ be some chosen bases for each Hilbert subspace $\mathcal{H}_{n_1}, \mathcal{H}_{n_2}, \cdots \mathcal{H}_{n_M}$, , where the superscript indicates which partite does the basis element belongs to. Then a basis for this quantum state would be formed as $\{|i_1\rangle^{(1)} \otimes |i_2\rangle^{(2)} \otimes \cdots \otimes |i_M\rangle^{(M)} \langle i_1|^{(1)} \otimes \langle i_2|^{(2)} \otimes \cdots \otimes \langle i_M|^{(M)}, 0 \leq i_1 \leq n_1 - 1, 0 \leq i_2 \leq n_2 - 1, \cdots, 0 \leq i_M \leq n_M - 1\}$, the superscript may sometimes be neglected for convenience.

The computational basis for a density operator follows the same idea with that of a pure state. Take 2-qubit quantum state as example, the computational basis is formed as:

$$|00\rangle\langle 00| = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad |00\rangle\langle 01| = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \cdots$$

Remark: The density matrix for a density operator without special notice would be in its standard basis.

3.2.2 Properties of a density matrix

A density matrix $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$ in its computational basis (if it is pure, then there would be only one term: $\rho = |\psi\rangle\langle\psi|$) will have the following properties/axioms:

1. ρ is a nonnegative definite hermitian matrix.

   $\rho^\dagger = (\sum p_i |\psi_i\rangle\langle\psi_i|)^\dagger = \sum p_i (|\psi_i\rangle\langle\psi_i|)^\dagger = \rho$ and for any vector $|u\rangle$ in the same Hilbert space of $\{|\psi_i\rangle\}$, we have:

   $$\langle u|\rho|u\rangle = \langle u| \sum p_i |\psi_i\rangle\langle\psi_i||u\rangle = \sum p_i \cdot \langle u|\psi_i\rangle\langle\psi_i|u\rangle \geq 0, \quad as\ p_i > 0$$

   (Notation: $A^\dagger = \bar{A}^T$ for any matrix A)

   Remark: According to Schur decomposition, all the density matrices(nonnegative definite hermitian matrices) will share the same eigenvalues with its singular values.

2. $tr(\rho) = 1$ for any quantum state, no matter pure or mixed.

   $$tr(\rho) = tr(\sum p_i |\psi_i\rangle\langle\psi_i|) = \sum p_i \cdot tr(|\psi_i\rangle\langle\psi_i|) = \sum p_i \cdot tr(\langle\psi_i|\psi_i\rangle) = \sum p_i = 1$$

If a matrix satisfies these two axioms, then it is a density matrix. Moreover, a density matrix ρ is a pure state if $tr(\rho^2) = 1$, and a mixed state if $tr(\rho^2) < 1$.

$$tr(\rho_{pure}^2) = tr(|\psi\rangle\langle\psi||\psi\rangle\langle\psi|) = tr(|\psi\rangle\langle\psi|) = tr(\langle\psi|\psi\rangle) = 1$$
$$tr(\rho_{mixed}^2) = tr((\sum p_i |\psi_i\rangle\langle\psi_i|)^2) = tr(\sum p_i^2 |\psi_i\rangle\langle\psi_i|) = \sum p_i^2 tr(|\psi_i\rangle\langle\psi_i|) = \sum p_i^2 < 1$$

For example, two two-qubit quantum state density matrices are given below, one mixed state $\rho_1 = (|00\rangle\langle 00| + |01\rangle\langle 01|)/2$ and one pure state $\rho_2 = |\psi\rangle\langle\psi|$ with $|\psi\rangle = (|01\rangle + |00\rangle)/\sqrt{2}$:

$$\rho_1 = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\rho_2 = \frac{|00\rangle\langle 00| + |01\rangle\langle 01| + |00\rangle\langle 01| + |01\rangle\langle 00|}{2} = \begin{bmatrix} 1/2 & 1/2 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

3.2.3 Reduced density operator

A density operator on a composite Hilbert space would be hard to analyze if it can not be break down into smaller systems. Thus we need an reverse operation to the tensor product in order to analyze the structure of a multipartite quantum state.

Definition Assume a density operator ρ^{AB} is a composite system as a tensor of two subsystems, one of the subsystem is A, and the other is B, then ρ^A, ρ^B are known as reduced density operators of the origin density operator:

$$\rho^A \equiv tr_B(\rho^{AB}), \quad \rho^B \equiv tr_A(\rho^{AB})$$

Here, tr_A, are known as the partial trace operator, a linear operator, over system A, while tr_B the partial trace operator over system B. In details, any system $\rho = |a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l|$, $tr_A(\rho) = tr_A(|a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_l|) = (\langle a_j|a_i\rangle)|b_k\rangle\langle b_l|$. For the special case, if $\rho^{AB} = \rho_1 \otimes \rho_2$, where ρ_1, ρ_2 are density matrices for the subsystems of the composite system ρ^{AB} ($\mathrm{tr}(\rho_1) = tr(\rho_2) = 1$)), then $\rho^A = tr_B(\rho_1 \otimes \rho_2) = \rho_1 tr_B(\rho_2) = \rho_1$.

Ex. let ρ be a two qubit density matrix with its standard basis, $\{|i_1\rangle|j_1\rangle\langle i_2|\langle j_2| = |i_1\rangle\langle i_2| \otimes |j_1\rangle\langle j_2|, 0 \leq i_1, i_2, j_1, j_2 \leq 1\}$ and $\rho = \sum_{i_1,i_2,j_1,j_2} a_{i_1,i_2,j_1,j_2}|i_1\rangle\langle i_2| \otimes |j_1\rangle\langle j_2|$.

$$\begin{aligned} tr_1(\rho) &= \sum_{i_1,j_1,i_2,j_2} a_{i_1 i_2 j_1 j_2} tr_1(|i_1\rangle\langle i_2| \otimes |j_1\rangle\langle j_2|) & , tr_2(\rho) &= \sum_{i_1,j_1,i_2,j_2} a_{i_1 i_2 j_1 j_2} tr_2(|i_1\rangle\langle i_2| \otimes |j_1\rangle\langle j_2|) \\ &= \sum_{i_1,j_1,i_2,j_2} a_{i_1 i_2 j_1 j_2}(\langle i_1|i_2\rangle)|j_1\rangle\langle j_2| & &= \sum_{i_1,j_1,i_2,j_2} a_{i_1 i_2 j_1 j_2}(\langle j_1|j_2\rangle)|i_1\rangle\langle i_2| \\ &= \sum_{j_1,j_2}(\sum_i a_{i i j_1 j_2})|j_1\rangle\langle j_2| & &= \sum_{i_1,i_2}(\sum_j a_{i_1 i_2 j j})|i_1\rangle\langle i_2| \end{aligned}$$

To be more specific:

$$tr_1(\frac{(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)}{2}) = tr_1(\frac{(|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|)}{2})$$
$$= \frac{(\langle 0|0\rangle|0\rangle\langle 0| + \langle 1|0\rangle|1\rangle\langle 0| + \langle 0|1\rangle|0\rangle\langle 1| + |\langle 1|1\rangle|1\rangle\langle 1|)}{2}$$
$$= \frac{(|0\rangle\langle 0| + |1\rangle\langle 1|)}{2}$$

Fact: It is easy to check that the reduced operator of a density operator is still nonnegative definite hermitian with trace one, thus is still a density matrix.

3.2.4 Quantum entanglement in density matrix

In this section, we are going to discuss the differences between quantum states with or without entanglement presented in matrix form.

The class of quantum states that are completely non entangled is also known as separable states. A separable state, no matter pure or mixed, could be present as a density matrix as the tensor product of some sub density matrices in each partite. Moreover, If the state is a pure state in this case, it could also be presented as a column vector which could be formed as the tensor product of some column vectors in each component Hilbert subspace for each partite.

For example, $|\psi_1\rangle = \frac{|00\rangle+|10\rangle-|01\rangle-|11\rangle}{2}$ is a separable two qubit quantum states, with $|\psi_1\rangle^{(1)} = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ in the first qubit, and $|\psi_1\rangle^{(2)} = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ in the second qubit.

$$|\psi_1\rangle = \frac{|00\rangle + |10\rangle - |01\rangle - |11\rangle}{2} = \begin{bmatrix} 1/2 \\ -1/2 \\ 1/2 \\ -1/2 \end{bmatrix}$$
$$= (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} \otimes \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$$
$$|\psi_1\rangle\langle\psi_1| = (\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}})(\frac{\langle 0| + \langle 1|}{\sqrt{2}} \otimes \frac{\langle 0| - \langle 1|}{\sqrt{2}}) = \begin{bmatrix} 1/4 & -1/4 & 1/4 & -1/4 \\ -1/4 & 1/4 & -1/4 & 1/4 \\ 1/4 & -1/4 & 1/4 & -1/4 \\ -1/4 & 1/4 & -1/4 & 1/4 \end{bmatrix}$$
$$|\psi_1\rangle\langle\psi_1| = ((\frac{|0\rangle + |1\rangle}{\sqrt{2}})(\frac{\langle 0| + \langle 1|}{\sqrt{2}})) \otimes ((\frac{|0\rangle - |1\rangle}{\sqrt{2}})(\frac{\langle 0| - \langle 1|}{\sqrt{2}})) = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \otimes \begin{bmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{bmatrix}$$

Comparably, an entangled state could not be decomposed into a tensor product of sub states in each partite. E.g. $|\psi\rangle = (|00\rangle + |11\rangle)/(\sqrt{2})$ is an entangled two qubit pure state and $\rho = 1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)$ is an entangled two qubit mixed state:

$$|\psi\rangle\langle\psi| = (\frac{|00\rangle + |11\rangle}{\sqrt{2}})(\frac{\langle 00| + \langle 11|}{\sqrt{2}}) = \begin{bmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix} \neq tr_2(|\psi\rangle\langle\psi|) \otimes tr_1|\psi\rangle\langle\psi|$$

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1\sqrt{2} \end{bmatrix} = 1/\sqrt{2} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} + 1/\sqrt{2} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq |\psi\rangle^{(1)} \otimes |\psi\rangle^{(2)}.$$

$$\rho = \begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{bmatrix} \neq tr_2(\rho) \otimes tr_1(\rho)$$

You can check that it is impossible to decompose these quantum states as a tensor of some sub state(density matrix) in each partite.

Moreover, an entangled pure state will have mixed reduced density operator, take the state $|\psi\rangle$ in last example as an example, the reduced density operator of $|\psi\rangle\langle\psi|$ by the partial trace on the first partite will be:

$$\begin{aligned} tr_1|\psi\rangle\langle\psi| &= tr_1(\frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2}) \\ &= \frac{\langle 0|0\rangle|0\rangle\langle 0| + \langle 1|0\rangle|1\rangle\langle 0| + \langle 0|1\rangle|0\rangle\langle 1| + \langle 1|1\rangle|1\rangle\langle 1|}{2} = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix} \end{aligned}$$

It could also be explained in a statistic perspective similar with the idea of the phase of a state: there is no entanglement in a quantum state suggests that the sub random variables correspond to each partite of the state are independent from each other; while that a state is entangled means that some of the corresponding random variables of its partite are correlated with each other. If two quantum states are highly correlated, in other words completely entangled, then you can measure one of the state to infer the state of the other.

