MUTUALLY UNBIASED UNITARY BASES AND ITS CONTEXT IN UNCERTAINTY RELATION FOR UNITARY OPERATORS

BY

RINIE NARINIE BINTI MOHD NASIR

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy in Computational and Theoretical Sciences

Kulliyyah of Science
International Islamic University Malaysia

NOVEMBER 2021

ABSTRACT

Analogous to Mutually Unbiased Bases (MUB) for d-dimensional Hilbert space, $\mathcal{H}_d$ capturing the notion of equiprobable transition between states in one basis to another, we consider a similar notion for some subspace of linear operators instead. Working mainly in terms of matrices, the notion of Mutually Unbiased Unitary Bases (MUUB) of $M(d, \mathbb{C})$ can be understood in terms of the equiprobable guess of a unitary operator in one basis for that in another. MUUBs has in fact shown to be useful in specific quantum key distribution (QKD) protocols, namely bidirectional QKD protocols akin to the role of MUBs for prepare and measure QKD schemes like the well-known BB84 protocol. The MUUB structure is strongly related to the notion of MUBs consisting only of maximally entangled states of space $\mathcal{H}_d \otimes \mathcal{H}_d$ or, mutually unbiased maximally entangled bases (MUMEBS). The two are essentially equivalent though much remains to be explored. In fact, for a d^2-dimensional space of $M(d, \mathbb{C})$, while it is known that the maximal numbers that MUUBs can have is $d^2 - 1$, there is no known recipe for constructing the maximal number of such bases. It is not even known if such a number may even be achieved for any d Focusing on the case for d being the prime numbers, we show that the minimal number for MUUBs is 3 and approaches its maximal $d^2 - 1$ for very large values of d. We further provide a numerical recipe in constructing MUUBs which gives us an explicit construction for the maximal number of MUUBs for subspaces of $M(3, \mathbb{C})$ and $M(2, \mathbb{C})$. Despite the possible use of the numerical search for any dimension, it quickly becomes inefficient as d grows. For a more analytical solution, we turn our focus to the case of some d-dimensional subspace for any prime d and report on the maximal number of MUUBs for such a subspace. By constructing monoids based on the underlying sets of $\mathcal{H}_d$ and a subspace of $M(d, \mathbb{C})$, an isomorphism between the monoids lead to an important theorem for constructing d MUUBs, i.e. the maximal possible number for such a subspace. Finally, we show how the notion of MUUBs arise in some setup relevant to the problem of incompatibility/uncertainty between pairs of unitary operators. Departing from some earlier works making use of standard deviations to quantify the uncertainty of pairs of unitary operators (similar to the uncertainties of observables), we formulate a more 'operational' notion of uncertainty of pairs of unitary operators in the context of a guessing game and derive an entropic uncertainty relation for such a pair. We show how distinguishable operators are compatible while maximal incompatibility of unitary operators can be connected to bases for some subspace of operators which are mutually unbiased. We conclude the thesis with some suggestions for future works.

