Mutually Unbiased Bases and Weyl Commutation Relations in Quantum State Distinguishability

by
Mukesh Taank

A Thesis
presented to
The University of Guelph

In partial fulfilment of requirements
for the degree of
Masters of Science
in
Mathematics and Statistics

Guelph, Ontario, Canada

ABSTRACT

MUTUALLY UNBIASED BASES AND WEYL COMMUTATION RELATIONS IN QUANTUM STATE DISTINGUISHABILITY

Advisors:

Mukesh Taank — Dr. Rajesh Pereira

University of Guelph, 2023 — Dr. David W. Kribs

This thesis explores the interplay between mutually unbiased bases, the Weyl commutation relation, and one-way local operations and classical communication (LOCC) distinguishability within quantum systems. We focus on three main concepts in this thesis: the Weyl commutation relation of matrices, the generalized Pauli matrices and mutually unbiased bases. We detail the well-known proof that in any dimension d, the number of mutually unbiased bases is at most $d + 1$. Specifically, we look at a proof that uses the argument of rank, as well as provide our own proof, which uses the argument of dimension. Leveraging these concepts, we develop an approach for distinguishing quantum states through one-way LOCC. Furthermore, we delve into established results related to common unbiased bases, which provide a framework for one-way LOCC distinguishability. The results and exposition contribute to a deeper understanding of quantum systems, with potential applications in secure communication protocols and quantum privacy.

Dedication

To my parents, Rashma and Ajay, and my brother Rishi. Thank you for all your love and support.

Acknowledgements

I would like to express my deepest appreciation and gratitude to my graduate supervisors, Dr. Rajesh Pereira and Dr. David W. Kribs. Thank you for taking a chance on me and providing me with the opportunity to study various intriguing topics in the field of quantum information theory. Your knowledge, expertise and guidance helped make complicated concepts more approachable. I am especially grateful for all the time and effort you put into my education.

Finally, to my amazing friends, Mahendra, Taheer, Michael, Dylan, Ajay, Kevin, Jawad, Jaskaran, Keishawn, Ijlal and Metal. Thank you for always encouraging me to do my best.

Contents

List of Figures

Chapter 1

Introduction

In the field of quantum information, local operations and classical communication, or LOCC, is an essential concept that refers to a class of operations that can be performed on quantum systems. The fundamental idea of LOCC is that quantum systems can be manipulated by local quantum operations, such as applying gates to individual qubits, and by classical communication, which permits the exchange of classical information between remote participants. A key component of quantum computing and communication, LOCC finds use in many different areas, including quantum simulation, quantum error correction, and cryptography. In LOCC protocols, the local parties operate on their own quantum systems, which can be initially constructed in an entangled state, to execute operations including measurements and unitary transformations. The two or more parties then exchange their measurement outcomes and other classical information using classical communication. However, LOCC protocols restrict quantum information from being shared between the local parties. LOCC protocols are used in a variety of applications, including the study of entanglement and the development of quantum error correction codes. In order to create effective and dependable quantum communication and computing protocols, understanding LOCC is crucial as it provides a framework for comprehending the capabilities and constraints of

quantum systems.

The work presented in this thesis focuses on important topics in quantum information, including Weyl-commuting matrices and the generalized Pauli matrices with the main goal to examine LOCC [5, 10, 24, 29, 43, 44, 50, 52, 84, 96, 97, 98, 99] more closely through these lenses.

The well-known Pauli matrices from quantum mechanics are generalized in a set of matrices called the generalized Pauli matrices. These matrices are often used in quantum information theory and provide a natural way to describe quantum operations on multi-level quantum systems such as qudits [25, 52]. In the context of LOCC, the generalized Pauli matrices are particularly useful because they form a basis for the space of traceless operators on a given number of qudits. This means that any traceless operator on a system of qudits can be expressed as a linear combination of the generalized Pauli matrices [15, 49].

Weyl-commuting matrices are those that commute with every member of the Weyl-Heisenberg group of unitary matrices, which also contain the Hadamard gate and the Pauli matrices. The essential relationship that describes the Weyl-Heisenberg group is the Weyl commutation relation [8, 87, 90]. Weyl-commuting matrices are critical for building mutually unbiased bases (MUBs) [4], which are essential for a number of quantum information tasks. The Weyl commutation relation is a key property of the Pauli group, which consists of the Pauli matrices and their tensor products. The Pauli group has been shown to be a maximal subgroup of the group of local operations that can be performed by parties who cannot communicate classically. Specifically, any two Pauli matrices are said to be Weyl-commuting if and only if they are capable of being derived from one another by local operations and conventional communication [9, 18, 52].

Quantum state distinguishability and quantum entanglement are two more key issues in quantum information theory, and they have been studied using MUBs. MUB-based quantum cryptography protocols and mutually unbiased quantum state tomography are two signifi-

cant uses of MUBs in quantum information. Mutually unbiased bases and Weyl-commuting matrices including the Weyl commutation relation have an important relationship with the concept of local operations and classical communication (LOCC) in quantum information theory. MUBs have been proven to be crucial in defining the set of states that can be differentiated by LOCC. It has been demonstrated that a group of states can only be identified by LOCC if and only if they are mutually unbiased toward each other [4, 19].

This thesis is organized as follows. In chapter 2, we provide relevant mathematical preliminaries and background concepts which will be important in understanding the newer concepts in later chapters. We start by looking at Hilbert spaces. After this, we provide a brief overview of C*-algebras. The last preliminary notion touched on in this chapter is the basics of quantum information theory, including qubits, Dirac notation and tensor products. We wrap up this chapter, by introducing mutually unbiased bases. In chapter 3, we cover some of the more advanced topics to be used in a later chapter. We start by covering one of the most important concepts of this thesis, which is the Weyl commutation relation. We then move on to looking at generalizations of the well-known Pauli matrices. To finish this chapter we return to mutually unbiased bases and provide an example wherein we walk through the calculation to find out how many bases consisting of the eigenstates of the generalized Pauli matrices are mutually unbiased. In chapter 4, we introduce the topic of local quantum operations and classical communication (LOCC) and detail the different LOCC schemes and details specifically one-way LOCC measurement procedures. We finish this chapter by making the connection between LOCC and MUBs for distinguishability purposes. To end chapter 5 and the thesis, a summary and conclusion are presented with a short section suggesting directions for further work.

Chapter 2

Mathematical Preliminaries and Background Concepts

This chapter will highlight some background concepts and mathematical preliminaries needed for this thesis. The first section covers topics including vector spaces, inner products, orthogonality and Hilbert spaces. The following section covers the basics of C*-algebras. Finally, the third section will cover some introductory quantum information theory including qubits, Dirac notation, and quantum operations.

2.1 Vector Spaces to Hilbert Spaces

2.1.1 Defining the Hilbert Space

The mathematics of quantum mechanics and quantum information theory both depend on Hilbert spaces. These spaces provide the mathematical framework suitable to describe concepts, principles and processes of the theory of quantum information. We will begin with inner product spaces.

Definition 2.1.1. *An **inner product** on a complex vector space, X, is a function, $\langle \cdot, \cdot \rangle$:*

$X \times X \to \mathbb{C}$, *such that for all* $u, v, w \in X$ *and* $c_1, c_2 \in \mathbb{C}$, *the following properties are met:*

- $\langle c_1 u + c_2 v, w\rangle = c_1\langle u, w\rangle + c_2\langle v, w\rangle$
- $\langle u, v\rangle = \overline{\langle v, u\rangle}$
- $\langle u, u\rangle \geq 0$.
- $\langle u, u\rangle = 0$ *if and only if* $u = 0$.

Often a linear space with an inner product is called an *inner product space*. Furthermore, an inner product space defines the notion of *length* as follows:

Definition 2.1.2. *Let* X *be an inner product space with inner product* $\langle \cdot, \cdot \rangle$. *The norm, or length, is a function* $V \to \mathbb{R}$ *denoted as* $||\cdot||$, *and defined as*

$$||u|| = \sqrt{\langle u, u\rangle}, \tag{2.1}$$

for all $u \in X$. *It also satisfies the conditions:*

- $||u|| \geq 0$ *with equality if and only if* $u = 0$.
- $||cu|| = |c|\,||u||$.
- $||u + v|| \leq ||u|| + ||v||$ *(Triangle Inequality).*

A vector space containing a norm is typically called a normed vector space.

Example 2.1.3. *The Euclidean norm on* $\mathbb{R}^n$ *is given by*

$$||u|| = \sqrt{\langle x, x\rangle} = \sqrt{x_1^2 + x_2^2 + ... + x_n^2}.$$

for all $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$.

Example 2.1.4. *The norm in the space of continuous functions, $C([0,1])$, is given by*

$$||f|| = \sqrt{\langle f, f\rangle} = \sqrt{\int_0^1 [f(x)^2]dx}.$$

Theorem 2.1.5 (Cauchy-Schwarz Inequality)**.** *[89, 92] Let u and v be arbitrary vectors in an inner product space, X, over the scalar field $\mathbb{C}$. Then*

$$|\langle u, v\rangle|^2 \leq \langle u, u\rangle\langle v, v\rangle = ||u||^2||v||^2, \tag{2.2}$$

for all $u, v \in X$, with equality if and only if u and v are linearly dependent vectors.

Proof. Let u and v be arbitrary vectors in an inner product space, X, over the scalar field $\mathbb{C}$. If $u = 0$ or $v = 0$, the inequality holds since $\langle u, 0\rangle = 0$ and $||0|| = 0$.

For the case of $u, v \neq 0$, we define a new vector, w, as

$$w = u - \frac{\langle u, v\rangle v}{||v||^2}.$$

Compute the inner product $\langle w, w\rangle$:

$$\begin{aligned}
\langle w, w\rangle &= \langle u, u\rangle - \frac{1}{||v||^2}\langle u, \langle u, v\rangle v\rangle - \frac{1}{||v||^2}\langle\langle u, v\rangle v, u\rangle + \frac{\langle u, v\rangle\overline{\langle u, v\rangle}}{||v||^2||v||^2}\langle v, v\rangle \\
&= ||u||^2 - \frac{|\langle u, v\rangle|^2}{||v||^2} - \frac{|\langle u, v\rangle|^2}{||v||^2} + \frac{|\langle u, v\rangle|^2}{||v||^2} \\
&= ||u||^2 - \frac{|\langle u, v\rangle|^2}{||v||^2} \\
&= \frac{||u||^2||v||^2}{||v||^2} - \frac{|\langle u, v\rangle|^2}{||v||^2}.
\end{aligned}$$

Now, make use of the non-negative property of the inner product that $\langle w, w \rangle \geq 0$.

$$\begin{aligned} 0 &\leq \frac{||u||^2||v||^2}{||v||^2} - \frac{|\langle u, v \rangle|^2}{||v||^2} \\ 0 &\leq ||u||^2||v||^2 - |\langle u, v \rangle|^2 \\ |\langle u, v \rangle|^2 &\leq ||u||^2||v||^2 \end{aligned}$$

And thus the result is proven. □

The inner product of a vector space allows for the introduction of the concept of orthogonality. We can define this concept for vectors and sets.

Definition 2.1.6. *Let X be an inner product space. Two vectors $u, v \in X$ are called **orthogonal**, written as $u \perp v$, if $\langle u, v \rangle = 0$.*

Let X be an inner product space. Two subsets, $A, B \subset X$, are orthogonal to each other, that is $A \perp B$, if all $\langle u, v \rangle = 0$ for all $u \in A$ and $v \in B$. More generally, if $C \subset X$ is a set, then a vector x is orthogonal to C, that is $x \perp C$ if $\langle x, u \rangle = 0$ for all $u \in C$.

Definition 2.1.7. *Let X be an inner product space. The set $A = \{a_1, a_2, \ldots, a_n\} \subset X$ is called an **orthonormal set** if all $\langle a_i, a_j \rangle = \delta_{ij}$ for all $i, j \in \{1, 2, \ldots, n\}$, where*

$$\delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases} \tag{2.3}$$

*is the **Kronecker delta function**.*

Definition 2.1.8. *Let X be an inner product space and let $S \subset X$, then the **orthogonal complement** of S is given as:*

$$S^{\perp} = \{u \in X : \langle u, s \rangle = 0 \text{ for all } s \in S\}.$$

In order to talk about what makes an inner product space a Hilbert space, we can speak about Cauchy sequences and define convergence first [41].

Definition 2.1.9. *Let X be an inner product space. The sequence of vectors, $\{x_k, k = 1, 2, 3, \dots\} \in X$, is said to be **convergent** to the vector $x \in X$ if, for all $\varepsilon > 0$, there exists a number, k_ε, such that if $k > k_\varepsilon$, then $|x - x_k| \leq \varepsilon$.*

Definition 2.1.10. *The sequence of vectors, $\{x_k, k = 1, 2, 3, \dots\} \in X$, is said to be a **Cauchy** sequence if, for all $\varepsilon > 0$, there exists a number, k_ε, such that if $m, n > k_\varepsilon$, then $|x_m - x_n| \leq \varepsilon$.*

Theorem 2.1.11. *Every convergent sequence is also a Cauchy sequence.*

Proof. Supposed the sequence $\{x_k\}$ converges to the vector x. Also for some $\varepsilon > 0$, there exists a number, k_ε, such that $|x_m - x| < \frac{\varepsilon}{2}$. Now for $m, n > k_\varepsilon$ and using the triangle inequality, we can see that

$$|x_m - x_n| = |x_m - x + x - x_n| \leq |x_m - x| + |x_n - x| = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

□

Definition 2.1.12. *A **complete** inner product space is one in which every Cauchy sequence converges.*

Finally, this leads us to our formal definition of a Hilbert space.

Definition 2.1.13. *[95] If X is an inner product space that is also complete, then X is called a **Hilbert Space**. We will denote Hilbert spaces using "$\mathcal{H}$". If X is a finite-dimensional inner product space, then it is already complete and thus it is a Hilbert space.*

2.1.2 Operators on Hilbert Spaces

With the definition of a Hilbert space now stated, an intuitive next step is to look at operators acting on Hilbert spaces. These operators will come up later on in this work, so it is beneficial to go over some important operators here.

Before going over the following operators, some important notation is needed. Denote an operator, T from one vector space to another, as $T : X_1 \to X_2$. Denote the set of all linear operators from one normed vector space to another as $\mathcal{L}(X_1, X_2)$. If $X_1 = X_2 = X$, then this is written as $\mathcal{L}(X, X) = \mathcal{L}(X)$. Similarly, denote the space of bounded linear operators from one normed vector space to another as $\mathcal{B}(X_1, X_2)$. If $X_1 = X_2 = X$, then this is written as $\mathcal{B}(X, X) = \mathcal{B}(X)$. Note, a linear operator between any two normed linear spaces is bounded if and only if it is continuous and every linear operator on a finite-dimensional space is bounded[12].

Definition 2.1.14. *A **linear operator** on a Hilbert space $\mathcal{H}$ is a linear transformation, $T : \mathcal{H} \to \mathcal{H}$.*

Lemma 2.1.15. *Let $\mathcal{H}_1, \mathcal{H}_2$ be a finite-dimensional inner product space over $\mathbb{C}$ with inner product $\langle \cdot, \cdot \rangle$. A linear operator $T \in \mathcal{B}(\mathcal{H}_1, \mathcal{H}_2)$ is uniquely determined by the values of $\langle Tu, v \rangle$ for all $u \in \mathcal{H}_1, v \in \mathcal{H}_2$. This means in particular that if $S, T \in \mathcal{B}(\mathcal{H}_1, \mathcal{H}_2)$ and $\langle Tu, v \rangle = \langle Su, v \rangle$ for all $u \in \mathcal{H}_1, v \in \mathcal{H}_2$, then $T = S$.*

Definition 2.1.16. *Let $\mathcal{H}$ be an n-dimensional complex Hilbert space. The **trace** of an $n \times n$ square linear operator, $T \in \mathcal{B}(\mathcal{H})$, is given as the sum of the diagonal entries of T:*

$$\mathrm{Tr}(T) = t_{11} + t_{22} + \cdots + t_{nn} = \sum_{k=1}^{n} t_{kk}, \tag{2.4}$$

where t_{kk} are the diagonal entries of any matrix representation of T.

We can also express the trace of T, given an orthonormal basis, in terms of an inner

product.

$$\mathrm{Tr}(T) = \sum_k u_k^* T u_k = \langle T u_k, u_k \rangle,$$

for the orthonormal basis $\{u_k\}_{1 \leq k \leq n}$.

Also note that $\mathrm{Tr}(\cdot)$ is a linear map and $\mathrm{Tr}(TS) = \mathrm{Tr}(ST)$ for all $S, T \in \mathcal{B}(\mathcal{H})$.