Chapter 4

LU equivalence of quantum states

As mentioned in the introduction, determining the LU equivalence of quantum states is an important way to classify the quantum states with different level of the entanglement. In this section, we start to deduct criterions to determine the LU equivalence of two partite quantum states.

4.1 Unitary transformations between quantum states

It is known that for any two pure states in the same Hilbert space these, they could be transformed into each other by some unitary transformation. This is because quantum state is "normalized" with the same norm one and there would always exist some unitary transformation to convert one pure state into the other. However, it is not so intuitive to check if two mixed states(density matrix form) are unitary equivalent:

Let ρ be some density matrix on the Hilbert space $\mathbb{C}^n$, or equivalently saying a mixed state, then the image of a unitary transformation $U \in U(n)$ acting on ρ is $U\rho U^\dagger$. It is also known as a unitarily similar term or the adjoint operation result of ρ under U. Since the global phase is unphysical in quantum information, we can restrict the unitary matrix group $U(n)$ to $SU(n)$ without losing generality. In addition, M^U will be defined as $UMU^\dagger$, for any square matrix M and any unitary matrix U of the same dimension following the general notation.

If two density operators are unitarily similar to each other, they are said to be unitary equivalent, and they would belong to the same unitary equivalence class.

Fact: Two density operators on the same Hilbert space (with the same subsystem structure) would have the same eigenvalues or singular values (including zero ones) and the same rank, if they are in the same unitary equivalence class.

For example, density operators of all pure states on the same space would belong to the same unitary equivalence class as they all have the same eigenvalue/singular values during which the unique nonzero value is one.

4.2 LU transformation in quantum system

LU transformation is a kind of unitary transformation such that the relation between these partites of a quantum state will not be changed under such transformation.

In a LU transformation, each subsystem, known as the local system, of a multipartite quantum state would also be under a unitary transformation. Suppose there is a quantum state on the same composite Hilbert space $\mathcal{H}$ which is composed of M local Hilbert space, $\mathcal{H}_1, \mathcal{H}_2, \cdots, \mathcal{H}_M$ with dimension $d_1, d_2, ..., d_M$, respectively, i.e. $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_M$. Then we can construct a unitary transformation by composing a series of unitary transformations $U_1 \in SU(d_1), U_2 \in SU(d_2), \cdots U_M \in SU(d_M)$ which match the dimension of each partite, respectively.

To be more specific, if the state is a pure state $|\psi\rangle$, then the unitary transformation would be present either in state vector form as $(U_1 \otimes U_2 \otimes \cdots \otimes U_M)|\psi\rangle$, or in density matrix form as $(U_1 \otimes U_2 \otimes \cdots \otimes U_M)|\psi\rangle\langle\psi|(U_1 \otimes U_2 \otimes \cdots \otimes U_M)^\dagger$; And if the state is a mixed state ρ, the only available form is the density form: $(U_1 \otimes U_2 \otimes \cdots \otimes U_M)\rho(U_1^\dagger \otimes U_2^\dagger \otimes \cdots \otimes U_M^\dagger)$

Then the linear transformation $U_1 \otimes U_2 \otimes \cdots \otimes U_M$ is said to be a LU transformation, and two states are said to be LU equivalent if there is some LU transformation to convert one to the other. Moreover, similar with unitary equivalence class, LU equivalent is also an equivalence relation and we could use this relation to classify all the quantum states on the same Hilbert space (with the same subspace structure as well) into LU equivalence classes.

To determine LU equivalence of quantum states, one important tool is the partial trace which is mentioned in last chapter. Let $U_1 \otimes U_2$ be a LU transformation on a bipartite state in its computational basis, $\rho = \sum_{i_1,j_1,i_2,j_2} a_{i_1 i_2 j_1 j_2} |i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \langle i_2|^{(1)} \langle j_2|^{(2)}$, the partial trace operation on each partite will keep the local information, including the unitary transformation on the partite that has not been traced out, i.e.

$$
\begin{aligned}
tr_1\left(U_1 \otimes U_2 \rho U_1^\dagger \otimes U_2^\dagger\right) &= tr_1\left(\sum_{i_1,j_1,i_2,j_2} a_{i_1 i_2 j_1 j_2} U_1 |i_1\rangle^{(1)} \langle i_2|^{(1)} U_1^\dagger \otimes U_2 |j_1\rangle^{(2)} \langle j_2|^{(2)} U_2^\dagger\right) \\
&= \sum_{j_1,j_2} (\sum_{i_1,i_2} a_{i_1 i_2 j_1 j_2} \langle i_2|^{(1)} U_1^\dagger U_1 |i_1\rangle^{(1)} \otimes U_2 |j_1\rangle^{(2)} \langle j_2|^{(2)} U_2^\dagger) \\
&= U_2 \left(\sum_{j_1,j_2} (\sum_i a_{i j_1 i j_2} |j_1\rangle^{(2)} \langle j_2|^{(2)}))\right) U_2^\dagger = U_2 tr_1(\rho) U_2^\dagger
\end{aligned}
$$

Similarly, $tr_2(U_1 \otimes U_2 \rho U_1^\dagger \otimes U_2^\dagger) = U_1 tr_2(\rho) U_1^\dagger$. This property allows us to use partial trace operator to gather information for a LU transformation on a multi-partite quantum states. When we deal with problems regarding multipartite quantum states, partial trace operator is of most importance.

Fact: If two multipartite state are LU equivalent, then the result density matrices of these two states by the partial trace with respect to any subsystem of them will be unitary equivalent.

4.3 LU transformation in different matrix folding

Basically, a new matrix folding of a matrix is a new arrangement of the elements of the matrix in a different manner. It could be treated as a linear map that would transform the dimension of the matrix. We may get some new perspective of the same matrix and its related unitary transformation under different matrix folding. Similar idea is also introduced in Higher-order singular value decomposition related papers [15].

We will start with the state without any subsystem. Let ρ be a one partite mixed state acting on a Hilbert space with dimensional d, then it would be a $d \times d$ square matrix in its computational basis $\{|i\rangle\langle j|, 0 \le i \le d-1, 0 \le j \le d-1\}$, i.e. $\rho = \sum_i \sum_{j=1}^n a_{ij} |i\rangle\langle j|$. However, we can map this density operator ρ on Hilbert space $\mathbb{C}^d$ into a tensor vector space $\mathbb{C}^d \otimes \mathbb{C}^d$, and get another matrix folding manner for ρ by the linear map $\phi_0 : \mathbb{C}^{d\times d} \to \mathbb{C}^d \otimes \mathbb{C}^d$, by $|i\rangle\langle j| \mapsto |i\rangle \otimes |j\rangle$, thus $\phi_0(\rho) = \phi_0(\sum_i \sum_j^n a_{ij}|i\rangle\langle j|) = \sum_i \sum_j a_{ij} \phi_0(|i\rangle\langle j|) = \sum_i \sum_j a_{ij} |i\rangle \otimes |j\rangle$.

Under a unitary transformation $U \in SU(d)$, a basis element $|i\rangle\langle j|$ of ρ will be transformed into $U|i\rangle\langle j|U^\dagger$, and its corresponding basis element in the new matrix folding would be $\phi_0(U|i\rangle\langle j|U^\dagger) = U|i\rangle \otimes U|j\rangle = U \otimes U(|i\rangle \otimes |j\rangle) = U \otimes U(|i\rangle \otimes |j\rangle)$.

And ρ under a unitary transformation U, $U\rho U^\dagger$, in its computational basis would be map to $\phi_0(U\rho U^\dagger) = \phi_0(U(\sum_i \sum_j a_{ij}|i\rangle\langle j|)U^\dagger) = \sum_i \sum_j a_{ij}\phi_0(U|i\rangle\langle j|U^\dagger) = \sum_i \sum_j a_{ij} U \otimes U(|i\rangle \otimes |j\rangle) = U \otimes U \phi_0(\rho)$ in this matrix folding.

For example, let $\rho = 3/4|0\rangle\langle 0| + 1/4|1\rangle\langle 1|$ be a one-qubit state, then it would be transformed into $\phi_0(\rho) = 1/4|0\rangle \otimes |0\rangle + 3/4|1\rangle \otimes |1\rangle$ under the new matrix folding, similarly if ρ is under unitary transformation $U = \begin{bmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{bmatrix}$, then this unitary transformation would be converted into the new matrix folding, $\phi_0(U\rho U^\dagger)$, as following:

$$\rho = \begin{bmatrix} 3/4 & 0 \\ 0 & 1/4 \end{bmatrix}, \phi_0(\rho) = \begin{bmatrix} 3/4 \\ 0 \\ 0 \\ 1/4 \end{bmatrix}, U\rho U^\dagger = \begin{bmatrix} 0.43 & 0.24 \\ 0.24 & 0.57 \end{bmatrix}, \phi_0(U\rho U^\dagger) = \begin{bmatrix} 0.43 \\ 0.24 \\ 0.24 \\ 0.57 \end{bmatrix}$$

And you can check that: $\phi_0(U\rho U^\dagger) = U \otimes U\phi_0(\rho)$

$$U \otimes U\phi_0(\rho) = \begin{bmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{bmatrix} \otimes \begin{bmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{bmatrix} \begin{bmatrix} 3/4 \\ 0 \\ 0 \\ 1/4 \end{bmatrix} = \begin{bmatrix} 0.43 \\ 0.24 \\ 0.24 \\ 0.57 \end{bmatrix} = \phi_0(U\rho U^\dagger)$$

Unfortunately, it is still not easy to check if two vector are unitary equivalent under unitary matrix with the form $U \otimes U$. Considering the norm for this matrix folding, we will have the same result of the criterion which is used to determine the pure state density matrix into our matrix folding:

Fact: If two density matrix ρ and ρ' are unitary equivalent, then their column vector foldings, $\phi_0(\rho)$ and $\phi_0(\rho')$ have the same norm. Moreover, any density matrix in its computational basis $\rho = \sum_{i,j} a_{ij}|i\rangle\langle j|$ is a pure state, $\rho = |\psi\rangle\langle\psi|$ if and only if its column vector folding, $\phi_0(\rho) = \sum_{i,j} a_{ij}|i\rangle \otimes |j\rangle = |\psi\rangle \otimes |\psi\rangle$, has norm one, i.e. $\sum_{i,j} a_{ij}a_{ij}^* = 1(tr(\rho^2) = 1)$, while ρ is a mixed state, $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, if and only if its column vector folding, $\phi_0(\rho) = \sum p_i|\psi_i\rangle \otimes |\psi_i\rangle$, has norm less than one, , i.e. $\sum_{i,j} a_{ij}a_{ij}^* < 1(tr(\rho^2) < 1)$.

4.3.1 Matrix folding in two partite quantum states

The new matrix folding of the density operator could also be applied to two partite case and as the structure is more complicated in this case, there are more than one approach to form the matrix folding. We classify all matrix foldings in multipartite case into two types. Let ρ be a two partite mixed state acting on a composite Hilbert space with dimensional d_1 and d_2, then it would be a $d_1d_2 \times d_1d_2$ square matrix in its computational basis $\{|i_1j_1\rangle\langle i_2j_2|, 0 \leq i_1, i_2 \leq d_1 - 1, 0 \leq j_1, j_2 \leq d_2 - 1\}$, i.e. $\rho = \sum_{i_1,i_2}\sum_{j_1,j_2} a_{i_1j_1i_2j_2}|i_1j_1\rangle\langle i_2j_2|$, and let $U \otimes V$ be a LU transformation on ρ, where $U \in SU(d_1), V \in SU(d_2)$. The two types of matrix folding will be in the following way:

Type I: A quantum state in this type of matrix folding will be in a column vector form, maps for this type of matrix foldings are analogue with the ones in one partite case.