خلاصة البحث

على غرار القواعد غير المتحيزة بشكل متبادل (MUB) لفضاء هيلبرت ذي الأبعاد d، $\mathcal{H}_d$ يلتقط فكرة الانتقال المتكافئ بين الحالات في أساس واحد إلى آخر، نحن نعتبر فكرة مماثلة لبعض الفضاء الجزئي للمشغلين الخطيين بدلاً من ذلك. من خلال العمل بشكل أساسي من حيث المصفوفات، يمكن فهم مفهوم القواعد الأحادية غير المتحيزة بشكل متبادل (MUUB) لـ $M(d,\mathbb{C})$من حيث التخمين المتساوي للمشغل الوحدوي في أساس واحد لذلك في آخر. في الواقع ، أظهرت MUUBs أنها مفيدة في بروتوكولات توزيع المفتاح الكمي (QKD)، وهي بروتوكولات QKD ثنائية الاتجاه المشابهة لدور MUBs لإعداد وقياس مخططات QKD مثل بروتوكول BB84 المعروف. ترتبط بنية MUUB ارتباطًا وثيقًا بمفهوم MUBs التي تتكون فقط من حالات التشابك القصوى للفضاء $\mathcal{H}_d \otimes \mathcal{H}_d$ أو قواعد التشابك القصوى غير المتحيزة بشكل متبادل (MUMEBS). كلاهما متكافئان بشكل أساسي على الرغم من أنه لا يزال هناك الكثير لاستكشافه. في الواقع ، بالنسبة إلى مساحة الإعلان d^2–الأبعاد لـ $M(d,\mathbb{C})$، بينما من المعروف أن الأرقام القصوى التي يمكن أن تحتوي عليها MUUBs هي d^2–1، فلا توجد وصفة معروفة لإنشاء العدد الأقصى لهذه القواعد . ليس من المعروف حتى ما إذا كان يمكن تحقيق مثل هذا الرقم لأي d مع التركيز في حالة d هي الأعداد الأولية، أوضحنا أن الحد الأدنى لعدد MUUBs هو 3 ويقترب من الحد الأقصى d^2–1 للأرقام الكبيرة جدًا من d. نقدم أيضًا وصفة عددية في إنشاء MUUBs والتي تعطينا بنية واضحة لأقصى عدد من MUUBs للمساحات الفرعية $M(3,\mathbb{C})$ و $M(2,\mathbb{C})$. على الرغم من إمكانية استخدام البحث العددي لأي بُعد، إلا أنه سرعان ما يصبح غير فعال مع نمو d. للحصول على حل أكثر تحليلاً، حولنا تركيزنا إلى حالة بعض الفضاء الجزئي ذي الأبعاد d لأي أول d ونبلغ عن العدد الأقصى من MUUBs لمثل هذه المساحة الفرعية. من خلال إنشاء أحاديات استنادًا إلى المجموعات الأساسية لـ $\mathcal{H}_d$ ومساحة فرعية من $M(d,\mathbb{C})$، يؤدي التماثل بين الأحاديات إلى نظرية مهمة لبناء dMUUBs، أي العدد الأقصى الممكن لمثل هذا الفضاء الجزئي. أخيرًا، أوضحنا كيف تنشأ فكرة MUUBs في بعض الإعدادات ذات الصلة بمشكلة عدم التوافق/عدم اليقين بين الأزواج من المشغلين الوحدويين. خلافا لبعض الأعمال السابقة عن استخدام الانحرافات المعيارية لتقدير عدم اليقين في أزواج المشغلين الوحدويين (على غرار عدم اليقين في الملاحظات)، قمنا بصياغة مفهوم أكثر "تشغيلية" لعدم اليقين من أزواج المشغلين الوحدويين في سياق لعبة التخمين واشتقاق علاقة عدم اليقين الحتمية لمثل هذا الزوج. أوضحنا مدى توافق المشغلين المميزين بينما يمكن ربط أقصى درجات عدم التوافق للمشغلين الوحدويين بقواعد بعض الفضاء الفرعي للمشغلين غير المتحيزين بشكل متبادل. نختتم الأطروحة ببعض الاقتراحات للأعمال المستقبلية.

APPROVAL PAGE

The thesis of Rinie Narinie binti Mohd Nasir has been approved by the following:

Assoc. Prof. Dr. Jesni Shamsul Shaari
Dept. of Physics
Kulliyyah of Science
International Islamic University Malaysia

Jesni Shamsul Shaari
Supervisor

Stefano Mancini
Co-Supervisor

DR. BAKHRAM UMAROV
Associate Professor
Department of Physics
Kulliyyah of Science
International Islamic University Malaysia

Bakhram Umarov
Internal Examiner

Hishamuddin Zainuddin
External Examiner

M. Taher Bin Bakhtiar
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigation, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Rinie Narinie binti Mohd Nasir

Signature…………………. Date …..................