Definition 2.1.17. *Given a linear operator $T \in \mathcal{B}(\mathcal{H}_1, \mathcal{H}_2)$, the **adjoint** of T is the operator $T^* \in \mathcal{B}(\mathcal{H}_2, \mathcal{H}_1)$ such that*

$$\langle Tu, v \rangle = \langle u, T^* v \rangle,$$

*for all $u \in \mathcal{H}_1, v \in \mathcal{H}_2$. Furthermore, T is referred to as **self-adjoint** or **Hermitian**, if $T = T^*$.*

Proposition 2.1.18. *Every eigenvalue of a self-adjoint operator is real, i.e., $\lambda \in \mathbb{R}$.*

Proof. Suppose $\lambda \in \mathbb{C}$ is an eigenvalue of an operator T, and $u \in X, u \neq 0$ is the corresponding eigenvector, such that $Tu = \lambda u$. Then

$$\lambda ||u||^2 = \langle \lambda u, u \rangle = \langle Tu, u \rangle = \langle u, T^* u \rangle = \langle u, Tu \rangle = \langle u, \lambda u \rangle = \overline{\lambda} \langle u, u \rangle = \overline{\lambda} ||u||^2.$$

This then implies that $\lambda = \overline{\lambda}$, and therefore $\lambda \in \mathbb{R}$. □

Definition 2.1.19. *A linear operator $T \in \mathcal{B}(\mathcal{H})$, is called **normal** if $TT^* = T^*T$.*

In general, $TT^* \neq T^*T$. Note that TT^* and T^*T are both self-adjoint for all $T \in \mathcal{B}(\mathcal{H})$. Also, any self-adjoint operator T is normal.

Proposition 2.1.20. *[3] Let $T \in \mathcal{B}(\mathcal{H})$. Then T is normal if and only if $||Tu|| = ||T^* u||$ for all $u \in \mathcal{H}$.*

Proof. [3] Let $T \in \mathcal{B}(\mathcal{H})$. We will prove both directions of this result at the same time. Note

that,

$$\begin{aligned} T \text{ is normal} &\iff T^*T - TT^* = 0 \\ &\iff \langle (T^*T - TT^*)u, u\rangle = 0, \text{ for all } u \in \mathcal{H} \\ &\iff \langle TT^*u, u\rangle = \langle T^*Tu, u\rangle, \text{ for all } u \in \mathcal{H} \\ &\iff ||Tu||^2 = ||T^*u||^2, \text{ for all } u \in \mathcal{H}, \end{aligned}$$

The equivalence of the first and last conditions above gives the desired result. □

Definition 2.1.21. *Let $P \in \mathcal{B}(\mathcal{H})$. The operator P is called a* ***projection*** *if $P^2 = P$. Moreover, P is called an* ***orthogonal projection*** *if $\langle Pu, v\rangle = \langle u, Pv\rangle$, for all $u, v \in \mathcal{H}$, which is to say that $P = P^*$.*

Definition 2.1.22. *Let $T \in \mathcal{B}(\mathcal{H})$. If T satisfies $||Tu|| = ||u||$ for all $u \in \mathcal{H}$, then T is called an* ***isometry****, a distance preserving operator.*

The next type of operator is called the unitary operator, often denoted by U. This is one of the more important operators, especially for this thesis. In general, in quantum information, unitary matrices are vastly seen due to their properties.

Definition 2.1.23. *Let $U \in \mathcal{B}(\mathcal{H})$. If U satisfies $UU^* = U^*U = \mathcal{I}$, where $\mathcal{I}$ is the identity matrix, then U is called a* ***unitary*** *operator. Thus, unitaries are invertible operators with $U^{-1} = U^*$.*

In real vector spaces, "orthogonal" operators are equivalent to unitary operators, which are linear operators in complex vector spaces. A unitary operator on an inner product space is an isomorphism of the space onto itself. Unitary matrices are very valuable in data transformation since they are always invertible and their inverse is likewise always unitary. In particular, as they depict the temporal development of quantum systems, unitary operators are essential to quantum information.

2.1.3 Spectral Theorem for Normal Operators

Definition 2.1.24. *[45] The **spectrum** of a linear operator, T is a generalization of the set of eigenvalues of a matrix. Specifically, a complex number λ is said to be in the spectrum of a bounded linear operator T if $(T - \lambda\mathcal{I})$is not invertible. We can write the spectrum as:*

$$\sigma(T) = \{\lambda \in \mathbb{C} : \det(T - \lambda\mathcal{I}) = 0\}. \tag{2.5}$$

In other words, for all $\lambda \in \sigma(T)$, there exists a nonzero vector, $u \in \mathcal{H}$ such that $Tu = \lambda u$.

Definition 2.1.25. *The **spectral radius** of T is defined as*

$$r(T) = \sup\{|\lambda| : \lambda \in \sigma(T)\}. \tag{2.6}$$

For completeness, we can state the spectral theorem for matrices.

Theorem 2.1.26. *For every finite normal matrix A, there is a unitary matrix, U, such that $A = U\Lambda U^*$, where Λ is a diagonal matrix. Note that in the diagonal matrix, the entries are the eigenvalues of A, and the columns of U encode the eigenvectors of A.*

2.2 Quantum Information Theory

2.2.1 Bits, Qubits and Representations

Quantum information science emerges at the crossroads of three fields: quantum mechanics, information theory, and computer science. Its origins can be traced back to conventional theory, where the focus lies on classical information science encompassing the handling and storage of sequences of bits. The fundamental entity is the bit,

$$x \in \{0, 1\}, \tag{2.7}$$

from which strings are formed and used to encode information [12]. Computation is essentially the processing of bit strings as a means to process the information that they encode.

Analogously, quantum information addresses the storage and manipulation of quantum states. Although it's possible to perform computations using states in various Hilbert spaces, the qubit serves as the fundamental unit due to its practicality. Observe the form of these qubits:

$$\text{one qubit} : |\psi\rangle \in \mathcal{H}_{\text{qubit}} \cong \mathbb{C}^2$$

$$|\psi\rangle \in \text{span}\{|0\rangle, |1\rangle\}$$

A classical bit can store information as either a 0 or a 1, but nothing in between. A qubit, on the other hand, can store a 0, a 1, or a linear combination (also called a "superposition") of both, meaning a combination of 0 and 1 with some probability. A notably renowned illustration of such superposition is Schrödinger's cat experiment [77], where a cat is envisioned to be enclosed within a box containing a poisonous substance with an equal probability of either killing the cat or not within an hour. Schrödinger postulated that after this hour, the cat could be considered simultaneously alive and dead, existing in a superposition of states until the box is opened. The act of observation, he proposed, arbitrarily establishes whether the cat is alive or dead. Unlike a scenario involving a coin toss where the result is exclusively heads or tails, qubits have the capacity to concurrently represent both heads and tails with a certain probability. This means that a qubit can encode more information than a classical bit, and can also exist in multiple states at the same time.

2.2.2 Dirac Notation

Before going forward, this is a good point to comment on the notation. We will mention quantum states quite a lot, and rather than express these states as huge column vectors, a

simplification can be made. It is more efficient to use the notation of the form "$|\cdot\rangle$". In terms of Dirac notation, these are called a "ket". On the other hand, row vectors are represented by a "bra" and are represented in Dirac notation as $\langle\cdot| = |\cdot\rangle^*$. With this notation, we can also reform the representation of inner products as $\langle\cdot|\cdot\rangle$ (a bra-ket) rather than $\langle\cdot,\cdot\rangle$ since evaluating the inner product is equivalent to writing $\langle\cdot||\cdot\rangle$. It just makes sense to get rid of the double line. So, for a vector, u, we can take the inner product of it with itself as $\langle u, u\rangle = \langle u|u\rangle = u^*u$. Moreover, the outer product can be represented by $|u\rangle\langle u| = uu^*$.

Now that we have established the useful Dirac notation, we can re-state the definitions of the linear operators and spectral theorem from sections 2.1.2 and 2.1.3 respectively, using this new notation.

Definition 2.2.1. *A linear operator, T, is a linear transformation, $T : \mathcal{H} \to \mathcal{H}$, such that for all $\alpha \in \mathbb{C}$, and $|\psi\rangle, |\phi\rangle \in \mathcal{H}$,*

$$T(\alpha|\psi\rangle + |\phi\rangle) = \alpha T|\psi\rangle + T|\phi\rangle.$$

Theorem 2.2.2. *Suppose $\{|u_k\rangle\}$ is an orthonormal basis for the Hilbert space, $\mathcal{H}$. Then every $T \in \mathcal{B}(\mathcal{H})$ can be written out as*

$$T = \sum_{k,l} T_{k,l}|u_k\rangle\langle u_l|, \tag{2.8}$$

where $T_{k,l} = \langle u_k|T|u_l\rangle$.

Definition 2.2.3. *Given any orthonormal basis $\{|u_k\rangle\}$ for a Hilbert space $\mathcal{H}$, the **identity** operator, $\mathcal{I}$, is given by $\mathcal{I}(|\psi\rangle) = |\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}$. This operator also decomposes as*

$$\mathcal{I} = \sum_k |u_k\rangle\langle u_k|. \tag{2.9}$$

Now we can return to the spectral theorem for normal operators.

Theorem 2.2.4. *[45] Let T be a normal operator acting on a finite-dimensional Hilbert space, $\mathcal{H}$. There exists an orthonormal basis for $\mathcal{H}$ consisting of eigenvectors, $|u_k\rangle$ of T. T is diagonal in its own eigenbasis, so we can write out the* ***spectral decomposition*** *of T as*

$$T = \sum_k \lambda_k |u_k\rangle\langle u_k|, \tag{2.10}$$

where λ_k is the eigenvalue corresponding to the eigenvector $|u_k\rangle$.

With these definitions now in place, we can move to a new concept which is quite important with operators: functional calculus.

Theorem 2.2.5. *[26] Suppose $f : \mathbb{C} \to \mathbb{C}$ is a function with Maclaurin series*

$$f(x) = \sum_{m=0}^{\infty} c_m x^m, c_m \in \mathbb{C}.$$

If T is a normal operator with spectral decomposition $T = \sum_k \lambda_k |u_k\rangle\langle u_k|$, and the eigenvalues of T lie within the disc of convergence of f, then $f(T)$ is defined as an operator, and

$$f(T) = \sum_k f(\lambda_k) |u_k\rangle\langle u_k|.$$

Sketch of Proof.

$$\begin{aligned} f(T) &= \sum_m c_m T^m \\ &= \sum_m c_m \left(\sum_k \lambda_k |u_k\rangle\langle u_k| \right)^m \\ &= \sum_m c_m \sum_k (\lambda_k)^m |u_k\rangle\langle u_k| \\ &= \sum_k \left(\sum_m c_m \lambda_k^m \right) |u_k\rangle\langle u_k| \\ &= \sum_k f(\lambda_k) |u_k\rangle\langle u_k|. \end{aligned}$$

□

2.2.3 Quantum States on Hilbert Spaces

The finite-dimensional Hilbert spaces of interest in quantum information theory are of dimension $N = d^n$, for some positive integers $n \geq 1$ and $d \geq 2$. This can be extended to infinite-dimensional space, but for this work, we mainly want to focus on finite-dimensional Hilbert spaces. For the common case of $d = 2$, we can define the n-fold *tensor product* (see section 2.2.4): $\mathcal{H}^{(N)} = \mathcal{H}^{(2^n)} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n}$. Furthermore, we use the convention that $\mathcal{H}^{(2^n)} = (\mathbb{C}^2)^{\otimes n} \simeq \mathbb{C}^{2^n}$. We will drop the superscript N in most cases as the dimension of the Hilbert space will be stated or implied [42].

Remark 2.2.6 (Notation)**.** *A quick note on the notation. We will denote a Hilbert space of dimension d, as $\mathcal{H}^{(d)}$. In cases where we are dealing with multiple Hilbert spaces, we will denote two different Hilbert spaces of dimension d as $\mathcal{H}_1^{(d)}$ and $\mathcal{H}_2^{(d)}$. In most cases, we will drop the superscript, d, as the dimension will be given. If dealing with two distinct Hilbert spaces, we will keep the subscript identifiers. If only dealing with one Hilbert space, we will drop the subscript identifiers.*

All quantum bits, or qubits, are described by 2-dimensional unit vectors in some linear space. Both bits and qubits have physical revelations that allow them to perform calculations, however in the interest of this discussion, we will concentrate on the abstract mathematical description of the qubit, and its linear algebraic representation as a unit vector,

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle,$$

where $\alpha, \beta \in \mathbb{C}$. There is the further condition that $|\alpha|^2 + |\beta|^2 = 1$, as $|\psi\rangle$ is a unit vector. The cases $\alpha = 0$ or $\beta = 0$ correspond to the classical states, and otherwise, $|\psi\rangle$ is said to be in a *superposition* of the states $|0\rangle$ and $|1\rangle$, as shown above. Here, the $|0\rangle$ and $|1\rangle$ are called basis vectors and are defined as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

We have introduced the notion of basis vectors, before formally defining the above basis, we can go over the general definition of orthonormal bases first.

Definition 2.2.7. *Let $\mathcal{H} = \mathcal{H}^{(d)}$ be a Hilbert space of dimension d. A set of vectors, $\mathcal{B} = \{|b_k\rangle\}_{k=0}^{d-1} \subseteq \mathcal{H}$ is called an* ***orthonormal basis*** *for $\mathbb{C}^d$ if*

$$\langle b_k | b_l \rangle = \delta_{kl}. \tag{2.11}$$

With this formalization, we can now define the basis containing the $|0\rangle$ and $|1\rangle$ states seen above.

Definition 2.2.8. *Let $\mathcal{H} = \mathcal{H}^{(2)} = \mathbb{C}^2$ be a 2-dimensional Hilbert space. The set $\{|0\rangle, |1\rangle\}$ is called the* ***standard basis*** *of $\mathcal{H}$, and $|0\rangle, |1\rangle$ are called the standard basis vectors. Note*

that these basis vectors are orthonormal to one another. This idea will be touched on in the next sections.

Observe that these are the basis vectors in the complex Hilbert space $\mathcal{H} = \mathbb{C}^2$. More generally, these basis vectors can be written as $|k\rangle \in \mathbb{C}^d$, where the d is the dimension of the Hilbert space, and k represents the entry of the vector that is 1, and the other $d-1$ entries are 0. More relevant for quantum information, we deal with 2-dimensional systems (qubits), and thus take $\dim(\mathcal{H}) = 2^n$; i.e., $\mathcal{H} = \mathbb{C}^{2^n}$. Similar to qubits, a "qudit" is a d-dimensional system.

Definition 2.2.9. *[85] A **qudit** is a quantum version of "d-ary digits" whose state can be described by a unit vector in the d-dimensional Hilbert space $\mathcal{H}^{(d)} = \mathbb{C}^d$. The space is spanned by a set of orthonormal basis vectors $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. The general form of qudits is given by*

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{d-1}|d-1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \in \mathbb{C}^d, \tag{2.12}$$

with $|\alpha_0|^2 + |\alpha_1|^2 + \cdots + |\alpha_{d-1}|^2 = 1$.

Remark 2.2.10. *In quantum information, it is the practice to use **zero-based counting** in the vector indexing, meaning that $|0\rangle$ will have the nonzero entry in the first spot, and the $|1\rangle$ vector will have the nonzero entry in the second spot, and so on.*

Example 2.2.11. *If working in a 2-qubit Hilbert space ($d = 4$): $\mathcal{H}^{(4)} = (\mathbb{C}^2)^{\otimes 2} = \mathbb{C}^4$, the*

basis vector, $|2\rangle$, would be represented in vector form as:

$$|2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{C}^4.$$

It is also possible to express any vector in $\mathcal{H}$ as the weighted sum of its basis vectors; which, of course, enables the mathematical depiction of **superposition states**. This fact enables us to establish what is called the "Hadamard basis", another basis for 2-dimensional Hilbert spaces.

Definition 2.2.12. *Let $\{|0\rangle, |1\rangle\}$ be the standard basis with states $|0\rangle, |1\rangle$ defined as above. The **Hadamard basis** is given as $\{|+\rangle, |-\rangle\}$, where*

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \; |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

For an n-qubit Hilbert space, we can fix a 'nice' orthonormal basis – called the **computational basis** – and identify its basis vectors with n-strings of 0's and 1's.

$$\{|00\ldots00\rangle, |00\ldots01\rangle, \ldots, |11\ldots10\rangle, |11\ldots11\rangle\} = \left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Observe that each column vector has 2^n entries (i.e., each vector is in $\mathbb{C}^{2^n}$), so the basis consists of a total of 2^n of these vectors.