For example, $\phi_0^2 : \mathbb{C}^{d_1 \times d_2} \otimes \mathbb{C}^{d_1 \times d_2} \to \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ with the mapping, $|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)}\langle i_2|^{(1)} \otimes \langle j_2|^{(2)} \mapsto |i_1\rangle^{(1)} \otimes |i_2\rangle^{(1)} \otimes |j_1\rangle^{(2)}|j_2\rangle^{(2)}$ is a type I matrix folding and it will convert ρ in its computational basis into a column vector. If under the LU transformation $U \otimes V$, ρ in this matrix folding will be transformed into $\phi_0^2((U \otimes V)(\rho)(U \otimes V)^\dagger) = U \otimes U \otimes V \otimes V\phi_{0.0}^{(2)}(\rho)$, where the superscript of the map ϕ_0^2 denote the number of partite in the state involved. There are many useful results based on this type of matrix foldings in the following sections.

There are other ways to form similar type I matrix folding as well. $\phi_{0.1}^2 : \mathbb{C}^{d_1d_2 \times d_1d_2} \to \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ with the mapping, $|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)}\langle i_2|^{(1)} \otimes \langle j_2|^{(2)} \mapsto |i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \otimes$

$|i_2\rangle^{(1)} \otimes |j_2\rangle^{(2)}$ is another map that gives a different column vector form of the state . If under the LU transformation $U \otimes V$, ρ in this matrix folding will be transformed into $\phi^2_{0.1}((U \otimes V)(\rho)(U \otimes V)^\dagger) = U \otimes V \otimes U \otimes V \phi^2_{0.1}(\rho)$.

Type II: This type of matrix folding will form a new matrix with different structure:

We will convert this ρ, on $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, into an ordinary matrix, by the linear map $\phi^2_1 : \mathbb{C}^{d_1 d_2 \times d_1 d_2} \to \mathbb{C}^{d_1^2 \times d_2^2}$, by $|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \langle i_2|^{(1)} \otimes \langle j_2|^{(2)} \mapsto |i_1\rangle^{(1)} \otimes |i_2\rangle^{(1)} \langle j_1|^{(2)} \otimes \langle j_2|^{(2)}$, where the superscript indicate which partite the state belongs to.

Under the LU transformation $U \otimes V$, ρ would be converted into $U \otimes V \rho (U \otimes V)^\dagger$. A basis element $|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \langle i_2|^{(1)} \otimes \langle j_2|^{(2)}$ of ρ will be transformed into $U|i_1\rangle^{(1)} \otimes V|j_1\rangle^{(2)} \langle i_2|^{(1)} U^\dagger \otimes \langle j_2|^{(2)} V^\dagger$, and its corresponding basis element in the new representation would be:

$\phi^2_1(U|i_1\rangle^{(1)} \otimes V|j_1\rangle^{(2)} \langle i_2|^{(1)} U^\dagger \otimes \langle j_2|^{(2)} V^\dagger) = U \otimes U (|i_1\rangle^{(1)} \otimes |i_2\rangle^{(1)} \langle j_1|^{(2)} \otimes \langle j_2|^{(2)})(V \otimes V)^\dagger$:

$$\begin{aligned}
\phi^2_1(U|i_1\rangle^{(1)} \otimes V|j_1\rangle^{(2)} \langle i_2|^{(1)} U^\dagger \otimes \langle j_2|^{(2)} V^\dagger) &= U|i_1\rangle^{(1)} \otimes U|i_2\rangle^{(1)} \langle j_1|^{(2)} V^\dagger \otimes \langle j_2|^{(2)} V^\dagger \\
&= U|i_1\rangle^{(1)} \otimes U|i_2\rangle^{(1)} \langle j_1|^{(2)} V^\dagger \otimes \langle j_2|^{(2)}) V^\dagger \\
&= U \otimes U (|i_1\rangle^{(1)} \otimes |i_2\rangle^{(1)} \langle j_1|^{(2)} \otimes \langle j_2|^{(2)})(V \otimes V)^\dagger
\end{aligned}$$

And ρ would be map to $\phi^2_1(U \otimes V \rho (U \otimes V)^\dagger) = U \otimes U \phi(\rho)(V \otimes V)^\dagger$ in this matrix folding:

$$\begin{aligned}
\phi^2_1(U \otimes V \rho (U \otimes V)^\dagger) &= \phi^2_1(U \otimes V \sum_{i_1,j_1} \sum_{i_2,j_2} a_{i_1 j_1 i_2 j_2} |i_1 j_1\rangle\langle i_2 j_2| (U \otimes V)^\dagger) \\
&= \sum_{i_1,j_1} \sum_{i_2,j_2} a_{i_1 j_1 i_2 j_2} \phi^2_1(U \otimes V |i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \langle i_2|^{(1)} \otimes \langle j_2|^{(2)} (U \otimes V)^\dagger) \\
&= \sum_{i_1,j_1} \sum_{i_2,j_2} a_{i_1 j_1 i_2 j_2} U \otimes U (|i_1\rangle^{(1)} \otimes |i_2\rangle^{(1)} \langle j_1|^{(2)} \otimes \langle j_2|^{(2)})(V \otimes V)^\dagger \\
&= U \otimes U \phi^2_1(\rho)(V \otimes V)^\dagger
\end{aligned}$$

where $U \otimes U$ is in $SU(d_1) \otimes SU(d_1)$, $V \otimes V$ is in $SU(d_2) \otimes SU(d_2)$.

For example, let $\rho = 3/4|00\rangle\langle 00| + 1/4|12\rangle\langle 12|$ be a two partite quantum state on Hilbert space $\mathcal{H}_2 \otimes \mathcal{H}_3$, then it would be transformed into $\phi(\rho) = 3/4|0\rangle^{(1)} \otimes |0\rangle^{(1)} \langle 0|^{(2)} \langle 0|^{(2)} + 1/4|1\rangle^{(1)} \otimes |1\rangle^{(1)} \langle 2|^{(2)} \otimes \langle 2|^{(2)}$ under the new matrix folding, similarly if ρ is under the LU transformation $U \otimes V = \begin{bmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12/13 & -5/13 \\ 0 & 5/13 & 12/13 \end{bmatrix}$, then this unitary transformation would be converted into the new matrix folding, $\phi(U \otimes V\rho(U \otimes V)^\dagger)$, as following:

$$\rho = \begin{bmatrix} 3/4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1/4 \end{bmatrix}, \quad \phi(\rho) = \begin{bmatrix} 3/4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/4 \end{bmatrix}$$

$$(U \otimes V)\rho(U \otimes V)^\dagger = \begin{bmatrix} 0.270 & 0.000 & 0.000 & 0.360 & 0.000 & 0.000 \\ 0.000 & 0.024 & -0.057 & 0.000 & -0.018 & 0.043 \\ 0.000 & -0.057 & 0.137 & 0.000 & 0.043 & -0.102 \\ 0.360 & 0.000 & 0.000 & 0.480 & 0.000 & 0.000 \\ 0.000 & -0.018 & 0.043 & 0.000 & 0.013 & -0.032 \\ 0.000 & 0.043 & -0.102 & 0.000 & -0.032 & 0.077 \end{bmatrix}$$

$$\phi_1^2((U \otimes V)\rho(U \otimes V)^\dagger) = \begin{bmatrix} 0.27 & 0 & 0 & 0 & 0.024 & -0.057 & 0 & -0.057 & 0.137 \\ 0.36 & 0 & 0 & 0 & -0.018 & 0.043 & 0 & 0.043 & -0.102 \\ 0.36 & 0 & 0 & 0 & -0.018 & 0.043 & 0 & 0.043 & -0.102 \\ 0.48 & 0 & 0 & 0 & 0.013 & -0.032 & 0 & -0.032 & 0.077 \end{bmatrix}$$

And you can check that: $\phi_1^2((U \otimes V)\rho(U \otimes V)^\dagger) = U \otimes U\phi_1^2(\rho)(V \otimes V)^\dagger$. Notice that density operator in this matrix folding will no longer following the same properties of a density matrix(they may not even be square matrices sometimes). And all the density operators in the same LU equivalence class would share the same singular values in this matrix folding, so we can get a small lemma here.

Lemma 4.1. If two bipartite quantum states ρ, ρ' on the same Hilbert space are LU equivalent, then the two density operators in the type II matrix folding, $\phi_1^2(\rho)$ and $\phi_1^2(\rho')$, will have the same singular values.

4.3.2 Matrix folding in multipartite quantum states

This matrix folding could be extended into multipartite as well, and there are many choices for that, one of them is analogue to the one in two partite quantum states, similar result can also be found in [15]:

Take three-partite quantum mixed state ρ acting on the Hilbert space $\mathcal{H}_{d_1} \otimes \mathcal{H}_{d_2} \otimes \mathcal{H}_{d_3}$ as an example, the computational basis is:

$$\{|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \otimes |k_1\rangle^{(3)} \langle i_2|^{(1)} \otimes \langle j_2|^{(2)} \otimes \langle k_2|^{(3)}, 0 \le i_1, i_2 \le d_1-1, 0 \le j_1, j_2 \le d_2-1, 0 \le k_1, k_2 \le d_3-1\}$$

Type I: column vector form. I will directly give the result of the map ϕ_0^3, as it is based on the same principles: $\phi_0^3 : \mathbb{C}_{d_1 d_2 d_3 \times d_1 d_2 d_3} \rightarrow \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3} \otimes \mathbb{C}^{d_3}$ will map ρ in its computational basis to a column vector by:
$|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \otimes |k_1\rangle^{(3)} \langle i_2|^{(1)} \otimes \langle j_2|^{(2)} \otimes \langle k_2|^{(3)} \mapsto |i_1\rangle^{(1)} \otimes |i_2\rangle^{(1)} \otimes |j_1\rangle^{(2)} \otimes |j_2\rangle^{(2)} \otimes |k_1\rangle^{(3)} \otimes |k_2\rangle^{(3)}$.

The result of LU transformation in this map will be:

$$\phi_0^3(U_1 \otimes U_2 \otimes U_3(\rho)(U_1 \otimes U_2 \otimes U_3)^\dagger) = U_1 \otimes U_1 \otimes U_2 \otimes U_2 \otimes U_3 \otimes U_3 \phi_0^3(\rho)$$

Type II: New matrix form.