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

MUTUALLY UNBIASED UNITARY BASES AND ITS CONTEXT IN UNCERTAINTY RELATION FOR UNITARY OPERATORS

I declare that the copyright holder of this thesis is Rinie Narinie binti Mohd Nasir.

Affirmed by Rinie Narinie binti Mohd Nasir

……..……..…………… ……………………..
Signature Date

ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious, and the Most Merciful. Praise be to Allah for His will I managed to complete this thesis.

First of all, I would like to express my gratefulness to my main supervisor, Assoc. Prof. Dr. Jesni Shamsul Shaari for his continuous guidance, word of encouragement and persistent help over the years of my Ph.D journey. The completion of this thesis would not have been possible to be an achievement without his excellent supervision and feedback.

Also, I would like to extend my sincere gratitude to my co-supervisor, Prof. Dr. Stefano Mancini for being a kind host for me and my family during our stay in University of Camerino, Italy in June 2019. It was a pleasant experience for us.

My warmest thanks to my friends Nor Raihan binti Mohamad Asimoni, Nur Zatul Akmar Hamzah, Siti Nurlaili Karim, Hafizah Bahaluddin, Nor Amirah Mohd Busul Aklan and Nur Rahimah Sakinah binti Abdul Salam, who provided me assistance and comfort in the time of distress.

Next, I would like to thank Ministry of Higher Education for providing me financial support in pursuing Ph.D degree under MyBRAIN15 scheme.

To my parents and siblings, thank you for all the support, prayers and sacrifices, as I completed my Ph.D degree. Finally, and most importantly, special thanks to my husband, Muhammad Faizul bin Ibrahim who always be there for me through thick and thin and my beloved daughter, Nur Farhaira Rania binti Muhammad Faizul who understands me more than ever when I was working on with the thesis.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

MUB	Mutually unbiased bases
MUUB	Mutually unbiased unitary bases
MES	Maximally entangled states
POVM	Positive-operator-valued measure
PPOVM	Process positive-operator-valued measure
QKD	Quantum key distribution
QPT	Quantum process tomography

CHAPTER ONE

INTRODUCTION

1.1 MOTIVATION

The advancement of quantum information has been of interest since the early 90s (Duwell, 2019). It deals mostly with the issue of how information is represented and communicated through quantum states. Notwithstanding the rich details of the field of quantum information theory, it can be described in a nutshell as dealing with the notion of retrieving or manipulating information encoded via quantum mechanical properties of a system. In other words, one's ability to know or manipulate a system is generally limited. As an example, the uncertainty principle limits the ability to precisely estimate value associated to non-commuting observables.

This is closely related to the issue of optimal estimation of a quantum states in the context of state estimation, where it deals with the maximal information extraction of the system's state. Considering quantum systems that can be represented by elements in a finite dimensional Hilbert space, measurements made in one basis may perturb the system and effectively result in introducing uncertainty of measurements made in another. More precisely, measuring a quantum state belonging to a basis along a mutually unbiased basis, one obtains as the result, a random vector of the latter basis and all the possible results are equiprobable (Durt et al. 2010). We refer such bases as mutually unbiased bases (MUBs). The simplest example for MUB is the spin states of a spin-$\frac{1}{2}$ particle for two perpendicular directions.

The concept of MUB was first introduced by Schwinger (1960). The next twenty years saw plenty of progress in this field. Alltop (1980) constructed for complex sequences (of period N where the sequences consist of Nth root of unity with N as a positive integer) with low periodic correlations for use in communication system where his sequences are the first construction of sets of MUBs. Then, Ivanovic (1981) provided the explicit construction of a complete set of MUBs for quantum system of odd prime dimensions. Wooters & Fields (1989) extended the construction of Alltop (1980) and Ivanovic (1981) to all prime powers of an odd number d, such that $d = p^m$ (m is a positive integer) by using mathematical framework of finite fields. The work of Wooters & Fields (1989) was expressed differently by Chaturvedi (2002) where the latter represented the $d+1$ MUB in respect of characters of the cyclic group G of order p. Meanwhile, Bandyopadhyay et al. (2002) showed an alternate proof that a complete set of MUBs exists in all prime power dimensions if one constructs sets of MUB from the eigenvectors of special unitary operators (this is known as the generalised Pauli operators). A summary of known constructions which include the sets of MUBs described by Alltop (1980), Ivanovic (1981) and Wooters & Fields (1989) was published by Klappenecker & Röttler (2003).