Example 2.2.13. *Consider the 2-qubit Hilbert space $\mathcal{H} = \mathbb{C}^4$. The computational basis can be described by $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, where*

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

Definition 2.2.14. *A vector state $|\psi\rangle \in \mathcal{H}$ is said to be **entangled** if it cannot be written as a tensor product of states from its component systems, so that $|\psi\rangle$ does not decompose as $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ for some vectors $|\psi_1\rangle, |\psi_2\rangle$.*

Definition 2.2.15. *Let $\{|\psi_k\rangle\}$ be a set of arbitrary quantum states with corresponding probabilities p_k, then we can define the **density operator** as the matrix that describes this quantum state, and is written as*

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|. \tag{2.13}$$

Furthermore, density operators obey the following conditions:

- $\sum_k p_k = 1$, *and* $p_k \geq 0$.
- $\rho \geq 0$, *and* $\mathrm{Tr}(\rho) = 1$.

Example 2.2.16. *Suppose we have the 2-qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$, then the density matrix is defined as*

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{pmatrix}.$$

Since this state is normalized, it is understood that $\mathrm{Tr}(\rho) = |\alpha|^2 + |\beta|^2 = 1$.

Proposition 2.2.17. *Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and let $\{|b_k\rangle\}_{k=0}^{d-1}$ be an orthonormal basis for $\mathcal{H}$. Then every state $|\psi\rangle \in \mathcal{H}$ can be written as*

$$|\psi\rangle = \sum_{k=0}^{d-1} \langle \psi | b_k \rangle b_k. \tag{2.14}$$

Proof. Since $\{|b_k\rangle\}_{k=0}^{d-1}$ is a basis for $\mathcal{H}$, then for each state $|\psi\rangle \in \mathcal{H}$, there exists scalars $c_0, c_1, \ldots, c_{d-1} \in \mathbb{C}$ such that

$$|\psi\rangle = c_0|b_0\rangle + c_1|b_1\rangle + \cdots + c_{d-1}|b_{d-1}\rangle = \sum_{k=0}^{d-1} c_k |b_k\rangle.$$

We want to show that $c_k = \langle \psi | b_k \rangle$ for all $k \in \{0, 1, \ldots, d-1\}$. Taking the inner product of both sides of the above equation with $|b_k\rangle$, we get that

$$\begin{aligned}
\langle \psi | b_k \rangle &= \langle c_0 b_0 + c_1 b_1 + \cdots + c_k b_k + \cdots + c_{d-1} b_{d-1} \,|\, b_k \rangle \\
&= \langle c_0 b_0 | b_k \rangle + \langle c_1 b_1 | b_k \rangle + \cdots + \langle c_k b_k | b_k \rangle + \ldots \langle c_{d-1} b_{d-1} | b_k \rangle \\
&= c_0 \langle b_0 | b_k \rangle + c_1 \langle b_1 | b_k \rangle + \cdots + c_k \langle b_k | b_k \rangle + \ldots c_{d-1} \langle b_{d-1} | b_k \rangle.
\end{aligned}$$

At this step, we can realize that since $\{|b_k\rangle\}_{k=0}^{d-1}$ is an orthonormal basis, then each inner product $\langle b_j | b_k \rangle = 0$, except when $j = k$, where $\langle b_k | b_k \rangle = 1$. And thus we have the result stated above that $c_k = \langle \psi | b_k \rangle$ for all $k \in \{0, 1, \ldots, d-1\}$, and so for any quantum state $|\psi\rangle \in \mathcal{H}$, the result is met. □

2.2.4 Tensor Products of Quantum States

Tensor products are an extremely useful tool in quantum information as they give us a way of essentially "multiplying" things like vectors, matrices/operators, spaces, etc., which also has a physical justification as they give the mathematical description of 'composite' quantum systems in quantum mechanics [1].

First, we will write the definition for the Kronecker product. The Kronecker product, denoted by, $\otimes$, is an operation on two operators of arbitrary size resulting in a block matrix. This operation serves as an extension of the tensor product (symbolized by the identical symbol) from vectors to matrices, leading to the resultant matrix of the tensor product assuming a linear mapping related to the choice of basis.

Remark 2.2.18 (Notation)**.** *Let the set of all complex matrices of size $n \times m$ be denoted as $M_{nm}(\mathbb{C})$ (If $n = m$, this will just be written as $M_n(\mathbb{C})$).*

Definition 2.2.19. *[31] Let $A \in M_{nm}(\mathbb{C})$ and $B \in M_{kl}(\mathbb{C})$. Then the Kronecker product, $A \otimes B \in M_{nm}(\mathbb{C}) \otimes M_{kl}(\mathbb{C})$ is described as:*

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \dots & a_{nm}B \end{pmatrix}, \tag{2.15}$$

where a_{ij} represents the ij^{th} position in A.

Example 2.2.20. *Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\mathcal{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We can evaluate the*

following Kronecker products:

$$X \otimes \mathcal{I}_2 = \begin{pmatrix} 0 \cdot \mathcal{I}_2 & 1 \cdot \mathcal{I}_2 \\ 1 \cdot \mathcal{I}_2 & 0 \cdot \mathcal{I}_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

$$Z \otimes X = \begin{pmatrix} 1 \cdot X & 0 \cdot X \\ 0 \cdot X & -1 \cdot X \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

With this definition, it is important to also go over the properties of the Kronecker product for matrices. These are presented in the following Lemma.

Lemma 2.2.21. *[1] Let $A \in M_{nm}(\mathbb{C}), B \in M_{n'm'}(\mathbb{C}), C \in M_{mr}(\mathbb{C}), D \in M_{m'r'}(\mathbb{C})$, and $c \in \mathbb{C}$. Then the Kronecker product obeys the following properties:*

1. $c \otimes A = A \otimes c = cA$
2. $A \otimes 0 = 0 \otimes A = 0$
3. $(A \otimes B)^* = A^* \otimes B^*$
4. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$
5. $A \otimes (B + C) = (A \otimes B) + (A \otimes C)$
6. $(A + B) \otimes C = (A \otimes C) + (B \otimes C)$
7. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

After looking at the Kronecker product for matrices, we can now switch to the analogous tensor product of vectors and spaces. Note, we will continue to use Dirac notation to represent vectors and states.

Let us start by looking at the tensor product of two Hilbert spaces, as this will provide some insight into how vectors will be affected.

Theorem 2.2.22. *Let $\mathcal{H}_1^{(d_1)}$ and $\mathcal{H}_2^{(d_2)}$ be Hilbert spaces with orthonormal bases $\{|\psi_j\rangle\}_{1\leq j\leq d_1}$ and $\{|\phi_k\rangle\}_{1\leq k\leq d_2}$ respectively. Then*

$$\{|\psi_j\rangle \otimes |\phi_k\rangle : 1 \leq j \leq d_1, 1 \leq k \leq d_2\}, \tag{2.16}$$

is an orthonormal basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$, where $\dim(\mathcal{H}_1 \otimes \mathcal{H}_2) = d_1 \times d_2$.

With the theorem of the tensor product Hilbert spaces now established, we can look into the properties of the tensor product.

Definition 2.2.23. *The tensor product of vectors is characterized by the following axioms:*

1. *For all $\alpha \in \mathbb{C}, |\psi_k\rangle \in \mathcal{H}_k, k = 1, 2,$*

$$\alpha(|\psi_1\rangle \otimes |\psi_2\rangle) = (\alpha|\psi_1\rangle) \otimes |\psi_2\rangle = |\psi_1\rangle \otimes (\alpha|\psi_2\rangle).$$

2. *For all $|\psi_1\rangle, |\phi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$,*

$$(|\psi_1\rangle + |\phi_1\rangle) \otimes |\psi_2\rangle = (|\psi_1\rangle \otimes |\psi_2\rangle) + (|\phi_1\rangle \otimes |\psi_2\rangle).$$

3. *For all $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle, |\phi_2\rangle \in \mathcal{H}_2$,*

$$|\psi_1\rangle \otimes (|\phi_1\rangle) + |\psi_2\rangle) = (|\psi_1\rangle \otimes |\phi_1\rangle) + (|\psi_1\rangle \otimes |\psi_2\rangle).$$

Example 2.2.24. *Let* $u = \begin{pmatrix} u_1 & u_2 \end{pmatrix}^T$ *and* $v = \begin{pmatrix} v_1 & v_2 \end{pmatrix}^T$. *Then*

$$u \otimes v = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \otimes \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} u_1 v \\ u_2 v \end{pmatrix} = \begin{pmatrix} u_1 \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \\ u_2 \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} u_1 v_1 \\ u_1 v_2 \\ u_2 v_1 \\ u_2 v_2 \end{pmatrix}.$$

Example 2.2.25. *Let* $\mathcal{H}_1 = \mathcal{H}_2 = \mathbb{C}^2$, *with the same orthonormal bases:* $\{|0\rangle, |1\rangle\}$, *with* $|0\rangle$ *and* $|1\rangle$ *defined above. Then the orthonormal basis for the 2-qubit space:* $\mathcal{H}_1 \otimes \mathcal{H}_2 = \mathbb{C}^2 \otimes \mathbb{C}^2$ *is given by* $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$, *where*

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

Remark 2.2.26. *We used a simplified notation to represent the vectors in the 2-qubit space from the previous example. For completeness, we can explicitly state these simplifications here as*

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

Another very important basis is called the Bell basis and consists of the "Bell states". The Bell states or EPR pairs are specific quantum states of two qubits that represent the simplest (and maximal) examples of quantum entanglement [6, 53].

Definition 2.2.27. *Four specific two-qubit states are referred to as the maximally entangled two-qubit* ***Bell states*** *and constitute the* ***Bell basis****, which is a maximally entangled basis*

in the four-dimensional Hilbert space for two qubits. These states are defined as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 + |1\rangle_1 \otimes |1\rangle_2) = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 - |1\rangle_1 \otimes |1\rangle_2) = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 + |1\rangle_1 \otimes |0\rangle_2) = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 - |1\rangle_1 \otimes |0\rangle_2) = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2)$$

with all states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle \in \mathcal{H}_1^{(2)} \otimes \mathcal{H}_2^{(2)}$.

2.2.5 Brief Introduction to Mutually Unbiased Bases

The final concept we will introduce in this chapter is about Mutually Unbiased Bases (MUBs). This concept will be touched on in more detail in the next chapter, but the foundations of this can be shown here first.

Before stating and defining mutually unbiased bases, we can first look at what it means for matrices to be unbiased and mutually unbiased.

Definition 2.2.28. *[14] A* $d \times d$ *unitary matrix,* $A \in \mathbb{C}^{d\times d}$ *is called* ***unbiased****, if all its matrix elements,* A_{jk}*, satisfy* $|A_{jk}| = \frac{1}{\sqrt{d}}$*, for all* $j, k \in \{0, 1, \ldots, d-1\}$.

Definition 2.2.29. *[14] Two unitary matrices* $A, B \in \mathbb{C}^{d\times d}$ *are called* ***mutually unbiased****, if the matrix* A^*B *is unbiased.*

Example 2.2.30. *An example of an unbiased unitary matrix is the $d \times d$ Fourier matrix,*

$$W = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{d-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(d-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{d-1} & \omega^{2(d-1)} & \dots & \omega^{(d-1)(d-1)} \end{pmatrix}, \tag{2.17}$$

where $\omega = e^{\frac{2\pi i}{d}}$.

With these definitions, we can take a closer look at MUBs.

Definition 2.2.31. *[40, 71] Two observables (self-adjoint operators) A and B of a finite-dimensional quantum system of dimension d, are called* ***complementary****, if their eigenvalues are non-degenerate and any two normalized eigenvectors, $|u_j\rangle$ of A and $|v_k\rangle$ of B satisfy*

$$|\langle u_j | v_k \rangle| = \frac{1}{\sqrt{d}}. \tag{2.18}$$

Definition 2.2.32. *[66, 90] Two orthonormal bases $\mathcal{B} = \{|b_k\rangle\}_{k=0}^{d-1}$, $\mathcal{B}' = \{|b'_{k'}\rangle\}_{k'=0}^{d-1} \in \mathbb{C}^d$ are called* ***mutually unbiased bases*** *if*

$$|\langle b_k | b'_{k'} \rangle| = \frac{1}{\sqrt{d}}, \tag{2.19}$$

for all $|b_k\rangle \in \mathcal{B}$ and $|b'_{k'}\rangle \in \mathcal{B}'$, and all $k, k' \in \{0, 1, \dots, d-1\}$.

These bases are considered unbiased, meaning that if a system is prepared in a state corresponding to one of these bases, all measurement outcomes related to the other basis are anticipated to occur with equal probabilities.

Chapter 3

Weyl Commutation Relation, Generalized Pauli Operators and Mutually Unbiased Bases

The main goal of this thesis is to exhibit a connection between the generalized Pauli matrices and mutually unbiased bases, and the ability to distinguish states by way of one-way LOCC. The topic of one-way LOCC will be introduced in the next chapter, but this chapter is a means to take a closer look at these generalized Pauli matrices and mutually unbiased bases.

In the realms of mathematics and physics, particularly within quantum information, the term "generalized Pauli matrices" (GPMs) pertains to collections of matrices that extend the algebraic characteristics of the well-known Pauli matrices. These Pauli matrices are complex matrices arising from Pauli's exploration of quantum mechanical spin properties.

In this chapter, we will first go over Weyl-commutative matrices and the Weyl commutation relation. The next section will cover the definitions and properties of the generalized Pauli matrices. Finally, the last section will cover mutually unbiased bases, provide some

details and connect them to the GPMs.

3.1 Weyl Commutation Relation

The understanding of quantum mechanical observables and the scrutiny of their spectral properties are reliant upon the presence of commutation relations among operators within a complex Hilbert space. Consequently, extensive investigation into these relationships has been conducted within the mathematical literature (such as the seminal work by Putnam in the field of commutation [60]). A captivating and interconnected subject involves the commutativity of operator pairs up to a scaling factor. This framework proves advantageous in understanding certain instances of non-commutativity. The well-known canonical (or Heisenberg) commutation relations [56, 62] for position Q and momentum P,

$$[Q, P] = i\hbar\mathcal{I}, \tag{3.1}$$

sometimes written equivalently as

$$QP - PQ \subset i\hbar\mathcal{I}. \tag{3.2}$$

These were be reformulated as the "Weyl relations", which were initially presented using the exponential forms of these operators, given as

$$e^{i\alpha Q}e^{i\beta P} = e^{-i\alpha\beta}e^{i\beta P}e^{i\alpha Q}, \tag{3.3}$$

for all $\alpha, \beta \in \mathbb{C}$ [13, 88]. One of the mathematical reasons for this formulation is that Eq. 3.3 gives unitary operators whereas the operators P and Q satisfying Eq. 3.1 are unbounded necessarily.

Sylvester was the first to introduce these concepts [73]. Later, they were applied to quantum mechanics by von Neumann [80], Weyl [88], and Schwinger [66, 67]. Since then, numerous others have explored these ideas in various scenarios. Over time, the Weyl-commutation relation has been extended to unitary operators within $\mathcal{B}(\mathcal{H})$. We will define this relation below.

Definition 3.1.1. *[13, 57, 83, 87, 97, 98] Let $\mathcal{H} = \mathbb{C}^d$ be a d-dimensional Hilbert space. Two unitary matrices $A, B \in \mathcal{B}(\mathcal{H})$ are called* ***Weyl-commutative matrices*** *if*

$$AB = \omega BA, \tag{3.4}$$

for some $\omega \in \mathbb{C}$, Necessarily, $|\omega| = 1$.

With the Weyl-commutation relation now stated and defined, we can take a look at some useful properties of these matrices. This leads us to the following propositions.

Proposition 3.1.2. *Let $\mathcal{H} = \mathbb{C}^d$ be a d-dimensional Hilbert space. Let $A, B \in \mathcal{B}(\mathcal{H})$ be unitary and Weyl-commutative matrices, such that $AB = \omega BA$. Then ω is a d^{th} root of unity.*

Proof. If $AB = \omega BA$, then the same can be true of their determinants. Using rules of determinants and some algebra, the result is clear;

$$\begin{aligned}
\mathrm{Det}(AB) &= \mathrm{Det}(\omega BA) \\
\mathrm{Det}(AB) &= \omega^d \mathrm{Det}(BA) \\
\mathrm{Det}(A)\mathrm{Det}(B) &= \omega^d \mathrm{Det}(B)\mathrm{Det}(A) \\
\frac{\mathrm{Det}(A)\mathrm{Det}(B)}{\mathrm{Det}(B)\mathrm{Det}(A)} &= \omega^d \\
1 &= \omega^d
\end{aligned}$$

Thus ω is a d^{th} root of unity. $\square$

Proposition 3.1.3. *[54] If A and B are $d\times d$ unitary matrices that obey the Weyl-commutation relation (i.e., $AB = \omega BA$) for some $\omega \neq 1$, then*

$$\mathrm{Tr}(A) = \mathrm{Tr}(B) = \mathrm{Tr}(AB) = 0.$$

Proof. The relation $AB = \omega BA$ is equivalent to $B^*AB = \omega A$. Thus, if we apply the trace operation, we have that

$$\begin{aligned}\mathrm{Tr}(B^*AB) &= \mathrm{Tr}(\omega A)\\ \mathrm{Tr}(BB^*A) &= \omega\mathrm{Tr}(A)\\ \mathrm{Tr}(A) &= \omega\mathrm{Tr}(A).\end{aligned}$$

Since ω is primitive, then $\mathrm{Tr}(A) = \omega\mathrm{Tr}(A)$ is only true if $\mathrm{Tr}(A) = 0$. Analogous reasoning leads to the same result, that $\mathrm{Tr}(B) = 0$.