We can also setup three linear maps:

$\phi_{1.1}^3 : M(d_1 \cdot d_2 \cdot d_3, \mathbb{C}) \rightarrow \mathbb{C}^{(d_1^2) \times (d_2^2 \cdot d_3^2)}$ by:

$$|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \otimes |k_1\rangle^{(3)} \langle i_2|^{(1)} \otimes \langle j_2|^{(2)} \otimes \langle k_2|^{(3)} \overset{\phi_{1.1}^3}{\mapsto} (|i_1\rangle^{(1)} \otimes |i_2\rangle^{(1)})(\langle j_1|^{(2)} \otimes \langle j_2|^{(2)} \otimes \langle k_1|^{(3)} \otimes \langle k_2|^{(3)})$$

$\phi_{1.2}^3 : M(d_1 \cdot d_2 \cdot d_3, \mathbb{C}) \rightarrow \mathbb{C}^{(d_2^2) \times (d_3^2 \cdot d_1^2)}$ by:

$$|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \otimes |k_1\rangle^{(3)} \langle i_2|^{(1)} \otimes \langle j_2|^{(2)} \otimes \langle k_2|^{(3)} \overset{\phi_{1.2}^3}{\mapsto} (|j_1\rangle^{(2)} \otimes |j_2\rangle^{(2)})(\langle k_1|^{(3)} \otimes \langle k_2|^{(3)} \otimes \langle i_1|^{(1)} \otimes \langle i_2|^{(1)})$$

$\phi_{1.3}^3 : M(d_1 \cdot d_2 \cdot d_3, \mathbb{C}) \rightarrow \mathbb{C}^{(d_3^2) \times (d_1^2 \cdot d_2^2)}$, by:

$$|i_1\rangle^{(1)} \otimes |j_1\rangle^{(2)} \otimes |k_1\rangle^{(3)} \langle i_2|^{(1)} \otimes \langle j_2|^{(2)} \otimes \langle k_2|^{(3)} \overset{\phi_{1.3}^3}{\mapsto} (|k_1\rangle^{(3)} \otimes |k_2\rangle^{(3)})(\langle i_1|^{(1)} \otimes \langle i_2|^{(1)} \otimes \langle j_1|^{(2)} \otimes \langle j_2|^{(2)})$$

For example, let ρ_1 be a three-qubit state $1/2|000\rangle\langle 000| + 1/2|111\rangle\langle 111|$, also known as the GHZ state in three qubit system, then it will be convert into some matrix that may not be square in these matrix folding:

$$\rho_1 = \begin{bmatrix} 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 \end{bmatrix}$$

$$\phi^3_{1.1}(\rho_1) = \begin{bmatrix} 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 \end{bmatrix}$$

Then under a LU transformation ρ will behave differently in these three matrix folding, according to the previous discussion:

$$\phi^3_{1.1}(U_1 \otimes U_2 \otimes U_3(\rho)(U_1 \otimes U_2 \otimes U_3)^\dagger) = (U_1 \otimes U_1)\phi^3_{1.1}(\rho)(U_2 \otimes U_2 \otimes U_3 \otimes U_3)^\dagger$$

$$\phi^3_{1.2}(U_1 \otimes U_2 \otimes U_3(\rho)(U_1 \otimes U_2 \otimes U_3)^\dagger) = (U_2 \otimes U_2)\phi^3_{1.2}(\rho)(U_3 \otimes U_3 \otimes U_1 \otimes U_1)^\dagger$$

$$\phi^3_{1.3}(U_1 \otimes U_2 \otimes U_3(\rho)(U_1 \otimes U_2 \otimes U_3)^\dagger) = (U_3 \otimes U_3)\phi^3_{1.3}(\rho)(U_1 \otimes U_1 \otimes U_2 \otimes U_2)^\dagger$$

Proposition 4.2. If two multipartite quantum states ρ, ρ' on the same Hilbert space are LU equivalent, then the two density operators in any of these type II matrix folding will have the same singular values.

4.4 LU transformations in pure states

4.4.1 LU equivalences in bipartite pure states

We have introduced matrix foldings of a density matrix in the previous section, and now we will apply this technique to determine the LU transformations in bipartite states through some inverse maps of type I.

Let $|\psi\rangle$ be a bipartite state in the Hilbert space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, with computational basis $\{|i\rangle^{(1)} \otimes |j\rangle^{(2)}, 0 \le i \le d_1 - 1, 0 \le j \le d_2 - 1\}$, i.e.

$$|\psi\rangle = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} a_{ij} |i\rangle^{(1)} \otimes |j\rangle^{(2)}$$

$(\phi_0)^{-1} : \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \to \mathbb{C}^{d_1 \times d_2}$, by $|i\rangle^{(1)} \otimes |j\rangle^{(2)} \mapsto |i\rangle^{(1)}\langle j|^{(2)}$ is the inverse map of ϕ_0, we can get a matrix presentation of the state $|\psi\rangle$ through this map:

$$(\phi_0)^{-1}(|\psi\rangle) = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} |i\rangle^{(1)}\langle j|^{(2)}$$

And let $U \otimes V$, where $U \in SU(d_1), V \in SU(d_2)$ be a LU transformation on $|\psi\rangle$, i.e.

$U \otimes V(|\psi\rangle)$. It is equivalent to $U((\phi_0)^{-1}(|\psi\rangle))V^\dagger$ in this inverse map:

$$\begin{aligned}(\phi_0)^{-1}(U \otimes V(|\psi\rangle)) &= (\phi_0)^{-1}(\sum_{i=0}^{d_1-1}\sum_{j=0}^{d_2-1} U|i\rangle^{(1)} \otimes V|j\rangle^{(2)}) \\ &= \sum_{i=0}^{d_1-1}\sum_{j=0}^{d_2-1} U|i\rangle^{(1)}\langle j|^{(2)} V^\dagger \\ &= U((\phi_0)^{-1}(|\psi\rangle))V^\dagger\end{aligned}$$

Theorem 4.3. Two bipartite pure state $|\psi_1\rangle$ and $|\psi_2\rangle$ on the same Hilbert space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ are LU equivalent, if and only if their matrix representations, $(\phi_0)^{-1}(|\psi_1\rangle)$ and $(\phi_0)^{-1}(|\psi_2\rangle)$, have the same singular values.

Proof. It has been proved that, as if $|\psi_1\rangle$ and $|\psi_2\rangle$ are LU equivalent under $U \otimes V \in SU(d_1) \otimes SU(d_2)$, then $U((\phi_0)^{-1}(|\psi_1\rangle))V^\dagger = (\phi_0)^{-1}(|\psi_2\rangle)$, thus they will have the same singular values.

Similarly, if $(\phi_0)^{-1}(|\psi_1\rangle)$ and $(\phi_0)^{-1}(|\psi_2\rangle)$, have the same singular values, it is equivalent to say that $U_0((\phi_0)^{-1}(|\psi_1\rangle))V_0^\dagger = (\phi_0)^{-1}(|\psi_2\rangle)$, for some $U_0 \in SU(d_1), V_0 \in SU(d_2)$. If we apply ϕ_0, the inverse map of $(\phi_0)^{-1}$, then we have: $\phi_0(U_0((\phi_0)^{-1}(|\psi_1\rangle))V_0^\dagger) = U_0 \otimes V_0|\psi_1\rangle = \phi_0(((\phi_0)^{-1}(|\psi_2\rangle))) = |\psi\rangle$, where $U_0 \otimes V_0 \in SU(d_1) \otimes SU(d_2)$. □

Example: Let $|\psi_1\rangle = 0.6|00\rangle + 0.8|12\rangle$ be a state in $\mathbb{C}^2 \otimes \mathbb{C}^3$, and $|\psi_2\rangle = \begin{bmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12/13 & -5/13 \\ 0 & 5/13 & 12/13 \end{bmatrix} |\psi_1\rangle$ be a pure state local unitary equivalent to $|\psi_1\rangle$. We will show that their singular values in the matrix folding under ϕ_0^{-1} are the same with the ones of $|\psi_1\rangle$:

$$|\psi_1\rangle = \begin{bmatrix} 0.6 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0.8 \end{bmatrix}, \text{ with } \phi_0^{-1}(|\psi_1\rangle) = \begin{bmatrix} \sqrt{2}/2 & 0 & 0 \\ 0 & 0 & \sqrt{2}/2 \end{bmatrix}, \text{ and } \phi_0^{-1}(|\psi_1\rangle)\phi_0^{-1}(|\psi_1\rangle)^\dagger = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix},$$

thus singular values are 0.8 and 0.6. After computation, we have $|\psi_2\rangle = \begin{bmatrix} 0.36 \\ 0.2464 \\ -0.59072 \\ 0.48 \\ -0.1848 \\ 0.44304 \end{bmatrix}$, with

$\phi_0^{-1}(|\psi_2\rangle) = \begin{bmatrix} 0.36 & 0.2464 & -0.59072 \\ 0.48 & -0.1848 & 0.44304 \end{bmatrix}$, and $\phi_0^{-1}(|\psi_2\rangle)\phi_0^{-1}(|\psi_2\rangle)^\dagger = \begin{bmatrix} 0.53926 & -0.13445 \\ -0.13445 & 0.46084 \end{bmatrix}$, with the same singular values 0.8 and 0.6.

Remark: In the bipartite case, the singular values of this matrix folding for the pure state will be the same as the coefficients in the maximal entangled states in the same LU equivalent class, $\sum_i \alpha_i |i\rangle \otimes |i\rangle$ [16].

4.4.2 LU equivalence in multipartite pure state

Similar with the case of matrix folding, we can use different matrix foldings under inverse maps of type I to get some result of LU equivalence in multipartite case. For instance, we can setup a series of inverse maps of type I for three partite pure state $|\psi\rangle = \sum_{i,j,k} a_{ijk} |i\rangle^{(1)} \otimes |j\rangle^{(2)} \otimes |k\rangle^{(3)}$ in $\mathbb{C}^{b_1} \otimes \mathbb{C}^{b_2} \otimes \mathbb{C}^{b_3}$:

$(\phi_{0.1}^3)^{-1} : \mathbb{C}^{b_1} \otimes \mathbb{C}^{b_2} \otimes \mathbb{C}^{b_3} \to \mathbb{C}^{b_1 \times b_2 b_3}$, by sending $|i\rangle^{(1)} \otimes |j\rangle^{(2)} \otimes |k\rangle^{(3)} \mapsto |i\rangle^{(1)} \langle j|^{(2)} \otimes \langle k|^{(3)}$

$(\phi_{0.2}^3)^{-1} : \mathbb{C}^{b_1} \otimes \mathbb{C}^{b_2} \otimes \mathbb{C}^{b_3} \to \mathbb{C}^{b_2 \times b_3 b_1}$, by sending $|i\rangle^{(1)} \otimes |j\rangle^{(2)} \otimes |k\rangle^{(3)} \mapsto |i\rangle^{(2)} \langle j|^{(3)} \otimes \langle k|^{(1)}$

$(\phi_{0.3}^3)^{-1} : \mathbb{C}^{b_1} \otimes \mathbb{C}^{b_2} \otimes \mathbb{C}^{b_3} \to \mathbb{C}^{b_3 \times b_1 b_2}$, by sending $|i\rangle^{(1)} \otimes |j\rangle^{(2)} \otimes |k\rangle^{(3)} \mapsto |i\rangle^{(3)} \langle j|^{(1)} \otimes \langle k|^{(2)}$

And the result of a LU transformation $U_1 \otimes U_2 \otimes U_3 \in SU(d_1) \otimes SU(d_2) \otimes SU(d_3)$ acting on $|\psi\rangle$ will be equivalent to the following in these matrix foldings:

$$(\phi_{0.1}^3)^{-1}(U_1 \otimes U_2 \otimes U_3)|\psi\rangle = U_1 (\phi_{0.1}^3)^{-1}(|\psi\rangle)(U_2 \otimes U_3)^\dagger$$

$$(\phi_{0.2}^3)^{-1}(U_1 \otimes U_2 \otimes U_3)|\psi\rangle = U_2 (\phi_{0.2}^3)^{-1}(|\psi\rangle)(U_3 \otimes U_1)^\dagger$$

$$(\phi_{0.3}^3)^{-1}(U_1 \otimes U_2 \otimes U_3)|\psi\rangle = U_3 (\phi_{0.3}^3)^{-1}(|\psi\rangle)(U_1 \otimes U_2)^\dagger$$

Similar with theorem 4.1, we can get anther lemma.