In principle, MUBs have been used in practical applications such as quantum key distribution (QKD), where the BB84 (Bennet, C. H. , Brassard, 1984) was the pioneering protocol as well as the various protocols proposed thereafter (we refer to Pirandola et al. (2020) for a thorough review of the subject matter) and quantum state tomography where Wooters & Fields (1989) showed that $d+1$ MUBs provide the optimal set of measurements. We provide the standard definition of MUBs in the following

Definition 1.1 *Two distinct orthonormal bases for a d-dimensional Hilbert space* $J^{(0)}=\{|\varphi_0\rangle,...,|\varphi_{d-1}\rangle\}$ *and* $J^{(1)}=\{|\phi_0\rangle,...,|\phi_{d-1}\rangle\}$ *are said to be mutually unbiased bases (MUB) provided that* $|\langle\varphi_i|\phi_j\rangle|=1/\sqrt{d}$ *, for every* $i,j=0,...,d-1.$

Nonetheless, in terms of composite dimensions which are not powers of primes, for example $d=6,$ still remains an open problem for the existence of a complete set of MUBs. In this context, the Zauner conjecture (Klappenecker, A., Röttler, 2003) stated that the number of MUBs for $d=6$ is three rather than seven MUBs.

Motivated by the study of MUB, we consider the notion of mutually unbiased unitary bases (MUUB) for the space of operators acting on a d-dimensional Hilbert based on considering the idea of equiprobable guesses of unitary transformations. This is closely related to the issue of optimal estimation of process determination where we focus on the estimation of the dynamics of a quantum system instead of state estimation. As the dynamical evolution of a closed quantum system is described by a unitary transformation, these equiprobable guesses are relevant to a procedure of identification of an unknown quantum dynamical process acting on a quantum state, i.e. quantum process tomography (QPT) (Scott, 2008). Quantum process tomography is a method for determining quantum channel (trace-preserving completely positive linear map) which acts upon a quantum system (note the difference with quantum state tomography which is a method for quantum state determination). It is noteworthy that prior to this, Scott (2008) first introduced the notion of MUUBs where one can have a maximal of d^2-1 MUUBs for the d^2-dimensional Hilbert space for dimension $d=2,3,5,7$ and 11.

1.2 PROBLEM STATEMENT

The construction of MUUBs for the d^2-dimensional Hilbert space was first done by Scott (2008) and is shown to have a maximal of d^2-1 MUUBs. It can be used for QPT and is shown to exist for $d = 2,3,5,7$ and 11. However, beyond that, little else is known. As a matter of fact, no known recipe exists for constructing the maximal number of MUUBs for d^2-dimensional Hilbert space, let alone subspaces for $M(d,\mathbb{C})$.

1.3 RESEARCH APPROACH AND OBJECTIVES

In this thesis, we aim to have a proper understanding of MUUBs for the subspace of operators acting on a d-dimensional Hilbert space. Motivated by the equiprobable transition between states in one basis to another in the case of MUBs, we aim to develop an analogous idea of equiprobable guesses of unitaries towards a notion of MUUB for the subspace of operators acting on a d-dimensional Hilbert and provide a systematic study of the notion's properties and construction as well as the relevance of MUUBs in the context of incompatibility between the unitary operators.