Now, using trace rules, we can write that

$$\mathrm{Tr}(BA) = \mathrm{Tr}(AB) = \omega\mathrm{Tr}(BA),$$

which leads to $\omega = 1$ or $\mathrm{Tr}(AB) = 0$. Since the former case cannot hold, therefore $\mathrm{Tr}(AB) = 0$. $\square$

Lemma 3.1.4. *[98] If two unitary matrices $A, B \in \mathcal{B}(\mathcal{H})$ do not commute, but satisfy the Weyl-commutation relation, then each eigenvector, $u \in \mathcal{H}$, of B satisfies*

$$\langle u|A|u\rangle = 0. \tag{3.5}$$

Proof. Let two unitary matrices A and B be not commutative, but Weyl-commutative ($AB =$

ωBA holds and $\omega \neq 1$). Suppose u is an eigenvector of B such that $B|u\rangle = \lambda|u\rangle$, where λ is the eigenvalue of A, and satisfies $\lambda\overline{\lambda} = 1$. We also have that $\langle u|B^* = \overline{\lambda}\langle u|$. Therefore

$$\begin{aligned}
\langle u|A|u\rangle &= \langle u|\overline{\lambda}A\lambda|u\rangle \\
&= \langle u|B^*AB|u\rangle \\
&= \langle u|B^*\omega BA|u\rangle \\
&= \omega\langle u|B^*BA|u\rangle \\
&= \omega\langle u|A|u\rangle,
\end{aligned}$$

and thus the result follows. □

We can make a connection to mutually unbiased bases using the above lemma, but first, we require another definition.

Definition 3.1.5. *[17] Given a data set of d data points $\{(x_0, y_0), (x_1, y_1), \ldots, (x_d, y_d)\}$, the* ***Lagrange interpolating polynomial*** *is defined as*

$$p_d(x) = \sum_{k=0}^{d} y_k \mathcal{L}_{d,k}(x), \tag{3.6}$$

where the polynomials $\{\mathcal{L}_{d,k}\}_{k=0}^{d}$ have the property that

$$\mathcal{L}_{d,k}(x_j) = \begin{cases} 0 & \text{if } j \neq k \\ \\ 1 & \text{if } j = k \end{cases}. \tag{3.7}$$

The polynomials $\{\mathcal{L}_{d,k}\}_{k=0}^{d}$ are called the ***Lagrange polynomials*** *for the interpolation points $x_0, x_1, \ldots, x_d$. They are defined by*

$$\mathcal{L}_{d,k}(x) = \prod_{m=0, m\neq k}^{d} \frac{x - x_m}{x_k - x_m}. \tag{3.8}$$

With this definition, we can now state the following theorem.

Theorem 3.1.6. *Let ω be a primitive d^{th} root of unity and let $A, B \in \mathcal{B}(\mathcal{H})$ be two Weyl commutative and unitary matrices satisfying $AB = \omega BA$, both of whose characteristic polynomials are of the form $p(x) = x^d - c$, for some $c \in \mathbb{C}$ with $|c| = 1$. Then the eigenvectors of A and the eigenvectors of B give a mutually unbiased basis pair.*

Proof. Note that if A is Weyl-commutative with B, then it is also Weyl-commutative with B^k for all $k \in \{0, 1, \ldots, d-1\}$. If A does not commute with B^k and u is an eigenvector of A, then $u^* B^k u = 0$ by Lemma 3.1.4, and hence $u^* p(B) u$ can be calculated for Lagrange interpolating polynomial, p, as

$$u^* p(B) u = u^* v v^* u = |\langle u, v \rangle|^2 = \frac{1}{d},$$

where v is an eigenvector of B. Using the spectral theorem, if p is taken to be a Lagrange interpolating polynomial at the eigenvalues of B, then $p(B) = vv^*$ is the eigenvector corresponding to the eigenvalue, λ, for which $p(\lambda) = 1$. □

3.1.1 Matrix Representations for the Weyl Relation

Let $A, B \in \mathbb{C}^{d \otimes d}$ be two unitary matrices that Weyl commute according to $AB = \omega BA$, where ω is a primitive d^{th} root of unity. We will assume that A is invertible and B is not nilpotent as a special case that has a particularly nice matrix representation and will be important in what follows. Then we can say that B is similar to ωB, i.e., $ABA^{-1} = \omega B$. This means that B and ωB have the same eigenvalues.

Let λ be a non-zero eigenvalue of B, then $\omega\lambda$ is also an eigenvalue. By the same logic, we can also see that $\omega^2\lambda$, $\omega^3\lambda$, …, $\omega^{d-1}\lambda$ are distinct eigenvalues of B. Because B has distinct

eigenvalues, B is diagonalizable and we can show this matrix by change of basis, as:

$$\frac{1}{\lambda}B = \begin{pmatrix} 1 & & & & \\ & \omega & & & \\ & & \omega^2 & & \\ & & & \ddots & \\ & & & & \omega^{d-1} \end{pmatrix}. \tag{3.9}$$

Now, let $A = [a_{jk}]$. We can write the product of AB as:

$$AB = [a_{jk}\omega^{k-1}]. \tag{3.10}$$

Similarly, we can write the product of BA and therefore ωBA as:

$$\begin{aligned} BA &= [\omega^{j-1}a_{jk}] \\ \omega BA &= [\omega^{j}a_{jk}]. \end{aligned} \tag{3.11}$$

Looking at the matrix entries, if $j = k - 1 \,(\mathrm{mod}\, d)$, then there is no issue. On the other hand, if $j \neq k - 1 \,(\mathrm{mod}\, d)$, then the only way AB and ωBA will be equal is if $a_{jk} = 0$ when $j \neq k - 1$. So we can write out the matrix representation of A as:

$$A = \begin{pmatrix} & & & & 1 \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{pmatrix}. \tag{3.12}$$

3.2 Generalized Pauli Operators

The generalized Pauli matrices or operators are groups of matrices that extend the mathematical properties of the well-known Pauli matrices. These concepts find significance in mathematics, physics, and particularly in the realm of quantum information. Within the extensive body of literature on this topic, these generalized Pauli operators have been alternately referred to as the "discrete Heisenberg group" or the "finite Weyl-Heisenberg group." They have also been given various other names, such as Schwinger bases [66, 67], Weyl operators [4], and generalized spin operators [58].

From an algebraic perspective, this structure corresponds to a generalized Clifford algebra (GCA) (see section 3.2.3), with two generators that adhere to the aforementioned commutation relation and are referred to as the generalized Pauli operators [69].

3.2.1 Pauli Matrices

The Pauli matrices, often referred to as the Pauli spin matrices, are complex matrices that emerged from Pauli's treatment of spin within quantum mechanics. Every Pauli matrix is Hermitian, and along with the identity matrix, they collectively cover the entire realm of 2×2 Hermitian matrices. In the context of quantum mechanics, Hermitian matrices represent observables. As a result, the Pauli matrices encompass the domain of observables within the 2-dimensional complex Hilbert space.

Definition 3.2.1. *The* ***Pauli matrices*** *are defined as*

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.13}$$

These matrices are also sometimes labelled as $\{\sigma_x, \sigma_y, \sigma_z\}$ *or* $\{\sigma_1, \sigma_2, \sigma_3\}$ *respectively.*

Lemma 3.2.2. *Let $X, Y, Z \in M_2(\mathbb{C})$ be the Pauli matrices. Then these matrices satisfy the following properties:*

- *Algebraic Properties:*
  - ❋ $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathcal{I}$.
  - ❋ $\mathrm{Det}(\sigma_k) = -1$ *for all* $k \in \{1, 2, 3\}$
  - ❋ $\mathrm{Tr}(\sigma_k) = 0$ *for all* $k \in \{1, 2, 3\}$
  - ❋ *eigenvalues*$(\sigma_k) = \pm 1$ *for all* $k \in \{1, 2, 3\}$
- *Commutation relations:*
  - ❋ $\sigma_x \sigma_y = i\sigma_z$
  - ❋ $\sigma_z \sigma_x = i\sigma_y$
  - ❋ $\sigma_y \sigma_z = i\sigma_x$
  - ❋ $\sigma_j \sigma_k = -i\sigma_k \sigma_j$ *for* $j \neq k$.

3.2.2 Generalized Pauli Operators and Generalized Bell States

Consider a finite-dimensional Hilbert space of dimension d. We can associate generalized Pauli matrices (GPMs) by equipping the space $\mathcal{B}(\mathcal{H})$ with two unitary operators (called generators), of the group, and label them as X and Z, which satisfy the Weyl-commutation relation

$$XZ = \omega ZX, \tag{3.14}$$

with $\omega = e^{\frac{2\pi i}{d}}$. In addition to being unitary, these operators also satisfy the following toroidal property [69] that

$$X^d = Z^d = \mathcal{I}. \tag{3.15}$$

We can define these generalized Pauli operators below and see how they act on states in a Hilbert space.

Definition 3.2.3. *[43] Let $\mathcal{H} = \mathbb{C}^d$ be the qudit d-dimensional Hilbert space with orthonormal basis $\{|k\rangle\}_{k=0}^{d-1}$ and let $\omega = e^{\frac{2\pi i}{d}}$. We define two unitary operators X and Z on $\mathcal{B}(\mathcal{H})$ as*

$$X|k\rangle = |k+1 \,(\mathrm{mod}\, d)\rangle,\ Z|k\rangle = \omega^k|k\rangle. \tag{3.16}$$

*Then the **generalized Pauli operators** are the set:*

$$U_{m,n} = \{X^m Z^n\}_{n,m=0}^{d-1}. \tag{3.17}$$

We can write these matrices as a sum of tensor states [28] as

$$X = \sum_{k=0}^{d-1} |k+1 \,(\mathrm{mod}\, d)\rangle\langle k|,\ Z = \sum_{k=0}^{d-1} \omega^k |k\rangle\langle k|. \tag{3.18}$$

We note that these were given as matrix representations above (see Section 3.1.1).

Observation 3.2.4. *We can see that the set of d^2 unitaries $\{U_{m,n}\}_{m,n=0}^{d-1} = \{X^m Z^n\}_{n,m=0}^{d-1}$ is an orthonormal base in the operator space $\mathbb{C}^d \otimes \mathbb{C}^d$,*

$$\mathrm{Tr}(U_{m,n}^* U_{m',n'}) = d\delta_{m,m'}\delta_{n,n'}.$$

Remark 3.2.5. *A note on the notation of the generalized Pauli operators. We can use a short form to represent these operators according to*

$$U_{m,n} = \{X^m Z^n\} = \{(m,n)\}.$$

Lemma 3.2.6. *[46] Any pair of generalized Pauli matrices are Weyl commutative. In fact,*

for two pairs of generalized Pauli operators $(m_j, n_j), (m_k, n_k) \in \mathbb{Z}_d \times \mathbb{Z}_d$*, we have*

$$X^{m_j} Z^{n_j} X^{m_k} Z^{n_k} = \omega^{m_k n_j - m_j n_k} X^{m_k} Z^{n_k} X^{m_j} Z^{n_j}.$$

Moreover, $X^{m_j} Z^{n_j}$ *and* $X^{m_k} Z^{n_k}$ *are commutative if and only if* $m_k n_j - m_j n_k \equiv 0 (\mathrm{mod}\, d)$*. This condition can be formulated as the determinant equation according to*

$$\begin{vmatrix} m_j & n_j \\ m_k & n_k \end{vmatrix} = 0.$$

With these generalized Pauli operators, we can use them to state the maximally entangled state (MES) and the generalized Bell states (GBSs).

The significance of maximally entangled states lies in their non-local nature. When two quantum systems are maximally entangled, any change or measurement made on one system instantaneously affects the other system, regardless of the spatial separation between them. This phenomenon is known as "spooky action at a distance" [27] and is a remarkable aspect of quantum entanglement.

Definition 3.2.7. *The standard* ***maximally entangled state*** *(MES) is given by*

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle \otimes |k\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d. \tag{3.19}$$

It is known that $(\mathcal{I} \otimes U)|\Phi\rangle = (U^T \otimes \mathcal{I})|\Phi\rangle$*, where "*$T$*" is the transpose operation, for any unitary matrix,* $U \in \mathcal{B}(\mathcal{H})$*. In general, any maximally entangled state can be written as* $|\psi\rangle = (\mathcal{I} \otimes U)|\Phi\rangle$*, where* U *is a unitary matrix.*

Definition 3.2.8. *[43, 46, 84, 93, 96] A maximally entangled state of the form:*

$$|\psi_{m,n}\rangle = (\mathcal{I} \otimes U_{m,n})|\Phi\rangle = (\mathcal{I} \otimes X^m Z^n)|\Phi\rangle, \tag{3.20}$$

is called a ***generalized Bell state*** *(GBS), where* $|\Phi\rangle$ *is as defined above.*

Remark 3.2.9. *When dealing with sets of generalized Bell states, we will call these sets,* $\mathcal{S}$ *and denote them as*

$$\mathcal{S} := \{|\psi_{m_k,n_k}\rangle\}_{k=0}^{d-1} \equiv \{X^{m_k}Z^{n_k}\}_{k=0}^{d-1} \equiv \{(m_k,n_k)\}_{k=0}^{d-1}. \tag{3.21}$$

Definition 3.2.10. *[96] For a set of GBSs,* $\mathcal{S} = \{(m_k,n_k)\}_{k=0}^{d-1} \in \mathbb{C}^d \otimes \mathbb{C}^d$*, the corresponding pairwise difference set, denoted as* $\Delta\mathcal{S}$*, means*

$$\Delta\mathcal{S} = \{(m_{jk},n_{jk}) : m_{jk} = m_j - m_k \in \mathbb{Z}_d, n_{jk} = n_j - n_k \in \mathbb{Z}_d, j \neq k\}. \tag{3.22}$$

The generalized Pauli operators form a subgroup of the $d \times d$ unitary matrices, which correspond to maximally entangled quantum states. Any pair of unitary matrices have a "simultaneous Schmidt decomposition" (see next definition) [78]; and we can derive a necessary and sufficient condition for larger sets of unitaries as well.

Definition 3.2.11. *[43] We say that a set of states* $\{(I \otimes M_k)|\psi_i\rangle\}_{k=0}^{d}$ *have a* ***simultaneous Schmidt decomposition*** *if there exists two unitary matrices* U *and* V *and* d *complex diagonal matrices,* D_k*, such that for each* k*,* $M_k = UD_kV$*.*

These decompositions are not strictly speaking Schmidt decompositions and are instead called "weak Schmidt decompositions" because we are not imposing any requirement that the entries of the diagonal matrices D_k be non-negative.

Proposition 3.2.12. *[43] Let* $M_j, M_k \in \mathcal{B}(\mathcal{H})$ *be two* $d \times d$ *complex matrices. Then here exists a* $d \times d$ *unitary matrix,* A*, such that* $\Delta(A^*M_k^*M_jA) = 0$ *when* $i \neq j$*, where* Δ *is the map that zeros out all the off-diagonal entries of a square matrix of a given size but leaves its diagonal entries unchanged.*

Observation 3.2.13. *We note that the sets* $\{X^k\}_{k=0}^{d-1}$ *and* $\{Z^k\}_{k=0}^{d-1}$ *form Abelian groups. We can also see that these operators satisfy the condition of the previous proposition (with these operators playing the role of the operators* M_j, M_k*).*

3.2.3 Clock and Shift Matrices

Recall from Definition 3.2.3, we described a construction of the generalized Pauli matrices as $\{X^m Z^n\}_{n,m=0}^{d-1}$. There are other unique constructions of these matrices. A particularly notable generalization of the Pauli matrices was constructed by Sylvester [73] in 1882.

Using the known properties of the 2-dimensional Pauli matrices, including the algebraic and commutation relations, as well as the Walsh–Hadamard conjugation matrix (typically shortened to Hadamard matrix) relation that $\sigma_x = W\sigma_3 W^*$, where

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.23}$$

The goal of this construction was to extend these to higher dimensions, d.

Before stating these clock and shift matrices, we can first cover the topic of Clifford algebras and generalized Clifford algebras, as the structure of these matrices corresponds to a generalized Clifford algebra (GCA). The relationship between Clifford algebras and the generalized Pauli matrices arises from the fact that the algebra of observables for a quantum system can be represented using a Clifford algebra. Specifically, the algebra of observables is represented by a sub-algebra of the Clifford algebra associated with the Hilbert space. This sub-algebra is generated by a set of matrices that can be identified with the generalized Pauli matrices.