Lemma 4.4. If two multipartite pure states in the same Hilbert space are LU equivalent, then these two states will have the same singular values in any of these inverse map of type I matrix folding.

4.5 LU transformations in mixed states

In general, LU equivalence problems in mixed states are complicated to solve. One approach to deal with these problems is to transform them into the ones in pure states.

Proposition 2 in [17] is an important result that can change problems in mixed states into the ones in pure states. In this proposition, an associated pure state $|\Psi_0\rangle = \sum_{i=1}^{n} \sqrt{p_i}|i\rangle \otimes |\psi_i\rangle$ is formed for any mixed state $\rho = \sum_{i=1}^{n} p_i|\psi_i\rangle\langle\psi_i|, 0 < p_i < 1$ with respect to pure states (eigenvectors) $\{|\psi_i\rangle\}$. The formation of an associated state for a mixed state, ρ, depends on the choice of eigenvectors $\{|\psi_i\rangle\}$. Therefore, if all the nonzero eigenvalues of a mixed state ρ are distinct, the mixed state would have a unique associated pure state; while, if some of the mixed state's nonzero eigenvalues are the same, then its associated states may not be uniquely determined. It is shown in the proposition that if two mixed states ρ_1 and ρ_2, if with unique associated pure state, acting on the same Hilbert space are LU equivalent if and only if their unique associated pure states are LU equivalent to each other.

Here, I would like to provide a different method in matrix folding to handle the uniqueness problem, and prove that the proposition is true even if the associated pure state is not uniquely determined.

Proposition 4.5. For a mixed state $\rho = \sum_{i=1}^{n} p_i|\psi_i\rangle\langle\psi_i|$ with one associated pure state $|\Psi_1\rangle = \sum_{i=1}^{n} \sqrt{p_i}|i\rangle \otimes |\psi_i\rangle$, then any other associated pure state $|\Psi_2\rangle$, if exists, for ρ can be converted into $|\Psi_1\rangle$ through a LU transformation which is composed of a series of identity maps except for the additional partite, i.e. $|\Psi_2\rangle = \sum_{i=1}^{n} \sqrt{p_i}U_0|i\rangle \otimes |\psi_i\rangle = U_0 \otimes I|\Psi_1\rangle$.

It is equivalent to say that all the associated pure states for ρ belong to the same local unitary equivalent class $|\Psi\rangle_{U\otimes I} = \{|\Psi_0\rangle | |\Psi_0\rangle = (\sum_{i=1}^{n} \sqrt{p_i}U|i\rangle \otimes |\psi_i\rangle), \forall U \in U(n)\}$.

Proof.

Lemma 4.6. For any two m by n($m > n$) matrix in the complex field, A and B, if $AA^\dagger = BB^\dagger$, then there exists some unitary matrix $V \in U(n)$, such that $A = BV$.

Proof. $AA^\dagger = BB^\dagger$ suggests that you can find some unitary matrix $U \in U(m)$ for both $AA^\dagger$ and $BB^\dagger$ such that they are simultaneously diagonalized, i.e. $U(AA^\dagger)U^\dagger = U(BB^\dagger)U^\dagger = \Sigma$, where Σ is a diagonal matrix with nonnegative real number on its diagonal(spectral decomposition). Therefore, by the definition of singular value decomposition, you can find a complete set of (left/right) eigenvectors that are shared by both $AA^\dagger$ and $BB^\dagger$, or equivalently speaking, a complete set of left singular vectors for both A and B.

Then A and B will have some singular value decompositions such that they have the same left singular matrix U for A and B, i.e. $A = U\Sigma' V_1^\dagger, B = U\Sigma' V_2^\dagger, U \in U(m), V_1, V_2 \in U(n)$ and Σ' is a m by n matrix all of whose nonzero entries are in the diagonal and $\Sigma'\Sigma'^\dagger = \Sigma$. Therefore, $A = BV$ with $V = V_2 V_1^\dagger \in U(n)$. ☐

For the mixed state $\rho = \sum_{i=1}^{n} p_i|\psi_i\rangle\langle\psi_i|$ with eigenvectors $\{|\psi_i\rangle\}$. It is equivalent to say that $\rho = (\sum_{i=1}^{n} \sqrt{p_i}|\psi_i\rangle\langle i|)(\sum_{j=1}^{n} \sqrt{p_j}|j\rangle\langle\psi_j|) = AA^\dagger$, if we let $A = \sum_{i=1}^{n} \sqrt{p_i}|\psi_i\rangle\langle i|$. Its associated pure state will have the relation: $|\Psi_1\rangle = \sum_{i=1}^n \sqrt{p_i}|i\rangle \otimes |\psi_i\rangle = \phi_0(A)$, where ϕ_0 is the matrix folding introduced in last section.

Then for another spectral decomposition $\rho = \sum_{i=1}^n p_i|\psi_i'\rangle\langle\psi_i'|$ based on $\{|\psi_i'\rangle\}$, ρ will have another associated pure state $|\Psi_2\rangle = \sum_{i=1}^n \sqrt{p_i}|i\rangle \otimes |\psi_i'\rangle$. It is equivalent to say that: $\rho = (\sum_{i=1}^n \sqrt{p_i}|\psi_i'\rangle\langle i|)(\sum_{j=1}^n \sqrt{p_j}|j\rangle\langle\psi_j'|) = (\sum_{i=1}^n \sqrt{p_i}|\psi_i\rangle\langle i|U_0^\dagger)(U_0 \sum_{j=1}^n \sqrt{p_j}|j\rangle\langle\psi_j|) = BB^\dagger$ for some unitary transformation $U_0 \in U(n)$ by Lemma 4.6, if we let $B = \sum_{i=1}^n \sqrt{p_i}|\psi_i\rangle\langle i|U_0^\dagger$.

Similar with the associated pure state $|\Psi_1\rangle$, $|\Psi_2\rangle = \sum_{i=1}^n \sqrt{p_i}|i\rangle \otimes |\psi_i'\rangle = \phi_0(B)$ $= \sum_{i=1}^n \sqrt{p_i}(U_0|i\rangle) \otimes |\psi_i\rangle = U_0 \otimes I|\Psi_1\rangle$ by ϕ_0.

Therefore, the associated pure states of the mixed state $\rho = \sum_{i=1}^n p_i|\psi_i\rangle\langle\psi_i|$ belong to an equivalent class: $|\Psi\rangle_{U\otimes I} = \{|\Psi_0\rangle| |\Psi_0\rangle = U \otimes I(\sum_{i=1}^n \sqrt{p_i}|i\rangle \otimes |\psi_i\rangle), \forall U \in U(n)\}$.

□

Moreover, if we set ρ_0 be the equivalent class $\{M|M = AU, U \in U(n)\} = \phi_0^{-1}(|\Psi\rangle_{U\otimes I})$, with $\rho = \rho_0\rho_0^\dagger$. Therefore, ρ can be map to the associated pure state equivalent class by a special map ϕ with mapping, $\phi(\rho_0\rho_0^\dagger) \mapsto \phi_0(\rho_0)$, based on the idea of ϕ_0.

Suppose ρ' is LU to ρ under some LU transformation, i.e. $\rho' = U_1 \otimes U_2 \otimes \cdots \otimes U_n(\rho)(U_1 \otimes U_2 \otimes \cdots \otimes U_n)^\dagger$, then $\rho' = U_1 \otimes U_2 \otimes \cdots \otimes U_n(\rho_0)(\rho_0)^\dagger(U_1 \otimes U_2 \otimes \cdots \otimes U_n)^\dagger$ which will be map to $U \otimes U_1 \otimes U_2 \otimes \cdots \otimes U_n|\Psi_0\rangle = I_n \otimes U_1 \otimes U_2 \otimes \cdots \otimes U_n|\Psi\rangle_{U\otimes I}$ via the same map ϕ.

Through matrix folding, we set up the equivalence relation between the LU problems in mixed states and pure states. Since there are a lot of other discussion regarding the LU equivalence in mutipartite pure states, like Kraus [16], this method provides a new perspective to analysis the LU equivalence in mixed states.

Chapter 5

Algorithms to determine the local unitary equivalence in two partite mixed states

In the last chapter, we have described the local unitary transformations in the computational basis and its behavior in different matrix folding. Here, we will use a special basis for a given quantum state, and then determine the conditions if two mixed states could be mutually transform into each other. The reason that we want to analyze two partite mixed state is because that a three partite pure state can be reduced into a two partite mixed state with equivalent behavior, thus a complete study of two partite mixed state helps to solve the LU problem in three partite pure states [1]. Moreover, any multipartite mixed state can be analysis by a similar approach by separated into two parts. Therefore, the result of two partite mixed state is very useful in all the LU problems.

5.1 Invariant polynomials in bipartite mixed states

Gell-Mann type basis is a special type of basis that consists of orthonormal and hermitian elements. All the entries in this matrix representation will be real numbers, this property restricts the field for the matrix and simplified our analysis and computation in practice.

5.1.1 The Gell-Mann type basis

Let ρ be some density operator acting on a Hilbert space $\mathcal{H}$ of dimension d equipped with the standard inner product $\langle u, v\rangle = uv^{\dagger}$. On the space of linear operators on $\mathcal{H}$ the standard inner product is $\langle f, g\rangle = tr(fg^{\dagger})$. Assume that the subspace $\mathcal{A}$ of hermitian operators on $\mathcal{H}$ is of dimension N, then ρ is a special positive operator in this space with $tr(\rho) = 1$.

We fix an orthonormal basis $\{\lambda_i\}$ of $\mathcal{A}$ such that $tr(\lambda_i \lambda_j^\dagger) = \delta_{ij}$. In particular, we can assume for one partite case that λ_0 is the identity operator with certain scale, which is restricted by the assumption. In the case of $d = 2$, the Pauli spin matrices up to scale are such an example: $\lambda_0 = I_2/\sqrt{2}$, $\lambda_1 = (|0\rangle\langle 0| - |1\rangle\langle 1|)/\sqrt{2}$, $\lambda_2 = (|0\rangle\langle 1| + |1\rangle\langle 0|)/\sqrt{2}$, and $\lambda_3 = (i|0\rangle\langle 1| - i|1\rangle\langle 0|)/\sqrt{2}$. In general, they can be chosen as the generalized Pauli spin matrices or Gell-Mann type matrices, which are hermitian and traceless except λ_0. Then any ρ can be expressed as

$$\rho = \sum_{i=0}^{d^2-1} u_i \lambda_i = \frac{1}{d} I_d + \sum_{i=1}^{d^2-1} u_i \lambda_i, \qquad u_i \in \mathbb{R}. \tag{5.1}$$

Here all the coefficients u_i are real numbers.

For the same one partite state ρ acting on Hilbert space $\mathcal{H}$ of dimension d like last section, we fix an orthonormal basis $\{\lambda_i\}$ of $\mathcal{A}$ such that $tr(\lambda_i \lambda_j^\dagger) = \delta_{ij}$. In particular, we can assume for one partite case that λ_0 is the identity operator with certain scale, which is restricted by the assumption. In the case of $d = 2$, the Pauli spin matrices up to scale are such an example: $\lambda_0 = I_2/\sqrt{2}$, $\lambda_1 = (|0\rangle\langle 0| - |1\rangle\langle 1|)/\sqrt{2}$, $\lambda_2 = (|0\rangle\langle 1| + |1\rangle\langle 0|)/\sqrt{2}$, and $\lambda_3 = (i|0\rangle\langle 1| - i|1\rangle\langle 0|)/\sqrt{2}$. In general, they can be chosen as the generalized Pauli spin matrices or Gell-Mann type matrices, which are hermitian and traceless except λ_0. Then any ρ can be expressed as

$$\rho = \sum_{i=0}^{d^2-1} u_i \lambda_i = \frac{1}{d} I_d + \sum_{i=1}^{d^2-1} u_i \lambda_i, \qquad u_i \in \mathbb{R}. \tag{5.2}$$

Here all the coefficients u_i are real numbers.