We start off by finding the minimal number of MUUBs that can be constructed for space of $M(d,\mathbb{C})$ based on the equivalence of MUUB for $M(d,\mathbb{C})$ and MUBs for bipartite systems whose Hilbert space is $\mathcal{H}_d \otimes \mathcal{H}_d$ consisting of only maximally entangled states (MES). Next, we construct the maximal number of MUUBs for some subspace of $M(d,\mathbb{C})$. Then, we hope to see the MUUBs would arise naturally by using the uncertainty relation to establish the entropic bounds between two unitary operators for some tester with measurement operators. This research aims to achieve the following objectives:

- To construct mutually unbiased unitary bases acting on d-dimensional Hilbert space.
- To ascertain the maximal number of mutually unbiased unitary bases on d-dimensional Hilbert space.
- To establish entropic bounds on the maximal amount of information.

In the following, we provide the necessary background of quantum mechanics that we would use throughout the thesis.

1.4 MATHEMATICAL PREREQUISITES

Before we delve into the discussion of MUUBs, it is instructive to outline certain basic concepts of linear algebra and the standard notation of quantum mechanics for linear algebraic concepts. We refer to Nielsen & Chuang (2010) for the following subsections.

1.4.1 Hilbert space

In the following $\mathcal{H}_d$ is referred as a d-dimensional Hilbert space, a complex vector space of dimension d equipped with an inner product. The Hilbert space must obey the properties of being a linear vector space, with a valid inner product. It is separable and also complete. The Dirac notation represents the standard quantum mechanical notation from linear algebra. It indicates that a vector of $\mathcal{H}_d$ would be expressed as the *ket* notation $|u\rangle$, and its *dual vector,* as the *bra* notation $\langle u|$. The inner product of $|u\rangle$ and $|w\rangle$ may be denoted as $\langle u|w\rangle$. A unit vector is a vector $|u\rangle$ such that $\||u\rangle\|$=1. For this case, $|u\rangle$ is also called *normalized*. Two vectors $|u\rangle$ and $|v\rangle$ are *orthogonal* if their inner product is equal to zero, which is $\langle u|v\rangle = 0$.

A basis $\mathcal{F}$ for $\mathcal{H}_d$ is a set of vectors such that any element in the space can be written as a linear combination of the elements of $\mathcal{F}$. This basis is *orthonormal* if all vectors are mutually orthogonal and of unit length.

A linear operator on $\mathcal{H}_d$ is defined to be a function $\mathcal{M}:\mathcal{H}_d \to \mathcal{H}_d$ which is linear in its inputs,

$$\mathcal{M}\left(\sum_i a_i |u_i\rangle\right) = \sum_i a_i \mathcal{M}(|u_i\rangle). \tag{1.1}$$

The identity operator will be expressed by $\mathbb{I}_d$. As a simple example, we let the identity and the Pauli operators on $\mathcal{H}_2$, which can be written with respect to the computational basis as

$$\begin{aligned}
\mathbb{I}_2 &= |0\rangle\langle 0| + |1\rangle\langle 1|, \\
Z &= |0\rangle\langle 0| - |1\rangle\langle 1|, \\
X &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\
Y &= -i|0\rangle\langle 1| + i|1\rangle\langle 0|.
\end{aligned} \tag{1.2}$$

A diagonal representation for a linear operator $\mathcal{M}$ on $\mathcal{H}_d$ is denoted by $\mathcal{M} = \sum_i \lambda_i |u_i\rangle\langle u_i|$, where the vectors $|u_i\rangle$ form an orthonormal basis of eigenvectors for $\mathcal{M}$ with corresponding λ_i. An operator $\mathcal{M}$ is then called a diagonalisable operator if it has such diagonal representation. Also, $\mathcal{M}$ is a normal operator if it commutes with its adjoint such that $\mathcal{M}\mathcal{M}^\dagger = \mathcal{M}^\dagger\mathcal{M}$. Note that a linear operator $\mathcal{M}$ on $\mathcal{H}_d$ is diagonalisable if and only if it is normal (spectral decomposition). $\mathcal{M}$ is unitary if $\mathcal{M}\mathcal{M}^\dagger = \mathcal{M}^\dagger\mathcal{M} = \mathbb{I}_d$. As $\mathcal{M}$ is a unitary operator, then $\mathcal{M}$ is normal and has a spectral decomposition. Therefore, the unitary operator is diagonalisable and normal.