Definition 3.2.14. *A **quadratic form** is a function $f : \mathbb{F}^n \to \mathbb{F}$ of form*

$$f(x) = x^T Ax, \tag{3.24}$$

where A is an $n \times n$ symmetric matrix.

With this, we can state the definition of Clifford algebras.

Definition 3.2.15. *[22] Let V be a vector space over the field $\mathbb{F}$ and let Q be a quadratic form on V, valued in $\mathbb{F}$. The **Clifford algebra**, denoted as Cliff(Q), is the algebra over $\mathbb{F}$ generated by V and defined by the relations*

$$v_1 v_2 + v_2 v_1 = 2Q(v_1, v_2) \cdot 1, \tag{3.25}$$

for $v_1, v_2 \in V$, and where 1 is the unit, considered to be the multiplicative identity in the ground field $\mathbb{F}$.

Definition 3.2.16. *[34, 81] The **generalized Clifford algebra** is a unital associative algebra over the field, $\mathbb{F}$, that generalizes the d-dimensional Clifford algebra, and is generated by*

$$e_j e_k = \omega e_k e_j,$$

$$\omega e_l = e_l \omega,$$

$$e_k^d = 1 = \omega^d$$

for all $j, k, l \in \{1, 2, \ldots, d\}$ and orthonormal basis $\{e_k\}_{k=1}^d \in \mathbb{C}^d$, with $\omega = e^{\frac{2\pi i}{d}}$ being the primitive d^{th} root of unity.

Definition 3.2.17. *Let $\mathcal{H}$ be a d-dimensional Hilbert space, and let $\omega = e^{\frac{2\pi i}{d}}$ be a primitive d^{th} root of unity. The **Clock and Shift matrices**, first defined by Sylvester [73], sometimes*

called the "Weyl-Heisenberg matrices" and "generalized Pauli matrices" [2, 32, 87], are defined as the following $d \times d$ matrices,

$$X_{shift,+} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}_{d\times d}, \; Z_{clock} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \omega & 0 & \dots & 0 \\ 0 & 0 & \omega^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \omega^{d-1} \end{pmatrix}_{d\times d}. \tag{3.26}$$

$X_{\text{shift},+}$ has all 1's on the *sub-diagonal* and a 1 in the *top right* entry with zeros everywhere else. Z has all elements in the main diagonal where each entry increases the power on ω by 1, up to $d-1$.

These matrices generalize the above-defined Pauli matrices σ_1 and σ_3. In some literature, these matrices are often labelled as Σ_1 and Σ_3 respectively, instead of X and Z. We will use these labels interchangeably. Just as stated in Definition 3.2.3, the generalized Pauli matrices are the operators $U_{m,n} = \{X^m Z^n\}_{n,m=0}^{d-1}$.

Remark 3.2.18. *In some other literature, [36, 37, 61, 71], the shift matrix is represented differently. We previously stated that the operator X acts on a state as: $X|k\rangle = |k+1 \,(\mathrm{mod}\, d)\rangle$. In other literature, this definition is changed according to*

$$X|k\rangle = |k-1 \,(\mathrm{mod}\, d)\rangle, \tag{3.27}$$

and so the shift matrix, X, is now represented by

$$X_{shift,-} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}_{d\times d} . \tag{3.28}$$

Notice that $X_{\text{shift},-}$ now has all 1's on the *super-diagonal* and a 1 in the *bottom left* entry with zeros everywhere else.

Remark 3.2.19 (Notation)**.** *We denote which version of the shift matrix we are referring to by adding a "+" or "−" sign in the subscript, as seen here. As a default, we will drop these subscripts and take the "+" case.*

It's worth noting that the tracelessness and unitarity found in the Pauli matrices carry over to these new clock and shift matrices. However, when moving beyond dimensions of 2, these matrices no longer maintain their Hermitian nature. These two matrices hold crucial significance as foundational components in Weyl's description of quantum mechanical dynamics within finite-dimensional vector spaces [64, 87, 88], finding extensive application across various domains of mathematical physics. The shift matrix functions as a straightforward translation operator within a cyclic vector space. On the other hand, the clock matrix is equivalent to the exponential of a position within a "clock" consisting of d hours. In finite dimensions, they represent the corresponding elements of the Weyl-Heisenberg group on a d-dimensional Hilbert space.

The following properties also echo and generalize the Pauli matrices.

Lemma 3.2.20. *Let X and Z be the Shift and Clock matrices respectively, as defined above.*

Then the following properties are satisfied:

- $\Sigma_1^d = \Sigma_3^d = \mathcal{I}_d$
- $\Sigma_1\Sigma_3 = \omega\Sigma_3\Sigma_1$
- $\Sigma_1\Sigma_3\Sigma_1^{d-1}\Sigma_3^{d-1} = \omega$

Corollary 3.2.21. *[72]With these generalized matrices, the Hadamard matrix can also be generalized. Note that in the $d = 2$ case:*

$$W = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & \omega^{2-1} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & \omega^{d-1} \end{pmatrix}.$$

And so in d-dimensions, this is extended to

$$\Rightarrow W = \frac{1}{\sqrt{d}}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^{d-1} & \omega^{2(d-1)} & \dots & \omega^{(d-1)(d-1)} \\ 1 & \omega^{d-2} & \omega^{2(d-2)} & \dots & \omega^{(d-1)(d-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega & \omega^2 & \dots & \omega^{d-1} \end{pmatrix}_{d\times d}. \tag{3.29}$$

In this matrix, we see that W is no longer Hermitian, but its unitarity is preserved. We can also see the relation that $\Sigma_1 = W\Sigma_3 W^*$. Thus, W arrays the eigenvectors of Σ_1, which has the same eigenvalues as Σ_3.

3.3 Mutually Unbiased Bases

In general, a collection of MUBs comprises of bases that are all pairwise unbiased. The maximal sets of MUBs, with the exception of certain Hilbert space dimensions (specifically prime-dimensional Hilbert spaces), are generally unknown [4, 58, 59, 91].

Theorem 3.3.1. *[71] In an d-dimensional Hilbert space, there cannot be more than $d+1$ mutually unbiased bases.*

The proof of this theorem for the prime case can be seen in the paper by I. Ivanovic [33]. These sets are maximal in the sense that it is not possible to find more than $d+1$ MUBs in any d-dimensional Hilbert space. We have seen the result for dimension d, but this result has also been proven for prime powers [91].

Below, we provide an alternative proof of this theorem inspired by Daniel P. May [47], using the *Gram matrix* [70]. Before detailing this proof, we introduce the notion of the *Hadamard product* [30], as we will use this concept in the proof.

Definition 3.3.2. *Let A and B be two $m \times n$ matrices with entries in $\mathbb{C}$. The **Hadamard product**, or **Schur product** [16], of A and B is defined by*

$$[A \circ B]_{ij} = [A]_{ij}[B]_{ij} \tag{3.30}$$

for all $1 \leq i \leq m$ and $1 \leq j \leq n$.

We can add the condition that A and B are positive definite matrices.

Proof. [47] A set of m mutually unbiased bases of $\mathbb{C}^d$ gives a set of md unit vectors, $\{v_1, v_2, \ldots, v_{md}\}$, where these vectors are ordered such that the first d vectors come from the first MUB, the next set of d vectors are from the second MUB and so on. Thus, we can define the matrix $V = v_j v_j^*$ with a note that each of these matrices is Hermitian.

The set of all $d \times d$ Hermitian matrices is a real vector space, $Herm(d)$, where d is the dimension, with an inner product $Herm(d) \times Herm(d) \to \mathbb{R}$ defined by $\langle A, B \rangle = \mathrm{Tr}(AB)$ for all $A, B \in Herm(d)$.

From here, we introduce a new matrix, the Gram matrix, $\mathcal{G}$, which has entries of the

form $[\langle v_i, v_j \rangle]_{ij}$:

$$\mathcal{G} = \begin{pmatrix} \mathcal{I}_d & * & \dots & * \\ * & \mathcal{I}_d & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \dots & \mathcal{I}_d \end{pmatrix}_{md \times md} \tag{3.31}$$

where we have m blocks. Also, note that this matrix is positive semi-definite (PSD).

As a next step, we consider the complex conjugate of $\mathcal{G}$, that is, $\overline{\mathcal{G}}$. Observe that this is just equal to its transpose and is still PSD. We now take the Schur product and form our new matrix:

$$\mathcal{G} \circ \overline{\mathcal{G}} = \begin{pmatrix} \mathcal{I}_d & \frac{1}{d} J_d & \dots & \frac{1}{d} J_d \\ \frac{1}{d} J_d & \mathcal{I}_d & \dots & \frac{1}{d} J_d \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{d} J_d & \frac{1}{d} J_d & \dots & \mathcal{I}_d \end{pmatrix}_{md \times md} \tag{3.32}$$

where J_d is the $d \times d$ matrix with all 1's as its entries.

We can verify the form of this matrix. Notice that

$$[\mathcal{G} \circ \overline{\mathcal{G}}]_{i,i} = \mathrm{Tr}(V_i V_i) = \mathrm{Tr}(v_i v_i^* v_i v_i^*) = \mathrm{Tr}(v_i v_i^*) = \mathrm{Tr}(V_i) = 1.$$

Note that $\mathrm{Tr}(v_i v_i^*) = \mathrm{Tr}(V_i) = 1$ because the v_i's are unit vectors. Further, if v_i and v_j are different vectors from the same orthonormal basis, then $v_i^* v_j = 0$, so

$$[\mathcal{G} \circ \overline{\mathcal{G}}]_{i,j} = \mathrm{Tr}(V_i V_j) = \mathrm{Tr}(v_i v_i^* v_j v_j^*) = 0.$$

Finally, if v_i and v_j are from different bases, then

$$[\mathcal{G} \circ \overline{\mathcal{G}}]_{i,j} = \mathrm{Tr}(V_i V_j) = \mathrm{Tr}(v_j^* v_i v_i^* v_j) = |\langle v_i, v_j \rangle| = \frac{1}{d}.$$

Thus, the matrix $\mathcal{G} \circ \overline{\mathcal{G}}$ form is verified. We note that $\mathcal{G} \circ \overline{\mathcal{G}}$ has 0 as an eigenvalue, with the corresponding eigenvector

$$\Big(1, 1, \ldots, 1, -1, -1, \ldots, -1, 0, 0, \ldots 0\Big)^T,$$

where there are d 1's, d -1's and $d(m-2)$ 0's. Any eigenvector of $\mathcal{G} \circ \overline{\mathcal{G}}$ corresponding to the eigenvalue 0 must have a similar form, containing d consecutive 1's and d consecutive -1's, with the remaining entries 0. Thus, the basis of the kernel of $\mathcal{G} \circ \overline{\mathcal{G}}$ is

$$\begin{aligned}\Big\{ &\Big(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0, 0, \ldots, 0\Big)^T, \\ &\Big(1, \ldots, 1, 0, \ldots, 0, -1, \ldots, -1, 0, \ldots, 0\Big)^T, \ldots, \\ &\Big(1, \ldots, 1, 0, \ldots, 0, 0, \ldots, 0, -1, \ldots, -1\Big)^T \Big\}\end{aligned}$$

There are $m-1$ possible choices for the placement of the -1's, so the nullity of $\mathcal{G} \circ \overline{\mathcal{G}}$ is $m-1$ and thus $rank(\mathcal{G} \circ \overline{\mathcal{G}}) = md - m + 1$.

A property of the Gram matrix that involves its rank, states that if $v_j \in V$ for some vector space, V, then $rank(\mathcal{G}) \leq \dim(V)$, for positive semi-definiteness. Since we have a set of m MUBs of dimension d, we know that $rank(\mathcal{G}) \leq d$. Note that $rank(\overline{\mathcal{G}}) \leq d$ as well. By decomposing the Schur product matrix into rank 1 matrices, we can observe that $rank(\mathcal{G} \circ \overline{\mathcal{G}}) \leq d^2$:

$$rank(\mathcal{G} \circ \overline{\mathcal{G}}) = dim(span(\{V_i\})) \leq dim(Herm(d)) = d^2.$$

With this, we set up the equation using both expressions related to the rank:

$$md + m - 1 \leq d^2. \tag{3.33}$$

With a bit of algebra, we obtain our result that $m \leq d+1$, and thus we have found an upper bound for positive semi-definiteness and thus an upper bound for the number of MUBs in a Hilbert space of dimension d. □

The initial instance of ambiguity arises in the situation when $d = 6$. This dimension holds significance as it's the smallest that cannot be expressed as an integer power of a prime. Additionally, it stands as the smallest dimension for which the number of mutually unbiased bases remains unknown. The methods employed to enumerate mutually unbiased bases when d is an integer power of a prime number cannot be directly applied in this case. For the specific scenario of $d = 6$, efforts to identify a collection of four mutually unbiased bases using Hadamard matrices [7] and numerical techniques [11] have proven unsuccessful.

Lemma 3.3.3. *In any dimension, there is an example where a basis is mutually unbiased to the standard basis. In a single element, every entry will have the same modulus, for example,*

$$v = \frac{1}{\sqrt{d}}(\omega_1, \omega_2, \ldots, \omega_d) \in \mathbb{C}^d.$$

Any orthonormal basis of this form will be mutually unbiased to the standard basis given by $\{e_1, e_2, \ldots, e_d\}$ *where* e_k *are the usual standard basis vectors.*

Lemma 3.3.4. *Consider the vector from the previous theorem, with* $|\omega| = 1$*. Any orthonormal basis with vectors of this form is mutually unbiased to the standard basis* $(e_1, e_2, ..., e_n)$*. Now let us consider*

$$v_\omega = \frac{1}{\sqrt{n}}(1, \omega^1, \omega^2, ..., \omega^n),$$

(call this the "Vandermonde" vector [38]). If we take the inner product of two of these vectors, we see

$$\langle v_{\omega_1}, v_{\omega_2} \rangle = \frac{1}{n} \sum_{k=0}^{n-1} (\omega \bar{z})^k = \frac{1 - (\omega \bar{z})^n}{n(1 - \omega \bar{z})}.$$

For orthogonality, $\omega\bar{z}$ would need to be an n^{th} root of unity. For v_{ω_1} and v_{ω_2} to be mutually unbiased, we would then consider the magnitude and set the absolute value equal to $\frac{1}{\sqrt{n}}$.

3.3.1 Proof that the eigenbases of the GPMs form a set of $d+1$ MUBs when d is prime

We can see an important theorem now which shows that if we have two bases consisting of eigenvectors for two unitary matrices, then we can show they these form a mutually unbiased pair.

This section follows the work presented in [4] and [79].

Theorem 3.3.5. *Let $\mathcal{B}_1 = \{a_0, a_1, \ldots, a_{d-1}\}$ be the orthonormal basis of $\mathbb{C}^d$. Suppose that there is a unitary operator V such that $V|a_j\rangle = \omega_j|a_{j+l}\rangle$, where $|\omega_j| = 1$ and $\gcd(l, d) = 1$. If $\mathcal{B}_2 = \{b_0, b_1, \ldots, b_{d-1}\}$ is the orthonormal basis consisting of the eigenvectors of V, then $\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased.*

Proof. Suppose that the eigenvector $|b_k\rangle$ is associated with the eigenvalue λ_k, that is $V|b_k\rangle = \lambda_k|b_k\rangle$. Since V is unitary we have $V^{-1} = V^*$, so $V^*|b_k\rangle = \lambda_k^{-1}|b_k\rangle$, and:

$$\langle a_j|V^*|b_k\rangle = \lambda_k^{-1}\langle a_j|b_k\rangle,$$
$$\langle b_k|V|a_j\rangle = \omega_j\langle b_k|a_{j+l}\rangle.$$

If we combine these two equations, we get:

$$\langle a_j|b_k\rangle^* = \lambda_k^*\langle a_j|V^*|b_k\rangle^* = \lambda_k^*\langle b_k|V|a_j\rangle = \lambda_k^*\omega_j\langle b_k|a_{j+l}\rangle.$$

If we note that $|\lambda_k| = |\omega_j| = 1$, and we apply the last equation several times, we can observe that:

$$|\langle b_k|a_j\rangle| = |\langle b_k|a_{j+l}\rangle| = |\langle b_k|a_{j+2l}\rangle| = \cdots = |\langle b_k|a_{j+(d-1)l}\rangle|.$$

Since $\gcd(l,d)=1$ we have $\{l,2l,\ldots,dl\}=\{0,1,\ldots,d-1\} \bmod d$. Taking $j=0$:

$$|\langle b_k|a_0\rangle| = |\langle b_k|a_1\rangle| = |\langle b_k|a_2\rangle| = \cdots = |\langle b_k|a_{d-1}\rangle|.$$

Since $\mathcal{B}_1$ and $\mathcal{B}_2$ are orthonormal bases, we know that $1 = ||b_k||^2 = \sum_j |\langle b_k|a_j\rangle|^2$. Therefore, we can conclude:

$$|\langle b_k|a_j\rangle|^2 = \frac{1}{d},$$

for all $0 \leq j \leq d-1$. □

We can take this theorem even further. If we let $\{v_j\}_{j=0}^{d-1}$ be the orthonormal basis $\mathcal{B}_1$, and let the unitary, U, be defined as: $U = \sum_{m=1}^{d} w^m v_m v_m^*$. Then from this, we can observe that since $UVv_j = w^{j+l}v_{j+l}$ and $VUv_j = w^j v_{j+l}$, then by linearity $UV = w^l VU$, which means that U and V Weyl-commute (This is touched on in the next section), and hence we see that two Weyl-commuting matrices form a mutually unbiased pair.