The matrix representation of ρ works multi-partite quantum states as well. In fact, the orthogonal basis for the tensor product spaces be taken as the tensor product of the Gell-Mann bases on the individual factors. For instance, let ρ be the density matrix of a mixed bipartite state on $\mathcal{H}_{d_1} \otimes \mathcal{H}_{d_2}$, and $\{\lambda_i^{(k)}, 0 \leq i \leq d_k^2 - 1, k = 1, 2\}$ be the Gell-Mann bases for each partite, then ρ can be expressed in Gell-Mann basis in the following form:

$$\begin{aligned} \rho = & \frac{1}{d_1 d_2} I_{d_1 d_2} + \sum_{i=1}^{N_1} u_i \lambda_i^{(1)} \otimes \lambda_0^{(2)} + \sum_{j=1}^{N_2} v_j \lambda_0^{(1)} \otimes \lambda_j^{(2)} \\ & + \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} w_{ij} \lambda_i^{(1)} \otimes \lambda_j^{(2)}, \quad N_k = d_k^2 - 1, k = 1, 2 \end{aligned} \tag{5.3}$$

where

$$u_i = \langle \rho, \lambda_i^{(1)} \otimes \lambda_0^{(2)} \rangle = tr(\rho(\lambda_i^{(1)} \otimes \lambda_0^{(2)}))$$
$$v_j = \langle \rho, \lambda_0^{(1)} \otimes \lambda_j^{(2)} \rangle = tr(\rho(\lambda_0^{(1)} \otimes \lambda_j^{(2)}))$$
$$w_{ij} = \langle \rho, \lambda_i^{(1)} \otimes \lambda_j^{(2)} \rangle = tr(\rho(\lambda_i^{(1)} \otimes \lambda_j^{(2)})).$$

Since all further discussion in this chapter will generally based on these special basis, it is convenient to make some definition before hands:

Definition. For the density matrix ρ of a bipartite mixed state on $H_{d_1} \otimes H_{d_2}$ with respect to the Gell-Mann basis $\{\lambda_i^{(1)} \otimes \lambda_j^{(2)}, 0 \leq i \leq d_1^2 - 1, 0 \leq j \leq d_2^2 - 1\}$, we denote N_k as $d_k^2 - 1, k = 1, 2$, $u(\rho)$ as $[u_1, u_2, \cdots, u_{N_1}]^T$, $v(\rho)$ as $[v_1, v_2, \cdots, v_{N_2}]^T$, and $W(\rho)$ as the N_1 by N_2 matrix such that the element in its ith row, jth column will be w_{ij}, where u_i, v_j, w_{ij} are the corresponding coefficients in this basis shown in equation 5.3 that, $1 \leq i \leq N_1, 1 \leq j \leq N_2$. Thus, each mixed bipartite quantum state with density matrix ρ is associated with corresponding *triple* $(W(\rho), u(\rho), v(\rho))$. Two mixed bipartite quantum state are the same if and only if their triple are the same.

Lemma 5.1. Suppose $\{v_i, 1 \leq i \leq N = d^2 - 1\}$ is an orthonormal traceless and hermitian basis of $sl_d(\mathbb{C})$ satisfying $\langle v_i, v_j \rangle = tr\{v_i v_j^\dagger\} = \delta_{ij}$, for all $1 \leq i, j \leq N$, and U is some element in $SU(N)$, then $\{v_i^U, 1 \leq i \leq N\}$ will also been an orthonormal traceless and hermitian basis of $sl_d(\mathbb{C})$. Moreover, if $v_i^U = \sum_{j=1}^N m_{ij} v_j$, for some m_{ij} in $\mathbb{R}$, then m_{ij} satisfies $\sum_{k=1}^N m_{ik} \bar{m_{jk}} = \sum_{k=1}^N m_{ik} m_{jk} = \delta_{ij}$, for all $1 \leq i, j \leq N$.

$$i.e. \quad \begin{bmatrix} v_1^U \\ v_2^U \\ \cdots \\ v_N^U \end{bmatrix} = \begin{bmatrix} U v_1 U^\dagger \\ U v_2 U^\dagger \\ \cdots \\ U v_N U^\dagger \end{bmatrix} = M \begin{bmatrix} v_1 \\ v_2 \\ \cdots \\ v_N \end{bmatrix}, M \in SO(N).$$

Proof. For any unitary matrix U, v_i^U is still in $sl_n(\mathbb{C})$, thus it can be expressed as a linear combination of the traceless hermitian basis as $\sum_{j=1}^N m_{ij} v_j$, for some m_{ij} in $\mathbb{C}$. Moreover, as v_i are hermitian, v_i^U is also hermitian, $v_i^U = U v_i U^\dagger = U v_i^\dagger U^\dagger = (v_i^U)^\dagger$. thus, $v_i^U = (v_i^U)^\dagger = \sum_{j=1}^N m_{ij} v_j = \sum_{j=1}^N \bar{m_{ij}} v_j \Rightarrow m_{ij} = \bar{m_{ij}}$, thus m_{ij} are real numbers, for all $1 \leq i, j \leq N$. And $tr(v_i^U v_j^U) = tr(U v_i v_j U^\dagger) = tr(v_i v_j U^\dagger U) = tr(v_i v_j)$, which indicate:

$$tr((\sum_{k=1}^N m_{ik} v_k)(\sum_{l=1}^N m_{jl} v_l)) = \sum_{k=1}^N \sum_{l=1}^N m_{ik} m_{jl}\ tr(v_k v_l)$$

$$= \sum_{k=1}^{N} m_{ik} m_{jk} = tr(v_i v_j) = \delta_{ij} \Rightarrow \sum_{k=1}^{N} m_{ik} m_{jk} = \delta_{ij}$$

$$i.e. \begin{bmatrix} v_1^U \\ v_2^U \\ \cdots \\ v_N^U \end{bmatrix} = \begin{bmatrix} Uv_1U^\dagger \\ Uv_2U^\dagger \\ \cdots \\ Uv_NU^\dagger \end{bmatrix} = M \begin{bmatrix} v_1 \\ v_2 \\ \cdots \\ v_N \end{bmatrix}, M \in SO(N). \qquad \square$$

Remark. The conclusion in Lemma 5.1 is a necessary condition in general, as even if there exists M in $O(N)$, satisfying the relation the lemma, there does not always exist such a unitary matrix that $[v_1^U, v_2^U, ..., v_N^U]^T = M[v_1, v_2, ..., v_N]$.

5.1.2 Local unitary equivalence

Theorem 5.2. For any two mixed bipartite quantum state on $\mathcal{H}_{d_1} \otimes \mathcal{H}_{d_2}$ with density ρ' and ρ associated with $(W(\rho), u(\rho), v(\rho))$ and $(W(\rho'), u(\rho'), v(\rho'))$, respectively, if ρ is local unitary equivalent to ρ', then there exists A in $SO(N_1)$, B in $SO(N_2)$, such that $u(\rho') = A^T u(\rho)$, $v(\rho') = B^T v(\rho)$, $W(\rho') = A^T W(\rho) B$.

Proof. Under local unitary transformation $U_1 \otimes U_2$, bipartite mixed state ρ on $H_{d_1} \otimes H_{d_2}$ will become:

$$\rho' = \rho^{U_1 \otimes U_2} = \frac{1}{d_1 d_2} I_{d_1 d_2} + \sum_{i=1}^{N_1} u_i (\lambda_i^{(1)})^{U_1} \otimes \lambda_0^{(2)}$$

$$+ \sum_{j=1}^{N_2} v_j \lambda_0^{(1)} \otimes (\lambda_j^{(2)})^{U_2} + \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} w_{ij} (\lambda_i^{(1)})^{U_1} \otimes (\lambda_j^{(2)})^{U_2}$$

From Lemma 5.1, it is shown that there exists some $a_{ij}, b_{ij} \in \mathbb{R}$ such that $(\lambda_i^{(1)})^{U_1} = \sum_{j=1}^{N_1} a_{ij} \lambda_j^{(1)}$, $(\lambda_i^{(2)})^{U_2} = \sum_{j=1}^{N_2} b_{ij} \lambda_j^{(2)}$, satisfying $\sum_{k=1}^{N_1} a_{ik} a_{jk} = \sum_{k=1}^{N_2} b_{ik} b_{jk} = \delta_{ij}$.

$$i.e. \quad \begin{bmatrix} (\lambda_1^{(1)})^{U_1} \\ (\lambda_2^{(1)})^{U_1} \\ \cdots \\ (\lambda_{N_1}^{(1)})^{U_1} \end{bmatrix} = A \begin{bmatrix} \lambda_1^{(1)} \\ \lambda_2^{(1)} \\ \cdots \\ \lambda_{N_1}^{(1)} \end{bmatrix}, \begin{bmatrix} (\lambda_1^{(2)})^{U_2} \\ (\lambda_2^{(2)})^{U_2} \\ \cdots \\ (\lambda_{N_2}^{(2)})^{U_2} \end{bmatrix} = B \begin{bmatrix} \lambda_1^{(2)} \\ \lambda_2^{(2)} \\ \cdots \\ \lambda_{N_2}^{(2)} \end{bmatrix}$$

for some $A \in O(N_1), B \in O(N_2)$, then,

$$\sum_{i=1}^{N_1} u_i (\lambda_i^{(1)})^{U_1} \otimes \lambda_0^{(2)} = \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} u_i a_{ij} \lambda_j^{(1)} \otimes \lambda_0^{(2)}$$

$$= \sum_{i=1}^{N}(\sum_{j=1}^{N_2} u_j a_{ji})\lambda_i^{(1)} \otimes \lambda_0^{(2)}, \quad i.e.\ u(\rho^{U_1 \otimes U_2}) = A^T u(\rho)$$

$$\sum_{i=1}^{N_1} v_i \lambda_0^{(1)} \otimes (\lambda_i^{(2)})^{U_2} = \sum_{i=1}^{N_1}\sum_{j=1}^{N_2} v_i b_{ij} \lambda_0^{(1)} \otimes \lambda_j^{(2)}$$

$$= \sum_{i=1}^{N_1}(\sum_{j=1}^{N_2} v_j b_{ji})\lambda_0^{(1)} \otimes \lambda_j^{(2)}, \quad i.e.\ u(\rho^{U_1 \otimes U_2}) = B^T v(\rho)$$

$$\sum_{i=1}^{N_1}\sum_{j=1}^{N_2} w_{ij}(\lambda_i^{(1)})^{U_1} \otimes (\lambda_j^{(2)})^{U_2} = \sum_{k=1}^{N_1}\sum_{l=1}^{N_2} w_{kl}(\sum_{i=1}^{N_1} a_{ki}\lambda_i) \otimes (\sum_{j=1}^{N_2} b_{lj}\lambda_j)$$

$$= \sum_{i=1}^{N_1}\sum_{j=1}^{N_2}(\sum_{k=1}^{N_1}\sum_{l=1}^{N_2} a_{ki} w_{kl} b_{lj})\ \lambda_i \otimes \lambda_j,$$

Since the matrix M preserves the bilinear form $tr(v_i v_j)$, the matrix M is orthogonal.

$$i.e. \quad W(\rho^{U_1 \otimes U_2}) = A^T W(\rho) B$$

Theorem 5.2 gives us a necessary condition in general for the reason in the remark of Lemma 1. But it is a sufficient and necessary condition when it is a two qubit case.