Given that $M(d,\mathbb{C})$ is the space of all $d \times d$ matrices with entries from $\mathbb{C}^d$. A matrix $\mathcal{K} \in M(d,\mathbb{C})$ is unitary if $\mathcal{K}^\dagger \mathcal{K} = \mathbb{I}_d$. Also, a matrix $\mathcal{K}$ is a Hermitian matrix if $\mathcal{K} = \mathcal{K}^\dagger$. This matrix is diagonal if $(\mathcal{K})_{ij} = 0$ for all $i \neq j$ (with i^{th} row and j^{th} column of $\mathcal{K}$). Note that the vectors of a basis may be presentation as the column of a matrix. The matrix constructed from an orthonormal basis can be unitary. An eigenvector of $\mathcal{K}$ on $M(d,\mathbb{C})$ is a non-zero vector $|u\rangle$ such that $\mathcal{K}|u\rangle = \lambda|u\rangle$, where λ is a complex number called the eigenvalue of $\mathcal{K}$ corresponding to $|u\rangle$. In quantum information theory, the identity and the *Pauli operators* on $\mathcal{H}_2$ represented by 2×2 matrices, namely the *Pauli matrices* are denoted as

$$\mathbb{I}_2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{1.3}$$

The Pauli matrices have been generalised for higher dimensions. The generalised Pauli matrices are defined as follows

$$\vec{k}_i = \vec{k}_{i+1},$$

$$X_d \vec{k}_i = \vec{k}_{i+1}, \quad Z_d \vec{k}_i = \omega_d^i \vec{k}_{i+1}, \tag{1.4}$$

where $\vec{k}_i$ is the i^{th} standard basis vector of $\mathbb{C}^d$ and ω_d is a d^{th} root of unity with the index i indicating the i^{th} power of ω_d. Note that the generalized Pauli matrices have the following properties (Bandyopadhyay S., Boykin P., 2002; Hall. J, 2011)

$$
\begin{aligned}
&Z_d X_d = \omega X_d Z_d, \\
&(X_d)^m (Z_d)^n \vec{k}_i = \omega^{ni} \vec{k}_{i+j}, \\
&X_d^d = Z_d^d = \mathbb{I}_d, \\
&\mathrm{Tr}\left(X_d^m Z_d^n\right) = 0 \qquad \text{for } m, n \neq d.
\end{aligned} \tag{1.5}
$$

The *trace* of a $d \times d$ matrix is the sum of the entries on the main diagonal.

$$\mathrm{Tr}(\mathcal{K}) = \sum_i (\mathcal{K})_{ii}. \tag{1.6}$$

The trace is *cyclic*, i.e. $\mathrm{Tr}(\mathcal{K}\mathcal{L}) = \mathrm{Tr}(\mathcal{L}\mathcal{K})$ and *linear*, $\mathrm{Tr}(\mathcal{K}+\mathcal{L}) = \mathrm{Tr}(\mathcal{K}) + \mathrm{Tr}(\mathcal{L}), \mathrm{Tr}(b\mathcal{K}) = b\,\mathrm{Tr}(\mathcal{K})$ where $\mathcal{K}$ and $\mathcal{L}$ are arbitrary matrices in $M(d,\mathbb{C})$ and b is a complex number. For a $d \times d$ matrix $\mathcal{K}$ and $\mathcal{L}$, $\mathrm{Tr}(\mathcal{K}^\dagger \mathcal{L})$ forms an inner product. It is said that the matrices are orthogonal if $\mathrm{Tr}(\mathcal{K}^\dagger \mathcal{L}) = 0$. Note that although $M(d,\mathbb{C})$ is the set of $d \times d$ matrices with complex entries, it is regarded as the set of operators acting on a d-dimensional Hilbert space (with prime d) because actually matrices represent such operators.