We can extend this theorem by looking back at the generalized Pauli matrices. We will show that for any prime d, the set of bases consisting of the normalized eigenvectors of the $X_d, Z_d, X_dZ_d, X_d(Z_d)^2, \ldots, X_d(Z_d)^{d-1}$ form a set of $d+1$ mutually unbiased bases.

Lemma 3.3.6. *[4, 79] Let d be odd. Then the t^{th} eigenvector of $X_d(Z_d)^k$ is given as*

$$|\psi_t^k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (\omega_d^t)^{d-j} (\omega_d^{-k})^{s_j} |j\rangle, \tag{3.34}$$

where $s_j = j + \cdots + (d-1), 0 \leq t \leq d-1$.

Proof. [4] By computation:

$$\begin{aligned}
X_d(Z_d)^k|\psi_t^k\rangle &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}(\omega_d^t)^{d-j}(\omega_d^{-k})^{s_j}X_d(Z_d)^k|j\rangle \\
&= \frac{1}{\sqrt{d}}\left(\sum_{j=0}^{d-2}(\omega_d^t)^{d-j}(\omega_d^{-k})^{s_j}\omega_d^{kj}|j+1\rangle + \omega_d^t(\omega_d^{-k})^{d-1}\omega_d^{k(d-1)}|0\rangle\right) \\
&= \frac{\omega_d^t}{\sqrt{d}}\left(\sum_{j=0}^{d-2}(\omega_d^t)^{d-(j+1)}(\omega_d^{-k})^{s_{j+1}}|j+1\rangle + |0\rangle\right) \\
&= \frac{\omega_d^t}{\sqrt{d}}\left(\sum_{j=0}^{d-1}(\omega_d^t)^{d-j}(\omega_d^{-k})^{s_j}|j\rangle + (\omega_d^t)^d(\omega_d^{-k})^{s_0}|0\rangle\right) \\
&= \frac{\omega_d^t}{\sqrt{d}}\left(\sum_{j=0}^{d-1}(\omega_d^t)^{d-j}(\omega_d^{-k})^{s_j}|j\rangle\right) \\
&= \omega_d^t|\psi_t^k\rangle,
\end{aligned}$$

where in the fourth line, we simplify by observing that $\omega_d^d = 1$ and $\omega_d^{s_0} = \omega_d^{\frac{d(d-1)}{2}} = 1$. □

Next, we can determine the effects of $X_d(Z_d)^l$ on the eigenvectors of $X_d(Z_d)^k$.

Lemma 3.3.7. *[4, 79] Let d be an odd number. Then*

$$X_d(Z_d)^l|\psi_t^k\rangle = \omega_d^{t+k-l}|\psi_{t+k-l}^k\rangle. \tag{3.35}$$

Proof. [4] By computation:

$$\begin{aligned}
X_d(Z_d)^l|\psi_t^k\rangle &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}(\omega_d^t)^{d-j}(\omega_d^{-k})^{s_j}X_d(Z_d)^l|j\rangle \\
&= \frac{1}{\sqrt{d}}\left(\sum_{j=0}^{d-2}(\omega_d^t)^{d-j}(\omega_d^{-k})^{s_j}\omega_d^{lj}|j+1\rangle + \omega_d^t(\omega_d^{-k})^{d-1}\omega_d^{l(d-1)}|0\rangle\right) \\
&= \frac{\omega_d^{t+k-l}}{\sqrt{d}}\left(\sum_{j=0}^{d-2}(\omega_d^t)^{d-(j+1)}(\omega_d^{-k})^{s_{j+1}}\omega_d^{(l-k)(j+1)}|j+1\rangle + |0\rangle\right) \\
&= \frac{\omega_d^{t+k-l}}{\sqrt{d}}\left(\sum_{j=0}^{d-1}(\omega_d^{t+k-l})^{d-j}(\omega_d^{-k})^{s_j}|j\rangle + |0\rangle\right) \\
&= \omega_d^{t+k-l}|\psi_{t+k-l}^k\rangle.
\end{aligned}$$

□

From these computations and lemmas from the cited references, we can take inspiration and generate a proof of the upper bound on the number of MUBs using a dimension-counting argument rather than a rank argument as used in the proof where we used the idea of the Gram matrix above.

Theorem 3.3.8. *In any dimension d, the number of mutually unbiased bases is at most $d+1$.*

Proof. Let $U_1, U_2, \ldots, U_m$ be unitary matrices whose columns are the orthonormal vectors from the mutually unbiased bases $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m$. Let V_0 represent the subspace of all trace zero $d \times d$ matrices. Consider the following linear map:

$$\begin{aligned}
&L : (D_d^0)^m \to M_d, \\
&L : (D_1, D_2, \ldots, D_m) \to \sum_{k=1}^{m} U_k D_k U_k^*,
\end{aligned} \tag{3.36}$$

where $(D_d^0)^m$ is the space of all trace zero diagonal matrices. Note that this space is of

dimension $m(d-1)$.

The question we now want to consider is what is the dimension of the forward image of L? We make the claim that L is in fact an invertible map because the kernel of L is zero. We prove this claim using a method of contradiction:

Suppose this map is not invertible, then there exists $A_1, A_2, \ldots, A_m$ trace zero matrices that are not all zero, such that

$$\sum_{k=1}^{m} U_k A_k U_k^* \neq 0.$$

Let us choose j such that $A_j \neq 0$. Solving for A_j and using the mutually unbiased basis condition, we see that:

$$A_j = -\sum_{j \neq k} (U_j^* U_k) A_k (U_j^* U_k)^*.$$

A nice thing we can observe here is that A_j is a diagonal matrix and the right-hand side of the previous equation has constant diagonal entries and zero trace. Therefore, the right-hand side of the equation must be equal to zero, which is a contradiction.

So we have the L is an invertible map, and hence, $\mathrm{Dim}(L((D_d^0)^m)) = m(d-1)$. Then, it is clear that this will be less than or equal to the dimension of the space of all trace zero matrices, i.e.,

$$m(d-1) \leq d^2 - 1. \tag{3.37}$$

With a bit of algebra, we can conclude that:

$$\begin{aligned} m(d-1) &\leq d^2 - 1 \\ m &\leq \frac{d^2-1}{d-1} \\ m &\leq \frac{(d-1)(d+1)}{d-1} \\ m &\leq d+1, \end{aligned}$$

which is the desired result. □

We have established that this upper bound is known, so we can look at an example to see this theorem in action by considering the case of $d = 3$.

Example 3.3.9. *Let $d = 2$, $\omega_2 = e^{\frac{2\pi i}{2}} = e^{\pi i} = -1$. The set of eigenvectors of the following 3 (i.e., $2 + 1$) generalized Pauli operators form a set of 3 MUBs:*

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

We define the standard basis, $\{|k\rangle\}_{k=0}^{d-1}$ to be the set of vectors whose entries are all zeros except in the k^{th} position. Then the MUBs are:

$$\begin{aligned} \mathcal{B}_2 &= \{|0\rangle, |1\rangle\} \\ \mathcal{B}_2^0 &= \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\} \\ \mathcal{B}_2^1 &= \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\} \end{aligned}$$

Observation 3.3.10. *If $d = p_1 p_2$ where $p_1 < p_2$ are prime numbers, then $\mathcal{B}_d, \mathcal{B}_d^0, \ldots, \mathcal{B}_d^{p_1 - 1}$ are mutually unbiased. This, therefore, gives us a collection of $p_1 + 1$ mutually unbiased bases which is known to be the best lower bound for the present case.*

Chapter 4

Distinguishability by Quantum LOCC and Mutually Unbiased Bases

A method used in quantum information theory called "local operations and classical communication," or LOCC, involves performing a local quantum (product) operation on one part of a system and then "communicating" the results to another part, where typically another local operation is carried out based on the information obtained. In addition to having potential uses in communication, data concealing, and cryptography, the study of the strengths and weaknesses of LOCC is intrinsically interesting as a way to comprehend entanglement [51].

Despite significant advancements in recent years, entanglement continues to be one of the most puzzling aspects of the quantum world. Several quantum protocols are based on the interaction between entanglement and locality. Concentrating or distilling the entanglement of a particular state is one of the problems involved in quantum information theory. There are essentially two categories of protocols that try to carry out such responsibilities. The first one is founded on quantum non-local measurements on several copies of the original state. The other exclusively addresses local operations on the state's only copy, including any

possible classical communication (LOCC). As local measurements may be made more easily than non-local ones, they are thus of particular interest from an experimental perspective [74].

LOCC is essential for the characterization and general comprehension of quantum entanglement because it provides a practical framework for studying and manipulating entangled quantum systems. LOCC operations involve locally manipulating and measuring quantum states while communicating the measurement outcomes classically [35, 51, 74, 75, 76, 86].

From the point of view of quantum communication, LOCC protocols are critical, as there is no ideal communication channel in the real world. So, it is only logical to explore how much entanglement can be extracted from the imperfectly entangled states that result, for instance, when two observers share a completely entangled state using just LOCC.

In the previous chapter, we discussed the topics of Weyl-commuting matrices, the generalized Pauli matrices and mutually unbiased bases. These concepts have many applications in the context of quantum state distinguishability. A special result from M. Nathanson [50] details the connection between LOCC and MUBs, and provides insight into how a set of states can be distinguished by one-way LOCC. This particular result looks at the concept of common unbiased bases, which are directly connected to mutually unbiased bases. We can also observe the applications of the Weyl commutation relation and its application in LOCC distinguishability. For this, we look at two papers from J. Yuan et al. [97] and Y. Yang et al. [94]. The takeaway result states that for a set of maximally entangled states whose unitaries are in the Weyl basis (the set of all matrices which Weyl commute with each other), the states can be perfectly distinguished by 1-LOCC if and only if they meet a certain condition. In total, the content of the previous section can be applied in the context of LOCC with great success, and the rest of this chapter will detail this further.

4.1 LOCC Operations and Discrimination

In the context of local bipartite quantum state discrimination, the scenario involves two parties, each responsible for a quantum system denoted by the finite-dimensional spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. Their collective system, represented as $\mathcal{H}_A \otimes \mathcal{H}_B$, has been initially prepared in a pure state chosen from a predefined set of states. Subsequently, the individual two-component systems are separated. Alice and Bob are both aware of this set of states and aim to determine which specific state was selected from this set. Due to their physical separation, their feasible measurement strategies are limited to those that solely employ local quantum operations and classical communication (LOCC).

Example 4.1.1. *Consider two observers, Alice (A) and Bob (B), who share the following Bell states:*

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B),$$

and are provided with a classical communication channel (a phone or the internet, etc.).

In this example, Alice and Bob can choose one of the two shared states, but they are missing the information about which state it is exactly. Alice and Bob can distinguish between these two states using LOCC. To do this, Alice only needs to measure her qubit and communicate to Bob the results of her measurement. After receiving this information, Bob now has to perform a measurement on his qubit. The result of this will tell Alice and Bob which state they have. For example, if Alice measured 0 and Bob measured 1, then they both had the state $|\Psi^-\rangle$. Thus with LOCC and two measurements, these two states can be distinguished perfectly.

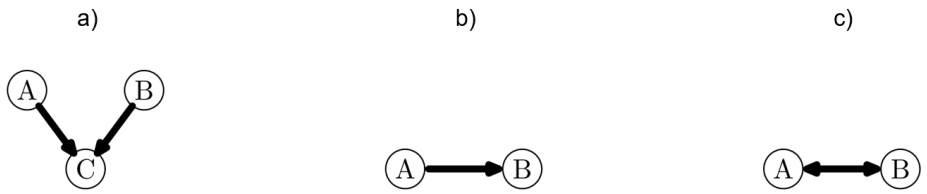

Figure 4.1: Schematic description for (a) local operations (b) one-way LOCC (c) full (two-way) LOCC.

4.2 LOCC Schemes

On the basis of how classical communication is employed, the class of bipartite LOCC measures can be further broken down. Local product measurements involve Alice and Bob conducting measurements independently, subsequently exchanging information to compare and evaluate their results. In the case of one-way LOCC, Bob might adjust his measurements based on Alice's classical information, but information flow in the opposite direction is restricted. Lastly, full (two-way) LOCC enables Alice and Bob to communicate classically as extensively as needed and allows them to iteratively modify their measurements throughout the process. We can visually observe these distinctions by taking a look at the schematic presented by M. Nathanson [51], in Figure 4.1.

(a) Local Operations (LO)

According to this scheme, Alice and Bob conduct independent measurements in their bases: $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Note that these bases can be of different dimensions. Keep in mind that Bob is not required to know of Alice's measurement outcomes. They communicate the results of their measurement separately to Charlie, a third party who recognizes Alice and Bob's initial state. Thus they only communicate after the fact to compare their results.

(b) One-way Local Operations and Classical Communication (1-LOCC)

In this scheme, Bob modifies his measurement based on the classical information he receives from Alice, but the reverse is not permitted. Examples of one-way LOCC include important quantum information protocols, such as quantum teleportation.

(c) Full (Two-way) Local Operations and Classical Communication (2-LOCC)

With this approach, Alice and Bob are free to communicate classically whenever they choose, and they can iteratively adjust their measurement as they go. It is also noted that this scheme includes the one-way LOCC scheme [55].

Remark 4.2.1. *This scheme is called full LOCC, but it is often referred to as "Two-way" LOCC or in some literature, authors drop the prefix and just say "LOCC". For the purposes of this thesis, when referring to this scheme, we will denote it as "2-LOCC".*

4.3 Characterizing One-Way LOCC Measurements

We are highly interested in understanding which sets of bipartite states can and cannot be distinguished using LOCC. The class of LOCC measurements, however, is notably difficult to mathematically characterize, thus we address the issue using the conventional nested set of measurement classes:

$$\text{LO} \subset \text{1-LOCC} \subset \text{2-LOCC}. \tag{4.1}$$

The subsets of LOCC are local product measures (LO) and one-way LOCC. The supersets of LOCC are not operationally described, but rather in terms of mathematical formalism and they include separable (SEP) measurements followed by positive partial transpose (PPT) measurements, i.e., LOCC $\subset$ SEP $\subset$ PPT [48, 51]. Mathematically, a LOCC measurement

is typically of the form:

$$\mathbb{M} = \{A_k \otimes B_{k,j}\}, \tag{4.2}$$

with the positive operators making up the measurement outcomes satisfying $\sum_k A_k = \mathcal{I}_A$ and $\sum_j B_{k,j} = \mathcal{I}_B$ for each k [43, 51]. A set of states, $|\psi_{k,j}\rangle$, can be perfectly distinguished by one-way LOCC if there exists a measurement, $\mathbb{M} = \{A_k \otimes B_{k,j}\}$, such that for any (k', j'), and all $(k, j) \neq (k', j')$, we have

$$\langle\psi_{k',j'}|A_k \otimes B_{k,j}|\psi_{k',j'}\rangle = 0. \tag{4.3}$$

Remark 4.3.1. *This statement is equivalent to the operator annihilating the state because of the operator $A_k \otimes B_{k,j}$ being positive, i.e.,*

$$(A_k \otimes B_{k,j})|\psi_{k',j'}\rangle = 0. \tag{4.4}$$

where here the right-hand side is the zero matrix.

If $|a \otimes b\rangle$ is an eigenvector of $A_k \otimes B_{k,j}$ with non-zero eigenvalue, then this implies that $|\langle\psi_{k',j'}|a \otimes b\rangle|^2 = 0$ from the spectral decomposition of $A_k \otimes B_{k,j}$. Hence, without loss of generality (WLOG), we can assume each $A_k = m_k|\overline{a_k}\rangle\langle\overline{a_k}|$ is a rank one matrix with trace equal to m_k. Note, $|\overline{a_k}\rangle$ is the entry-wise complex conjugate of $|a_k\rangle$ in the computational basis.

Using the representation $|\psi\rangle = (\mathcal{I} \otimes U_i)|\Phi\rangle$, the non-normalized state of Bob's system after Alice's measurement is then given by $U_i|a_k\rangle$. These can then be distinguished if and only if the states $\{U_i|a_k\rangle\}_{i=0,1,\ldots,d-1}$ form an orthonormal set [51].