Theorem 5.3. For two 2-qubit quantum state ρ' and ρ associated with $(W(\rho), u(\rho), v(\rho))$ and $(W(\rho'), u(\rho'), v(\rho'))$, respectively. Then ρ is local unitary equivalent to ρ' if and only if there exists A,B in $SO(3)$, such that $u(\rho') = A^T u(\rho)$, $v(\rho') = B^T v(\rho)$, $W(\rho') = A^T W(\rho) B$.

Proof. It only needs to prove the backwards. Suppose there exists A, B in $O(3)$ such that $u(\rho') = A^T u(\rho)$, $v(\rho') = B^T v(\rho)$, $W(\rho') = A^T W(\rho) B$. And the Gell Mann Type basis of ρ and ρ' be the Pauli matrices up to scale, i.e. ρ, ρ' are in $V_3 = 1/2 I_2 + Span_{\mathbb{R}}\{\sigma_1, \sigma_2, \sigma_3\}$.

Set up a lie group homomorphism by considering the group action $U(2)$ on $\{\sigma_1, \sigma_2, \sigma_3\}$ by adjoint operation:

$$\phi : U(2) \to GL(3, \mathbb{R}), \text{ with } U \mapsto Ad_U, \quad \forall U \in U(2)$$

It is equivalent to consider this homomorphism in the lie algebra representation:

$$\psi : u(2) \to gl(3, \mathbb{R}), \text{ with } u \mapsto ad_u, \quad \forall u \in u(2)$$

By definition, $u(2) = \{A \in M(2, \mathbb{C}) | A = -A^*\} = Span_{\mathbb{R}}\{h_1 = ie_{11},\ h_2 = ie_{22},\ a = e_{12} + e_{21},$

$b = ie_{12} - ie_{21}\}$. The map is as following:

$$ad_{h_1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}, \quad ad_{h_2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$ad_a = \begin{bmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ -2 & 0 & 0 \end{bmatrix}, \quad ad_b = \begin{bmatrix} 0 & 2 & 0 \\ -2 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Notice that $Span_{\mathbb{R}}\{ad_{h_1}, ad_{h_2}, ad_a, ad_b\} = so(3,\mathbb{R})$, i.e. $im\psi = so(3)$. Equivalently, $im\phi = SO(3)$, it suggests that if there exists A, B in $SO(3)$ that $u(\rho') = A^T u(\rho)$, $v(\rho') = B^T v(\rho)$, and $W(\rho') = A^T W(\rho)B$. Then there exists some element U_1, U_2 in $U(2)$ such that $\phi(U_1) = A$, $\phi(U_2) = B$, thus $U_1 \otimes U_2 \rho (U_1 \otimes U_2)^\dagger = \rho'$. □

5.2 The normal form of a bipartite mixed state

To classify the local unitary equivalence of mixed bipartite quantum states, we introduce a new concept, *the Normal Form of Bipartite Quantum States*:

Definition 5.4. For a bipartite quantum state ρ in $H_{d_1} \otimes H_{d_2}$, associated with $(W(\rho), u(\rho), v(\rho))$, this form defined as the Smith normal form of $\lambda W(\rho) + u(\rho)v(\rho)^T$, a $N_1 = d_1^2 - 1$ by $N_2 = d_2^2 - 1$ matrix such that all its nonzero elements are on its diagonal and they divides each other from top to bottom and all its zero elements stay at the bottom [24, 25, 26].

$$\text{i.e.} \quad \begin{bmatrix} d_1(\lambda) & 0 & \cdots & 0 & 0 & \cdots \\ 0 & d_2(\lambda) & \cdots & 0 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_m(\lambda) & 0 & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}_{N \times M}$$

Here, $d_i(\lambda) \in \mathbb{C}[\lambda]$ such that $d_i(\lambda) | d_{i+1}(\lambda)$, $\forall 1 \leq i \leq m$ and $m \leq N$.

The smith normal form of the matrix $\lambda W(\rho) + u(\rho)$ with all entries in its principal ideal domain $\mathbb{C}[\lambda]$ is uniquely determined by definition. It is obtained though left and right multiplication of some invertible matrices $P(\lambda) \in Gl(N_1, \mathbb{C}[\lambda])$, $Q_1 \in Gl(N_2, \mathbb{C}[\lambda])$ with nonzero scale determinant to $\lambda W(\rho) + u(\rho)$, i.e. $P(\lambda)(\lambda W(\rho) + u(\rho))Q(\lambda)$.

5.2.1 Result in the normal form of states

Proposition 5.5. For any bipartite quantum state ρ' and ρ associated with $(W(\rho), u(\rho), v(\rho))$ and $(W(\rho'), u(\rho'), v(\rho'))$. If ρ is local unitary equivalent to ρ', then the normal forms of ρ and ρ' will be the same.

Lemma 5.6. For any matrices $W, W' \in M_N(\mathbb{C})$, column vectors u, v, u' and $v' \in \mathbb{C}^N$, there exists $U_1, U_2 \in U(N)$, such that $U_1 W U_2^\dagger = W', u' = U_1 u$ and $v' = U_2 v$ if and only if u, u' have the same length, i.e. $u^\dagger u = u'^\dagger u'$ and there exists $V_1, V_2 \in U(N)$ such that $V_1 W V_2^\dagger = W'$ and $V_1 u v^\dagger V_2^\dagger = u' v'^\dagger$.

Proof. The former statement naturally leads to the latter one, we only need to prove the backwards. Suppose $u^\dagger u = u'^\dagger u'$ and there exists $V_1, V_2 \in U(N)$, that $u^\dagger u = u'^\dagger u'$, $V_1 W V_2^\dagger = W'$ and $V_1 u v^\dagger V_2^\dagger = u' v'^\dagger$:

$V_1 u v^\dagger V_2^\dagger = u' v'^\dagger$ suggests that $V_1 u = (\frac{v'^\dagger V_2 v}{v^\dagger v}) u'$. If we denotes the coefficient of u' as α, then α be a scale with length 1, under the assumption u, u' have the same length.

Similarly, $V_1 u v^\dagger V_2^\dagger = u' v'^\dagger$ suggests that $(V_2 v)^\dagger = (\frac{u^\dagger V_1^\dagger u'}{u^\dagger u}) v'^\dagger$ and β be a scale with length 1, if we denote the coefficient of $v'^\dagger$ as β. And α and β are inverse to each other, since $V_1 u v^\dagger V_2^\dagger = \alpha u' \beta v'^\dagger = u' v'$.

Let $U_1 = \beta V_1$, $U_2 = \beta V_2$, then $U_1 U_1^\dagger = (\beta\bar{\beta}) V_1 V_1^\dagger = U_2 U_2^\dagger = I$, i.e. $U_1, U_2 \in U(N)$, then, U_1, U_2 be in $U(N)$, and $U_1 W U_2^\dagger = W', u' = U_1 u$ and $v' = U_2 v$

□

Lemma 5.7. For any matrices X, X', Y and $Y' \in M_N(\mathbb{C})$, there exists $U_1, U_2 \in U(N)$, such that $U_1 X U_2^\dagger = X', U_1 Y U_2^\dagger = Y'$ if and only if there exists $U_1, U_2 \in U(N)$, such that $U_1(X + \lambda Y) U_2^\dagger = (X' + \lambda Y')$.

Proof. Suppose there exists $U_1, U_2 \in U(N)$, that $U_1 X U_2^\dagger = X'$, $U_1(\lambda Y) U_2^\dagger = \lambda U_1 Y U_2^\dagger = \lambda Y'$, thus $U_1(X + \lambda Y) U_2^\dagger = (X' + \lambda Y')$.

Proof of backwards. Suppose there exists $U_1, U_2 \in U(N)$, such that $U_1(X + \lambda Y) U_2^\dagger = (X' + \lambda Y')$. Consider the limit of this structure:

$$\lim_{\lambda \to 0} U_1(X + \lambda Y) U_2^\dagger = \lim_{\lambda \to 0} U_1 X U_2^\dagger = X';$$

$$\lim_{\lambda \to \infty} \frac{U_1(X + \lambda Y) U_2^\dagger}{\lambda} = \lim_{\lambda \to 0} U_1(\frac{X}{\lambda} + Y) U_2^\dagger = Y'$$

, where $\frac{X}{\lambda} \to 0$, as $\lambda \to \infty$. □

Proof of the propostion. By Theorem 5.2, we know if ρ is equivalent to ρ', then there exists U_1, U_2 in $SO(N)$, such that $u(\rho') = U_1^T u(\rho)$, $v(\rho') = U_2^T v(\rho)$, $W(\rho') = U_1^T W(\rho) U_2$. By lemma 5.4., we get $V_1 W(\rho) V_2^\dagger = W(\rho')$ and $V_1 u(\rho) v(\rho)^\dagger V_2^\dagger = u(\rho') v(\rho')^\dagger$ for some $V_1, V_2 \in U(N)$.

By lemma 5.6, it is suggested that there exists $U_1, U_2 \in U(N)$, such that $U_1(\lambda W(\rho) + u(\rho)v(\rho)^\dagger)U_2^\dagger = \lambda W(\rho') + u(\rho')v(\rho')^\dagger$, thus they will have the same normal form, i.e. they have the same invariant polynomials. □

5.2.2 Examples for the invariant polynomials

$$\frac{1}{26}\begin{bmatrix} 9 & 5-i & -4+i & 1+4i \\ 5+i & 2 & 5+6i & 5-i \\ -4-i & 5-6i & 6 & 7 \\ 1-4i & 5+i & 7 & 9 \end{bmatrix}, \frac{1}{52}\begin{bmatrix} 13 & 2 & 12 & -1 \\ -2 & 5 & -2 & -1 \\ 1 & -9 & 6 & -2 \\ 0 & 2 & 10 & 4 \end{bmatrix}$$

After changing the basis through our algorithm, we get the matrix in our hermitian Basis, and its normal form will been as following:

$$\begin{bmatrix} \frac{5}{52}\lambda - \frac{1}{676} & -\frac{1}{26}\lambda - \frac{3}{338} & -\frac{1}{52}\lambda + \frac{1}{1352} \\ -\frac{9}{52}\lambda + \frac{1}{1352} & \frac{3}{26}\lambda + \frac{3}{676} & -\frac{1}{26}\lambda - \frac{1}{2704} \\ \frac{1}{26}\lambda & \frac{5}{26}\lambda & \frac{1}{13}\lambda \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^2 - \frac{139}{2236}\lambda \end{bmatrix}$$