1.4.2 Tensor products

Let $|u\rangle$ and $|v\rangle$ are vectors in U and V, and $\mathcal{M}$ and $\mathcal{N}$ are linear operators on U and V respectively. Then, a linear operator $\mathcal{M} \otimes \mathcal{N}$ on $U \otimes V$ is defined as follows

$$\mathcal{M} \otimes \mathcal{N}\left(|u\rangle \otimes |v\rangle\right) \equiv \mathcal{M}|u\rangle \otimes \mathcal{N}|v\rangle. \tag{1.7}$$

The definition of $\mathcal{M} \otimes \mathcal{N}$ can be extended to all elements of $U \otimes V$ to ensure linearity of $\mathcal{M} \otimes \mathcal{N}$, which is

$$(\mathcal{M}\otimes\mathcal{N})\left(\sum_i a_i|u_i\rangle\otimes|v_i\rangle\right)\equiv\sum_i a_i\mathcal{M}|u_i\rangle\otimes\mathcal{N}|v_i\rangle \tag{1.8}$$

The trace for tensor products of $\mathcal{M}\otimes\mathcal{N}$ would be defined as follows

$$\mathrm{Tr}(\mathcal{M}\otimes\mathcal{N})\equiv\mathrm{Tr}(\mathcal{M})\mathrm{Tr}(\mathcal{N}). \tag{1.9}$$

1.5 THE POSTULATES OF QUANTUM MECHANICS

Quantum mechanics provides a mathematical foundation or framework for the construction of physical theories, as is well known. Therefore, this section provides the fundamental concepts of quantum mechanics by means of its postulates.

1.5.1 Postulate 1 (State space)

Associated to any isolated physical system is a complex vector space with inner product (that is, 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.

The Quantum bit or known as qubit is is a quantum system whose state lies in a 2-dimensional Hilbert space. For example, consider an orthonormal basis $\{|0\rangle,|1\rangle\}$ of $\mathcal{H}_2$. Then, any state vector in a qubit can be written as $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$ where α and β are complex numbers such that $|\alpha|^2+|\beta|^2=1$. This is due to $|\varphi\rangle$ being a unit vector, $\langle\varphi|\varphi\rangle=1$ which is known as the *normalization condition* for the state vectors.

1.5.2 Postulate 2 (Evolution)

This postulate states that the evolution of a closed system is described by a unitary transformation. The Pauli operators are the best examples of allowed operations on such quantum system (particularly on qubits) since they are unitary.

1.5.3 Postulate 3 (Quantum general measurement)

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

$$p(m) = \langle\psi|\mathrm{M}_{\mathrm{m}}^{\dagger}\mathrm{M}_{\mathrm{m}}|\psi\rangle, \tag{1.10}$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^{\dagger}M_m|\psi\rangle}}. \tag{1.11}$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^{\dagger}M_m = \mathbb{I}_d. \tag{1.12}$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^{\dagger}M_m|\psi\rangle. \tag{1.13}$$

This postulate describes how to extract information from the quantum system particularly the problem of *distinguishing quantum states*. For example, consider the cryptographic scheme between two parties, Alice and Bob. Alice selects a state $|\psi_i\rangle(0 \le i \le n)$ from a fixed set of states that both users are familiar with and submits it to Bob, whose task is to find the index i associated with it.

Let the states $|\psi_i\rangle$ are orthonormal, then Bob can perform a quantum measurement to distinguish the states in the following procedure. Let $M_i \equiv |\psi_i\rangle\langle\psi_i|$ be measurement operators, one for each possible index i, and let M_0 be another measurement operator denoted as the positive square root of the positive operator $\mathbb{I}_d - \sum_{i\neq 0} |\psi_i\rangle\langle\psi_i|$. The completeness relation.is satisfied by these operators. If the state $|\psi_i\rangle$ is prepared then $p(i) = \langle\psi_i|\mathrm{M_i}|\psi_i\rangle = 1$. Therefore, the result i occurs with certainty. Thus, the orthonormal states $|\psi_i\rangle$ may be reliably distinguished.

In contrast, if the states $|\psi_i\rangle$ are not orthonormal, then no quantum measurement is capable of distinguishing the states.