We can take a look at an example of how quantum measurements are used to communicate information from one part of a system to another.

Example 4.3.2 (Quantum Teleportation)**.** *[48] In the protocol of quantum teleportation, Alice and Bob share the entangled state:* $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$*. Alice has her unknown state* $|\phi\rangle$*, which she wants to send to Bob. Alice performs her measurement and conveys the result of the measurement to Bob. Using the information that Alice provides, Bob performs the proper operation to obtain the exact unknown state* $|\phi\rangle$*, which is exactly what Alice wanted. Suppose that the qubit with Bob is in the state* $|b\rangle$*, then*

- *If Alice measures the state* $|00\rangle$*, then Bob applies the* $\mathcal{I}$ *operator, and* $|\phi\rangle = \mathcal{I}|b\rangle = |b\rangle$*.*
- *If Alice measures the state* $|01\rangle$*, then Bob applies the* X *operator, and* $|\phi\rangle = X|b\rangle$*.*
- *If Alice measures the state* $|10\rangle$*, then Bob applies the* Z *operator, and* $|\phi\rangle = Z|b\rangle$*.*
- *If Alice measures the state* $|11\rangle$*, then Bob applies the* XZ *operator, and* $|\phi\rangle = XZ|b\rangle$*.*

For more details on quantum measurement processes and their use in quantum communication, see [52].

4.4 Conditions for Distinguishability by One-way LOCC

With the information from this and the last chapter, we can now introduce some results wherein we observe some conditions on matrices and sets of states that make them distinguishable by LOCC, in particular, 1-LOCC.

We can first show this by looking at an arbitrary set of states.

Proposition 4.4.1. *[51] Given a set of states* $S = \{|\psi_i\rangle = (\mathcal{I} \otimes U_i)|\Phi\rangle\} \subset \mathbb{C}^d \otimes \mathbb{C}^d$ *with* $|\Phi\rangle$ *being the standard maximally entangled state, the elements of* S *can be perfectly distinguished with one-way LOCC if and only if there exists a set of states* $\{|\phi_k\rangle\} \subset \mathbb{C}^d$ *and a set of positive numbers* $\{m_k\}$ *such that*

$$\sum_{k=1}^{d} m_k |\phi_k\rangle\langle\phi_k| = \mathcal{I}_d, \tag{4.5}$$

and

$$\langle \phi_k | U_j^* U_i | \phi_k \rangle = 0. \tag{4.6}$$

for all $i \neq j$.

In the case of maximally entangled states, the U_i are unitary matrices. This means that Alice's initial measurement provides no information about the identity of the prepared state. See Corollary 3 in Bandyopadhyay et al. [5] wherein they provide the necessary condition for one-way LOCC discrimination that there must exist at least one vector $|\phi_k\rangle$ that satisfies the inner product in equation 4.6.

A similar and stronger result can be stated below for one-way LOCC distinguishability of pairwise orthogonal maximally entangled states that arise from Weyl-commuting matrices. Before stating the lemma, it is beneficial to define a key term here: the Weyl basis.

Definition 4.4.2. *[94] The* ***Weyl basis****,* $\mathfrak{W}$ *is an orthonormal basis of unitary matrices in which* $U_i U_j$ *is proportional to* $U_j U_i$*, for all* $U_i, U_j \in \mathfrak{W}$.

Lemma 4.4.3. *[94] Given a set of maximally entangled states* $|\psi_i\rangle = (\mathcal{I} \otimes U_i)|\Phi\rangle$*, with* $\{U_i\}$ *a subset of the Weyl basis, then the states* $|\psi_i\rangle$ *can be perfectly distinguished with one-way LOCC if and only if there exists a state* $|\alpha\rangle$*, such that*

$$\langle \alpha | U_i^* U_j | \alpha \rangle = 0,$$

for all $i \neq j$.

An important result to touch on here is one from M. Nathanson [50]. We introduce the concept of common unbiased bases, which is connected to MUBs.

Definition 4.4.4. *Let* $\mathcal{A} = \{\mathcal{A}_i : i \in I\}$ *be a family of orthonormal bases of* $\mathbb{C}^d$*, with* $\mathcal{A}_i = \{|a_{i1}\rangle, |a_{i2}\rangle, \ldots, |a_{id}\rangle\}$ *and* I *be some index set.*

A basis $\mathcal{B} \in \mathbb{C}^d$ is called a ***common unbiased basis*** *for $\mathcal{A}$ if, for all $|b\rangle \in \mathcal{B}$ and for all $i \in I$, $1 \leq j \leq d$:*

$$|\langle b|a_{ij}\rangle|^2 = \frac{1}{d}.$$

So, a set of bases $\mathcal{A}$ is mutually unbiased if and only if for all $i \in I, \mathcal{A}_i$ is a common unbiased basis for $\mathcal{A} - \{\mathcal{A}_i\}$.

This helps describe the following result:

Proposition 4.4.5. *[50] Let $|\Psi_1\rangle, |\Psi_2\rangle, \ldots, |\Psi_k\rangle$ be orthogonal, maximally entangled vectors in $\mathbb{C}^d \otimes \mathbb{C}^d$ with $|\Psi_i\rangle = (\mathcal{I} \otimes B_i)|\Phi\rangle$.*

For each pair (i, j) let $\mathcal{A}_{ij}$ be a basis of eigenvectors of $B_i^* B_j$, and let

$$\mathcal{A} = \{\mathcal{A}_{ij} : 1 \leq i < j \leq k\}.$$

If the family $\mathcal{A}$ has a common unbiased basis, then the k states can be perfectly distinguished by LOCC.

Proof. Let $\mathcal{B} = \{|b_1\rangle, |b_2\rangle, \ldots, |b_d\}$ be the common unbiased basis. We need to show that for any $i \neq j$, and any k, the vectors $B_i|b_k\rangle$ and $B_j|b_k\rangle$ are orthogonal. Using the eigenbasis $\mathcal{A}_{ij}$, write

$$B_i^* B_j = \sum_{s=1}^{d-1} \lambda_s |e_s\rangle\langle e_s|. \tag{4.7}$$

Then for all k,

$$\begin{aligned} \langle b_k|B_i^* B_j|b_k\rangle &= \sum_{s=0}^{d-1} \lambda_s |\langle b_k|e_s\rangle|^2 \\ &= \frac{1}{d} \sum_{s=0}^{d-1} \lambda_s \\ &= \frac{1}{d} \mathrm{Tr}(B_i^* B_j) \\ &= 0. \end{aligned} \tag{4.8}$$

□

This result is actually more general, as we do not require that the states be maximally entangled, only that the matrices $B_i^* B_j$ be diagonalizable.

This proposition then leads to a key result from H. Fan [20], that involves the generalized Pauli matrices from Chapter 3 and the generalized Bell basis:

$$\mathcal{BB}_d = \{(\mathcal{I} \otimes X^m Z^l)|\Phi\rangle : 0 \leq m, l \leq d-1\} \in \mathbb{C}^d \otimes \mathbb{C}^d. \tag{4.9}$$

Corollary 4.4.6. *[20] Let d be a prime number. Then if k is any natural number satisfying $k(k-1)/2 \leq d$, any k vectors in $\mathcal{BB}_d$ can be perfectly distinguished by LOCC.*

Proof. This follows from the fact that for d prime, the eigenbases of $\{X^m Z^l : 0 \leq m, l \leq d-1\}$ form a maximum set of $(d+1)$ mutually unbiased bases in $\mathbb{C}^d$ (see Theorem 1.1 from [58]). Then up to a global phase,

$$(X^{m_i} Z^{l_i})^* (X^{m_j} Z^{l_j}) \equiv X^{m_j - m_i} Z^{l_j - l_i},$$

so the eigenbases of the pairwise products also belong to the set of MUBs. As long as the number of pairs (i, j) is less than the number of MUBs, then there exists a *common unbiased basis* and the proposition can be applied, further details of this proof can be found in the paper from H. Fan [20]. □

4.4.1 Orthogonal States

Another key topic with distinguishability is quantum orthogonal states. The distinguishability of orthogonal states is a crucial concept in quantum mechanics and quantum information theory, enabling the development of quantum technologies and applications that

take advantage of the unique properties of quantum systems. Before we state the theorem and proof, it is beneficial to introduce some key results which will help the proof.

We start by taking a look at the maximally entangled state. Recall the maximally entangled state from Eq. 3.19 was written according to:

$$|\psi\rangle = (\mathcal{I} \otimes U)|\Phi\rangle,$$

where $|\Phi\rangle$ is the Bell state also known as the standard maximally entangled state and is of the form:

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle \otimes |k\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d.$$

Let us now consider an example where the matrix U, in the maximally entangled state above, is one of the generalized Pauli matrices. We can rewrite the Bell state above, but now in terms of the eigenvectors of this generalized Pauli matrix according to the following:

$$|\Gamma\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |v_k\rangle \otimes |v_k\rangle, \tag{4.10}$$

where the $|v_k\rangle$'s form an arbitrary orthonormal basis. Note that we change this state to be called $|\Gamma\rangle$. This is a small piece of notation to differentiate the state from the standard maximally entangled state. Let us define the $|v_k\rangle$ vectors as:

$$|v_k\rangle = \sum_{i=0}^{d-1} u_{k_i} |i\rangle. \tag{4.11}$$

If we take a look at this vector tensored with itself (as written in the Bell state), we can observe:

$$|v_k\rangle \otimes |v_k\rangle = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} u_{k_i} u_{k_j} |i\rangle \otimes |j\rangle,$$

and taking the sum of this over k,

$$\begin{aligned}
\sum_{k=0}^{d-1} |v_k\rangle \otimes |v_k\rangle &= \sum_{k=0}^{d-1}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1} u_{k_i}u_{k_j}|i\rangle \otimes |j\rangle \\
&= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\sum_{k=0}^{d-1} u_{k_i}u_{k_j}|i\rangle \otimes |j\rangle \\
&= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\left(\sum_{k=0}^{d-1} u_{k_i}u_{k_j}\right)|i\rangle \otimes |j\rangle \\
&= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1}(\delta_{ij})|i\rangle \otimes |j\rangle \\
&= \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle.
\end{aligned}$$

We note that it is assumed the eigenvectors of the matrix U are real. So this tells us that $|\Gamma\rangle = |\Phi\rangle$. From this, we can gather that the distinguishability using a maximally entangled state does not depend on the orthonormal basis.

The next result is one from M. Nathanson and gives conditions for the one-way distinguishability of eigenvectors of the generalized Pauli matrices.

Lemma 4.4.7. *[51] The maximally entangled state which uses the eigenvectors of an arbitrary generalized Pauli matrix is one-way LOCC distinguishable if and only if there exists a $d \times n$ partial isometry W, such that $WW^* = \mathcal{I}_d$ such that $W^*U_i^*U_jW$ has all zeros as its diagonal entries for all $i \neq j$.*

From this lemma, we gather that if $U_{i,j} \in M_d(\mathbb{C})$, then the total product, $W^*U_i^*U_jW$, would be of dimension $n \times n$ for $n \geq d$, meaning $W \in M_{dn}(\mathbb{C})$ and thus $W^* \in M_{nd}(\mathbb{C})$. Finally, there is the condition that $WW^* = \mathcal{I}_d$.

If we think of the rows of W as row vectors, and the columns of W^* as column vectors,

i.e.,

$$W = \begin{pmatrix} - & w_1 & - \\ - & w_2 & - \\ & \vdots & \\ - & w_d & - \end{pmatrix}_{d\times n}, W^* = \begin{pmatrix} | & | & & | \\ \overline{w_1} & \overline{w_2} & \dots & \overline{w_d} \\ | & | & & | \end{pmatrix}_{n\times d}.$$

Then we can take the product and observe:

$$\begin{aligned} WW^* &= \begin{pmatrix} - & w_1 & - \\ - & w_2 & - \\ & \vdots & \\ - & w_d & - \end{pmatrix} \begin{pmatrix} | & | & & | \\ \overline{w_1} & \overline{w_2} & \dots & \overline{w_d} \\ | & | & & | \end{pmatrix} \\ &= \begin{pmatrix} ||w_1||^2 & \langle w_1|w_2\rangle & \dots & \langle w_1|w_d\rangle \\ \langle w_2|w_1\rangle & ||w_2||^2 & \dots & \langle w_2|w_d\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle w_d|w_1\rangle & \langle w_d|w_2\rangle & \dots & ||w_d||^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \\ &= \mathcal{I}_d. \end{aligned}$$

The final result we will touch on is from P. Fillmore, which proves that every matrix is unitarily equivalent to a matrix with a constant diagonal.

Definition 4.4.8. *Two complex matrices, A and B, are said to be* ***unitarily equivalent*** *if there exists a unitary matrix U, such that $B = U^*AU$. Two matrices which are unitarily equivalent are also* ***similar****.*

Theorem 4.4.9. *[21] The complex square matrix A is unitarily equivalent to a matrix whose main diagonal has all zero entries except the first position who's entry is* $\mathrm{Tr}(A)$*, if and only if* $\mathrm{Tr}(A)$ *is in the numerical range of A (denoted as $\mathcal{W}(A)$).*

Proof. [21] Recall that the numerical range $\mathcal{W}(A)$ of a matrix A is given by

$$\mathcal{W}(A) = \{\langle Ax|x\rangle : ||x|| = 1\}. \tag{4.12}$$

If $x_1, x_2, \ldots, x_d$ is an orthonormal basis in which the matrix A has main diagonal $(\mathrm{Tr}(A), 0, \ldots, 0)$, then $\mathrm{Tr}(A) = \langle Ax_1|x_1\rangle \in \mathcal{W}(A)$. For the next part of the proof, we use the method of induction on the size, d of the matrix A. By the hypothesis, there is a unit vector, x such that $\langle Ax_1|x_1\rangle = \mathrm{Tr}(A)$. The matrix A in any orthonormal basis $x_1, x_2, \ldots, x_d$ with $x_1 = x$ has the form:

$$\begin{pmatrix} \mathrm{Tr}(A) & B \\ C & D \end{pmatrix},$$

where D is of size $(d-1) \times (d-1)$. It follows that D is a trace zero matrix. If $d = 2$, we have the case of $D = 0$ and the proof is complete. If $d > 2$, in order to apply the induction hypothesis, we need to confirm that $0 \in \mathcal{W}(D)$. This can be seen as follows. If $\lambda_1, \lambda_2, \ldots, \lambda_{d-1}$ are the eigenvalues of D (with multiplicities), then

$$\frac{1}{d-1}(\lambda_1 + \lambda_2 + \cdots + \lambda_{d-1}) = \frac{1}{d-1}\mathrm{Tr}(D) = 0.$$

Hence, we know that 0 is in the convex hull of the spectrum of D, but $\mathcal{W}(D)$ is convex and contains the eigenvalues of D, thus $0 \in \mathcal{W}(D)$. Therefore, there is a unitary matrix U such that U^*DU has a main diagonal consisting of zeros. To complete the proof we observe that the matrix

$$V = \begin{pmatrix} 1 & 0 \\ 0 & U \end{pmatrix},$$

is unitary, and that

$$V^* \begin{pmatrix} \mathrm{Tr}(A) & B \\ C & D \end{pmatrix} V,$$

has main diagonal $(\mathrm{Tr}(A), 0, 0, \ldots, 0)$. □

This theorem leads us to the following further results.

Corollary 4.4.10. *[21] A matrix with a trace of zero is unitarily equivalent to a matrix with a main diagonal consisting of all zeros.*

Since for all $d \times d$ matrices A, the matrix $A - \left(\frac{\mathrm{Tr}(A)}{d}\right) \mathcal{I}_d$ has zero trace, and therefore we get the following result:

Corollary 4.4.11. *[21] Any matrix is unitarily equivalent to a matrix with a constant main diagonal.*

With these results, we can state and prove the following theorem:

Theorem 4.4.12. *[82] Any two orthogonal pure states are distinguishable with one-way LOCC.*

Proof. To distinguish the two orthogonal states, we can use M. Nathanson's result, but to do this, we require the partial isometry matrix, W. This is the change of basis matrix that takes the products $U_1^* U_2$ and $U_2^* U_1$ and transforms them into matrices of constant diagonal. This gives us the case of $i \neq j$. Considering the case of $i = j$, we apply Fillmore's result and use the definition of a unitary matrix to show that $U_1^* U_1$ and $U_2^* U_2$ are just equal to the identity, which is already a matrix of constant diagonal. With this now, we apply M. Nathanson's result and thus it is proven that these states can be distinguished by 1-LOCC. □

We showed the result for two states, but we can also consider more than two states. For this, we note another Theorem from M. Nathanson [51], wherein he gives an example

using three pure orthogonal states. He finds a set of three states that actually cannot be distinguished by 1-LOCC, indicating that in the above theorem, we cannot just simply replace the two states by three or more states.