We can get a local unitary equivalent state by some local unitary transformation, $U_1 \otimes U_2 \rho (U_1 \otimes U_2)^\dagger$, and go through the whole process again, here we use $U_1 \otimes U_2 = \begin{bmatrix} 3/5 & 4/5i \\ -4/5i & -3/5 \end{bmatrix} \otimes \begin{bmatrix} 5/13 & 12/13 \\ -12/13 & 5/13 \end{bmatrix}$. Go through the same steps to the new state, the representation in our hermitian basis is given and the normal form is also computed and listed below, it comes out that the normal form of our new state by local unitary transformation is the same as that of the origin state:

$$\begin{bmatrix} \frac{1}{4} & \frac{601}{4394} & -\frac{417}{2197} & -\frac{1}{52} \\ \frac{7}{650} & \frac{28933}{219700} & -\frac{15893}{109850} & -\frac{103}{1300} \\ -\frac{1}{52} & -\frac{1791}{8788} & -\frac{183}{4394} & \frac{1}{26} \\ \frac{12}{325} & -\frac{6653}{109850} & -\frac{9349}{109850} & \frac{1}{325} \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^2 - \frac{139}{2236}\lambda \end{bmatrix}$$

Example 2. A random mixed two partite quantum state ρ in $\mathcal{H}_2 \otimes \mathcal{H}_3$ generated by maple. Its representation under our hermitian basis can be obtained through the same procedures:

$$\frac{1}{40}\begin{bmatrix} 9 & 6-I & 8+5I & 5+4I & 2+5I & 3+6I \\ 6+I & 4 & 8-I & 4-I & 8I & 3I \\ 8-5I & 8+I & 5 & 2+6I & 2-I & 3+2I \\ 5-4I & 4+I & 2-6I & 9 & 3+6I & 2I \\ 2-5I & -8I & 2+I & 3-6I & 6 & 8+4I \\ 3-6I & -3I & 3-2I & -2I & 8-4I & 7 \end{bmatrix}$$

$$\begin{bmatrix} \frac{\sqrt{6}}{12} & \frac{9}{80} & \frac{1}{16} & \frac{1}{10} & \frac{7}{80} & \frac{1}{5} & \frac{3}{80} & \frac{1}{20} & \frac{\sqrt{3}}{120} \\ -\frac{\sqrt{6}}{120} & \frac{3}{80} & -\frac{7}{80} & \frac{1}{10} & \frac{3}{80} & 0 & -\frac{1}{16} & \frac{1}{80} & \frac{\sqrt{3}}{240} \\ \frac{\sqrt{6}}{30} & \frac{3}{40} & \frac{3}{40} & \frac{1}{16} & 0 & \frac{1}{40} & \frac{1}{20} & \frac{1}{16} & -\frac{\sqrt{3}}{240} \\ -\frac{\sqrt{6}}{120} & -\frac{1}{20} & -\frac{1}{40} & -\frac{3}{20} & -\frac{1}{80} & -\frac{1}{40} & -\frac{1}{40} & \frac{1}{20} & -\frac{\sqrt{3}}{30} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & ... & 0 \\ 0 & \lambda & 0 & 0 & ... & 0 \\ 0 & 0 & \lambda^2 & 0 & ... & 0 \end{bmatrix}$$

Similarly, a local unitary equivalent state will be generated by some local unitary transformation: $U_1 \otimes U_2 = \begin{bmatrix} 3/5 & 4/5i \\ -4/5i & -3/5 \end{bmatrix} \otimes \begin{bmatrix} 5/13 & 12i/13 & 0 \\ -12i/13 & -5/13 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} \frac{\sqrt{6}}{12} & -\frac{9}{80} & \frac{215}{2704} & \frac{1}{260} & \frac{227}{1040} & \frac{1}{260} & -\frac{111}{1040} & \frac{31}{3380} & \frac{\sqrt{3}}{120} \\ \frac{7\sqrt{6}}{120} & -\frac{3}{80} & -\frac{817}{338000} & \frac{41}{6500} & \frac{27}{2000} & -\frac{3}{100} & -\frac{3199}{26000} & \frac{23897}{992875} & \frac{37\sqrt{3}}{1200} \\ -\frac{\sqrt{6}}{30} & \frac{3}{40} & -\frac{657}{6760} & \frac{23}{1040} & -\frac{3}{130} & \frac{1}{104} & \frac{1}{13} & -\frac{25}{2704} & \frac{\sqrt{3}}{240} \\ -\frac{\sqrt{6}}{120} & \frac{1}{20} & \frac{9403}{169000} & -\frac{51}{500} & -\frac{493}{26000} & -\frac{71}{2600} & \frac{107}{1000} & \frac{4501}{84500} & -\frac{\sqrt{3}}{75} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & ... & 0 \\ 0 & \lambda & 0 & 0 & ... & 0 \\ 0 & 0 & \lambda^2 & 0 & ... & 0 \end{bmatrix}$$

It is shown from the result that the local unitary equivalent states will have the same normal form. However, use the normal form to determine the local unitary transformation between two

5.3 Other method to determine the conditions

5.3.1 Algorithm through Specht's theorem

Definition 5.8. Two matrices A and B are said to be unitarily equivalent if there exists a Unitary matrix U, such that $U(A)U^{\dagger} = B$. And a word of two variables x and y are defined to be $W(x, y) = x^{m_1}y^{m_2}x^{m_3}y^{m_4} \cdots x^{m_i} \cdots y^{m_p}$, where $m_i, 1 \leq i \leq p$ are non-negative integers, such that the degree of the word is $m_1 + m_2 + \cdots + m_p$.

Use these definitions, we can introduce the Specht's theorem:

Two matrices A and B are unitarily equivalent if and only if tr W(A, A*) = tr W(B, B*) for all words W. This is a sufficient and necessary condition to check if two matrices are unitarily equivalent discovered by Wilhelm Specht in 1940, and we can extend this theorem to our case.

Theorem 5.9. For two bipartite quantum state ρ' and ρ associated with $(W(\rho), u(\rho), v(\rho))$ and $(W(\rho'), u(\rho'), v(\rho'))$. If ρ is local unitary equivalent to ρ', then $tr((W(\rho) + \lambda u(\rho)v(\rho)^\dagger)(W(\rho)^\dagger + \lambda v(\rho)u(\rho)^\dagger))^n = tr((W(\rho') + \lambda u(\rho')v(\rho')^\dagger)(W(\rho')^\dagger + \lambda v(\rho')u(\rho')^\dagger))^n$ for all positive integer n.

Proof. It has been proved that, there exists some unitary matrices A, B, such that $AW(\rho)B^\dagger = W(\rho')$, $Au(\rho) = u(\rho')$, $Bv(\rho) = v(\rho')$, or $A(W(\rho) + \lambda u(\rho)v(\rho)^\dagger)B^\dagger = W(\rho') + \lambda u(\rho')v(\rho')^\dagger$, for any λ. Then it would satisfy the Specht's theorem. □

This theorem is a strong condition which gives us a series of invariant polynomials in terms of λ instead of numbers, which could be translate into ordinary trace invariants. Ex. $tr((X_1 + \lambda Y_1)(X_1 + \lambda Y_1)^\dagger) = tr((X_2 + \lambda Y_2)(X_2 + \lambda Y_2)^\dagger)$ is one condition, it is equivalent to $tr(X_1 X_1^\dagger) = tr(X_2 X_2^\dagger)$, $tr(X_1 Y_1^\dagger + Y_1 X_1^\dagger) = tr(X_2 Y_2^\dagger + Y_2 X_2^\dagger)$ and $tr(Y_1 Y_1^\dagger) = tr(Y_2 Y_2^\dagger)$; Similarly, $tr((X_1 + \lambda Y_1)(X_1^\dagger + \lambda Y_1^\dagger))^2 = tr((X_2 + \lambda Y_2)(X_2^\dagger + \lambda Y_2^\dagger))^2$ is equivalent to $tr(X_1 X_1) = tr(X_2 X_2)$, $tr(X_1 Y_1 + Y_1 X_1) = tr(X_2 Y_2 + Y_2 X_2)$ and $tr(Y_1 Y_1) = tr(Y_2 Y_2)$.

In general, there will be infinite many invariants that needs to check according to the lemma. Fortunately, in the practice, most of the invariants are duplicated and could be reduced to finite some.

REFERENCES

[1] M. A. Neilsen and I. L. Chuang. *"Quantum Computation and Quantum Information".* Cambridge University Press(2000).

[2] C.E. Shannon, W. Weaver. *"The Mathematical Theory of Communication".* Univ of Illinois Press(1949).

[3] *"The Nobel Prize in Physics 1921".* Nobel Foundation. Retrieved 2013-03-16.

[4] L. de Broglie *Nobel Lecture.* **12**, (1929).

[5] A.I. Ekimov et al. *Solid State Communications.* **56**, 11, 921-924 (1985).

[6] T. D. Ladd et al. *nature.* **464**, 4(2010)

[7] S. Barz, J. F. Fitzsimons, E. Kashefi and P. Walther *nature* **81**, 865 (2009).

[8] A. K. Ekert *Phys. Rev. Lett.* **67**, 661 (1991)

[9] A. Peres. *Phys. Rev. Lett.* **77**, 1413-1415 (1996)

[10] M. Horodecki et al. *Physics Letters A.* **223**, 1-8 (1996).

[11] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. *Rev. Mod. Phys.* **81**, 865 (2009).

[12] C. Meyer *"Matrix Analysis and Applied Linear Algebra"* SIAM(2000).

[13] H. Smith. Phil. *Trans. R. Soc. Lond.* **151**, 1: 293326, (1861).

[14] R. Raussendorf and H. J. Briegel. *Phys. Rev. Lett.* **86**, 5188 (2001).

[15] L. De Lathauwer. *SIAM J. MATRIX ANAL. APPL.* **20**, 4, 1253-1278(2000)

[16] C. Kruszynska and B. Kraus. *Phys. Rev. A.* **79**, 052304(2009).

[17] J. Li, C. Qiao *J. Phys. A: Math. Theor.* **46**, 075301 (2013)

[18] C. H. Bennett, David P. DiVincenzo, J. Smolin, W. Wootters. *Phys. Rev. A.* **54**, 3824-3851(1996).

[19] J. Jing, et al. *Phys. Rev. Lett.* **90**, 167903(2003).

[20] Joe, Kilian. *Proc. ACM STOC* **88**, pp.20-31(1988) .

[21] C. Zhou, T. G. Zhang, S.-M. Fei, N. Jing, and X. Li-Jost, *Phys. Rev. A.* **86**, 010303(R) (2012).

[22] C.H. Bennett, H. Bernstein, S. Popescu, and B. Schu- macher. *Phys. Rev. A.* **53**, 2046-2052 (1996).

[23] Yu. G. Makhlin, *Quantum Info. Proc.* **1**, 243-254 (2002).

[24] F.R.Gantmacher. "Matrix Theory". 2nd Edition, Vol. 1, (Chelsea Publishing Company, 1990).

[25] Jacobson, Nathan. "Basic Algebra I". 2nd Edition, (W.H. Freeman and Company, 1985).

[26] R. A. Horn and C. R. Johnson. "Matrix Analysis". (Cambridge University Press, Cambridge, England, 1990).

[27] T.G. Zhang, M.J. Zhao, S.M. Fei and X. Li-Jost, *Phys. Rev. A*. **88**, 042304 (2013).

[28] B. Kraus, *Phys. Rev. Lett.* . **104**, 020504 (2010).

[29] B. Kraus, *Phys. Rev. A*. **82**, 032121 (2010).

[30] B. Liu, et al. *Phys. Rev. Lett.*. **108**, 050501 (2012).

[31] H-K. Lo and S Popescu. *Phys.Rev.Lett.* **83**, 1459, (1999).