A special class of this general measurements postulate is known as the projective measurements, together with unitary transformations (as explained in Postulate 2) are adequate to implement in an equivalent way a general measurement. Suppose the measurement operators M_m in Postulate 3, in addition to satisfying the completeness relation $\sum_m M_m^\dagger M_m = \mathbb{I}_d$, also satisfy the conditions that M_m are orthogonal projectors, that is, the M_m are Hermitian, and $M_m M_{m'} = \delta_{m,m'} M_m$. With these additional restrictions, Postulate 3 reduces to as the following.

1.5.4 Postulate 3.1 (Quantum projective measurement)

A projective measurement is described by an observable, M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition,

$$M = \sum_m m P_m, \tag{1.14}$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. The possible outcomes of the measurement correspond to the eigenvalues, m, of the observable. Upon measuring the state $|\psi\rangle$, the probability of getting result m is given by

$$p(m) = \langle\psi|P_m|\psi\rangle. \tag{1.15}$$

Given that outcome m occurred, the state of the quantum system immediately after the measurement is

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}. \tag{1.16}$$

It is worth noting that the commonly used expression "to measure in a basis $|m\rangle$" where $|m\rangle$ denotes an orthonormal basis, simply refers to perform the projective measurement with projectors $P_m = |m\rangle\langle m|$. For example, consider a projective measurement on the vector state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ by the Z Pauli operator as the observable Z. The observable Z has eigenvalues $+1$ and -1 with corresponding eigenvectors $|0\rangle$ and $|1\rangle$, then one obtains the results $+1$ with probability $\langle\psi|0\rangle\langle 0|\psi\rangle = 1/2$ and analogously the result -1 with probability $\langle\psi|1\rangle\langle 1|\psi\rangle = 1/2$.

1.5.5 Postulate 4 (Composite systems)

The state space of a composite physical system is the tensor product of the states spaces of the component physical system. Moreover, if we have systems numbered 1 through n, *and system number* i *is prepared in the state* $|\psi_i\rangle$, *then the joint state of the total system is* $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$.

This postulate explains the description of the composite system based on the combined of state spaces from different quantum systems. Note that if the state of the composite system can be represented by any unit vector of the tensor product, then it is possible that this vector is not a pure tensor product. Such corresponding state is called *entangled*. The simplest example of entanglement is the entangled state of two qubits, $\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)$. Note that the well-known kind of entanglement is the maximally entangled states (MES) for qubit, i.e. the Bell states. The Bell states are defined

$$\begin{aligned}\left|\Phi^{+}\right\rangle&=\frac{|00\rangle+|11\rangle}{\sqrt{2}},\quad \left|\Phi^{-}\right\rangle=\frac{|00\rangle-|11\rangle}{\sqrt{2}},\\ \left|\psi^{+}\right\rangle&=\frac{|10\rangle+|01\rangle}{\sqrt{2}},\quad \left|\psi^{-}\right\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}.\end{aligned} \tag{1.17}$$

A state $|\Phi\rangle$ is said to be a maximally entangled state such that

$$|\Phi\rangle=\frac{1}{\sqrt{D}}\sum_i|i_A i_B\rangle, \tag{1.18}$$

where A and B are the subsystems of Hilbert spaces such that $\mathcal{H}_A\otimes\mathcal{H}_B$.

1.5.6 Shannon entropy

Given that a random variable X with a probability distribution, $p_1,...,p_n$. The Shannon entropy of a random variable X, $H(X)$ can be viewed as a measure of uncertainty about X before one learn of its outcome. This entropy can be written as

$$H(X)\equiv H(p_1,..,p_n)\equiv-\sum_x p_x\log_2 p_x. \tag{1.19}$$

An alternate way to view this entropy is, eq. (1.19) gives the measure of uncertainty about X after one learn of its outcome.

1.6 THESIS ORGANIZATION

All chapters have been arranged in such a way the contents are mathematically concise and chronological to provide for a coherent reading.