Chapter 5

Conclusions and Future Directions

In this thesis, we have explored the concept of mutually unbiased bases and local operations and classical communication and its importance in quantum information theory. LOCC is a powerful tool that allows us to manipulate entangled quantum systems through local operations and classical communication and has important applications in quantum computing, quantum communication, and other areas of physics.

One of the key insights we have gained is the role of the generalized Pauli matrices as a basis for the space of traceless operators on a system of qubits. The generalized Pauli matrices allow us to study entanglement and its manipulation through LOCC, and to construct quantum gates using LOCC. Furthermore, we have shown how the Weyl-commuting matrices and mutually unbiased bases are related to the generalized Pauli matrices and can be used to study the properties of entanglement and the limits of what can be achieved through LOCC.

The connection between LOCC and the generalized Pauli matrices, Weyl-commuting matrices, and mutually unbiased bases provides a powerful framework for studying and manipulating quantum systems and has many important applications in quantum information theory. Moreover, this work highlights the importance of understanding the basic principles

of quantum mechanics and the role of LOCC as a fundamental tool for studying quantum entanglement and other phenomena.

This thesis has provided a comprehensive overview of LOCC and its applications in quantum information theory and has connected LOCC to the generalized Pauli matrices, Weyl-commuting matrices, and mutually unbiased bases. By gaining a deeper understanding of these concepts, we can continue to develop new technologies and applications that harness the power of quantum mechanics. Our results have important implications for the design of quantum communication and computing protocols, and they open up new avenues for future research in this exciting area of quantum information theory.

5.1 Future Applications

Much of the research on LOCC and the concepts of mutually unbiased bases, Weyl-commuting matrices, and generalized Pauli matrices has been focused on qubits. Future research could explore the use of these concepts in higher-dimensional systems, like qudits, and investigate the properties and manipulation of entanglement in these systems.

The concepts of mutually unbiased bases, Weyl-commuting matrices, and generalized Pauli matrices have already been used to develop quantum algorithms, such as quantum phase estimation and quantum Fourier transform. Future research could investigate the use of these concepts in developing new quantum algorithms, with a focus on those that can be implemented through LOCC.

While much of the research on these topics has been theoretical, experimental validation of these concepts is necessary to fully understand their properties and limitations. Future research could focus on experimental implementations of these concepts, with a focus on demonstrating their effectiveness in manipulating entangled quantum systems.

5.1.1 Quantum Privacy

In traditional classical communication, privacy can be protected using encryption techniques, but due to the laws of quantum mechanics, information security in the quantum world presents special difficulties. In order to overcome these difficulties and guarantee the confidentiality of quantum communication, the idea of quantum privacy channels was developed. The primary problem with quantum communication is the vulnerability of quantum states to interception or eavesdropping. The process of eavesdropping on quantum communication is known as quantum interception or quantum wiretapping. The confidentiality of the communication can potentially be jeopardized if an eavesdropper is able to access the transmitted quantum states and extract information without being noticed. To identify and thwart eavesdropping attempts, quantum privacy channels use a variety of techniques. One method, in particular, is Quantum Key Distribution (QKD) [65, 68], which enables two parties to create a shared secret key across an unsecured quantum channel. If any interference or measurement disturbance is discovered, to find an eavesdropper, QKD techniques often apply the principles of quantum mechanics. The communicating parties can abort the key exchange process and ensure that their communication is secure. Another technique used in quantum privacy channels is error correction codes [39, 63]. These codes aid in the detection and correction of issues that may occur while transmitting quantum information. The privacy of the communication is maintained by using error correction codes, which enable the participants involved in the conversation to determine whether a third party has interfered with the communicated quantum states.

In the context of quantum privacy, mutually unbiased bases play a crucial role in privacy protocols such as quantum key distribution. QKD enables the establishment of a secure shared key between two parties, typically referred to as Alice and Bob, over an unreliable quantum channel. The security of QKD protocols relies on the principles of quantum me-

chanics and the impossibility of perfectly cloning an unknown quantum state. The notion of mutually unbiased bases comes into play when Alice and Bob wish to find an eavesdropper, commonly referred to as Eve. In this protocol, Alice sends a series of quantum states from one basis to Bob over the quantum channel and Bob measures these states using a different basis. If Eve tries to intercept the quantum states to gain information, her measurements will introduce disturbances and errors, which can be detected through the analysis of measurement outcomes in different bases. Thus MUBs can be used to identify the presence of an eavesdropper. Eve will inject biases into her subsequent measurements if she measures the quantum states in one basis first. When Alice and Bob compare the results of their measurements, these biases can then be identified statistically. Then if the measurement outcomes exhibit correlations that are inconsistent with the properties of mutually unbiased bases, it indicates the presence of a potential eavesdropper. By employing mutually unbiased bases in the measurement outcome analysis, Alice and Bob can enhance the security of their communication by exposing possible eavesdropping attempts. It provides a way to assess the security of the quantum privacy channel and to identify any potential breaches of privacy. The violation of the unbiasedness condition [23] provides a basis for error estimation, error correction, and privacy amplification protocols in quantum communication systems.

The idea of mutually unbiased bases provides numerous applications in quantum privacy channels and thus the work on MUBs in this thesis can help provide a good starting point in further research into this area of quantum information.

Bibliography

[1] Alexanderian, A. (2013). A brief note on tensor product of Hilbert spaces. *The University of Texas, Mathematics Journal*.

[2] Appleby, D. M. (2005). Symmetric informationally complete–positive operator valued measures and the extended Clifford group. *Journal of Mathematical Physics*, *46*(5), 052107.

[3] Axler, S. (2015). *Linear algebra done right*. Springer.

[4] Bandyopadhyay, S., Boykin, P. O., Roychowdhury, V., & Vatan, F. (2002). A new proof for the existence of mutually unbiased bases. *Algorithmica*, *34*(4), 512–528.

[5] Bandyopadhyay, S., Ghosh, S., & Kar, G. (2011). LOCC distinguishability of unilaterally transformable quantum states. *New Journal of Physics*, *13*(12), 123013.

[6] Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, *1*(3), 195.

[7] Bengtsson, I. (2007). Three ways to look at mutually unbiased bases. *AIP Conference Proceedings*, *889*(1), 40–51.

[8] Bengtsson, I., & Życzkowski, K. (2017). *Geometry of quantum states: An introduction to quantum entanglement*. Cambridge University Press.

[9] Bennett, C., Harrow, A., Leung, D., & Smolin, J. (2003). On the capacities of bipartite Hamiltonians and unitary gates. *IEEE Transactions on Information Theory*, *49*(8), 1895–1911.

[10] Bennett, C. H., DiVincenzo, D. P., Fuchs, C. A., Mor, T., Rains, E., Shor, P. W., Smolin, J. A., & Wootters, W. K. (1999). Quantum nonlocality without entanglement. *Physical Review A*, *59*(2), 1070.

[11] Butterley, P., & Hall, W. (2007). Numerical evidence for the maximum number of mutually unbiased bases in dimension six. *Physics Letters A*, *369*(1-2), 5–8.

[12] Chatwin-Davies, A. (2020). Introductory notes on quantum information and computation.

[13] Cho, M., Lee, J. I., & Yamazaki, T. (2009). On the operator equation $AB = zBA$. *Scientiae Mathematicae Japonicae*, *69*(2), 257–263.

[14] Combescure, M., & IPNL, B. P. D. (2007). The mutually unbiased bases revisited. *Contemporary Mathematics*, *447*, 29.

[15] Dankert, C., Cleve, R., Emerson, J., & Livine, E. (2009). Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, *80*(1), 012304.

[16] Davis, C. (1962). The norm of the schur product operation. *Numerische Mathematik*, *4*(1), 343–344.

[17] Davis, P. J. (1975). *Interpolation and approximation*. Courier Corporation.

[18] DiVincenzo, D. P., Shor, P. W., & Smolin, J. A. (1998). Quantum-channel capacity of very noisy channels. *Physical Review A*, *57*(2), 830.

[19] Duan, R., Severini, S., & Winter, A. (2013). Zero-error communication via quantum channels, noncommutative graphs, and a quantum Lovasz number. *IEEE Transactions on Information Theory*, *59*(2), 1164–1174.

[20] Fan, H. (2004). Distinguishability and indistinguishability by local operations and classical communication. *Physical Review Letters*, *92*(17), 177905.

[21] Fillmore, P. A. (1969). On similarity and the diagonal of a matrix. *The American Mathematical Monthly*, *76*(2), 167–169.

[22] Garling, D. J. (2011). *Clifford algebras: An introduction* (Vol. 78). Cambridge University Press.

[23] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics*, *74*(1), 145.

[24] Gottesman, D., & Lo, H.-K. (2003). Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, *49*(2), 457–475.

[25] Gross, D., & Eisert, J. (2007). Novel schemes for measurement-based quantum computation. *Physical Review Letters*, *98*(22), 220503.

[26] Haase, M. (2006). The functional calculus for sectorial operators. In *The functional calculus for sectorial operators* (pp. 19–60). Springer.

[27] Hardy, L. (1998). Spooky action at a distance in quantum mechanics. *Contemporary physics*, *39*(6), 419–429.

[28] Hashimoto, T., Horibe, M., & Hayashi, A. (2021). Simple criterion for local distinguishability of generalized Bell states in prime dimension. *Physical Review A*, *103*(5), 052429.

[29] Hayashi, M. (2008). Discrete realization of group symmetric LOCC-detection of maximally entangled state. *arXiv preprint arXiv:0810.3381*.

[30] Horn, R. A. (1990). The hadamard product. *Proceedings of Symposia in Applied Mathematics*, *40*, 87–169.

[31] Horn, R. A., & Johnson, C. R. (2012). *Matrix analysis*. Cambridge University Press.

[32] Howard, M., & Vala, J. (2012). Qudit versions of the qubit $\pi/8$ gate. *Physical Review A*, *86*(2), 022316.

[33] Ivonovic, I. (1981). Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, *14*(12), 3241.

[34] Jagannathan, R. (2010). On generalized Clifford algebras and their physical applications. In *The legacy of Alladi Ramakrishnan in the mathematical sciences* (pp. 465–489). Springer.

[35] Kent, A., Linden, N., & Massar, S. (1999). Optimal entanglement enhancement for mixed states. *Physical Review Letters*, *83*(13), 2656.

[36] Kibler, M. R. (2009). An angular momentum approach to quadratic fourier transform, hadamard matrices, gauss sums, mutually unbiased bases, the unitary group and the pauli group. *Journal of Physics A: Mathematical and Theoretical*, *42*(35), 353001.

[37] Kibler, M. R. (2010). Bases for spin systems and qudits from angular momentum theory. *Communications in Nonlinear Science and Numerical Simulation*, *15*(3), 752–763.

[38] Klinger, A. (1967). The Vandermonde matrix. *The American Mathematical Monthly*, *74*(5), 571–574.

[39] Knill, E., & Laflamme, R. (1997). Theory of quantum error-correcting codes. *Physical Review A*, *55*(2), 900.

[40] Kraus, K. (1987). Complementary observables and uncertainty relations. *Physical Review D*, *35*(10), 3070.

[41] Kreyszig, E. (1978). Introductory functional analysis with applications. jonh wiley & sons. *Inc., New York*.

[42] Kribs, D. W. (2005). A quantum computing primer for operator theorists. *Linear Algebra and its Applications*, *400*, 147–167.

[43] Kribs, D. W., Mintah, C., Nathanson, M., & Pereira, R. (2017). Operator structures and quantum one-way LOCC conditions. *Journal of Mathematical Physics*, *58*(9), 092201.

[44] Kribs, D. W., Mintah, C., Nathanson, M., & Pereira, R. (2021). Operator and graph theoretic techniques for distinguishing quantum states via one-way LOCC. *Applied Sciences*, *11*(20), 9542.

[45] Lankham, I., Nachtergaele, B., & Schilling, A. (2007). The spectral theorem for normal linear maps. *University of California, Davis*.

[46] Li, M.-S., Shi, F., & Wang, Y.-L. (2022). Local discrimination of generalized Bell states via commutativity. *Physical Review A*, *105*(3), 032455.

[47] May, D. P. (2010). *Mutually unbiased bases: The standard construction and automorphisms*. University of Wyoming.

[48] Mintah, C. (2016). *Operator theory and conditions for quantum local operations and classical communication* (Doctoral dissertation). University of Guelph.

[49] Myrvold, W. C., Christian, J., & Gisin, N. (2009). Bell inequalities: Many questions, a few answers. *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony*, 125–138.

[50] Nathanson, M. (2005). Distinguishing bipartite orthogonal states using LOCC: Best and worst cases. *Journal of Mathematical Physics*, *46*(6), 062103.

[51] Nathanson, M. (2013). Three maximally entangled states can require two-way local operations and classical communication for local discrimination. *Physical Review A*, *88*(6), 062316.

[52] Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information, 10th anniversary Cambridge University Press.

[53] Nielsen, M. A., & Chuang, I. L. (2001). Quantum computation and quantum information. *Physics Today*, *54*(2), 60.

[54] Ojo, O. R. (2021). *Universality of Weyl unitaries*. The University of Regina (Canada).

[55] Owari, M., & Hayashi, M. (2008). Two-way classical communication remarkably improves local distinguishability. *New Journal of Physics*, *10*(1), 013006.

[56] Petz, D. (1990). *Algebra of the canonical commutation relation*. Leuven University Press Leuven.

[57] Petz, D. (2007). *Quantum information theory and quantum statistics*. Springer Science & Business Media.

[58] Pittenger, A. O., & Rubin, M. H. (2004). Mutually unbiased bases, generalized spin matrices and separability. *Linear Algebra and its Applications*, *390*, 255–278.

[59] Planat, M., Rosu, H. C., & Perrine, S. (2006). A survey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements. *Foundations of Physics*, *36*(11), 1662–1680.

[60] Putnam, C. R. (2012). *Commutation properties of Hilbert space operators and related topics* (Vol. 36). Springer Science & Business Media.

[61] Ramakrishnan, A. (1971). Generalized Clifford algebra and its applications or a new approach to internal quantum numbers. *Proc. Conf. on Clifford Algebra, Its Generalizations, and Applications*, 87–95.

[62] Rieffel, M. A. (1972). On the uniqueness of the Heisenberg commutation relations. *Duke Mathematical Journal*, *39*(4), 745–752.

[63] Roffe, J. (2019). Quantum error correction: An introductory guide. *Contemporary Physics*, *60*(3), 226–245.

[64] Santhanam, T., & Tekumalla, A. (1976). Quantum mechanics in finite dimensions. *Foundations of Physics*, *6*(5), 583–587.

[65] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of modern physics*, *81*(3), 1301.

[66] Schwinger, J. (1960). Unitary operator bases. *Proceedings of the National Academy of Sciences*, *46*(4), 570–579.

[67] Schwinger, J. (2003). Quantum mechanics: Symbolism of atomic measurements.

[68] Sharma, P., Agrawal, A., Bhatia, V., Prakash, S., & Mishra, A. K. (2021). Quantum key distribution secured optical networks: A survey. *IEEE Open Journal of the Communications Society*, *2*, 2049–2083.

[69] Singh, A., & Carroll, S. M. (2018). Modeling position and momentum in finite-dimensional Hilbert spaces via generalized Pauli operators. *arXiv preprint arXiv:1806.10134*.

[70] Sreeram, V., & Agathoklis, P. (1994). On the properties of gram matrix. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *41*(3), 234–237.

[71] Šulc, P., & Tolar, J. (2007). Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions. *Journal of Physics A: Mathematical and Theoretical*, *40*(50), 15099.

[72] Sylvester, J. J. (1867). Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, *34*(232), 461–475.

[73] Sylvester, J. J. (1909). *The collected mathematical papers of James Joseph Sylvester* (Vol. 3). University Press.

[74] Verstraete, F., Dehaene, J., & De Moor, B. (2003). Normal forms and entanglement measures for multipartite quantum states. *Physical Review A*, *68*(1), 012103.

[75] Verstraete, F., Dehaene, J., & DeMoor, B. (2001). Local filtering operations on two qubits. *Physical Review A*, *64*(1), 010101.

[76] Verstraete, F., & Wolf, M. M. (2002). Entanglement versus Bell violations and their behavior under local filtering operations. *Physical Review Letters*, *89*(17), 170401.

[77] Villars, C. (1986). The paradox of Schrödinger's cat. *Physics Education*, *21*(4), 232.

[78] Virmani, S., Sacchi, M. F., Plenio, M. B., & Markham, D. (2001). Optimal local discrimination of two multipartite pure states. *Physics Letters A*, *288*(2), 62–68.

[79] Vitória, P. (2008). Mutually unbiased bases: A brief survey.

[80] von Neumann, J. (1931). Die eindeutigkeit der schrödingerschen operatoren. *Mathematische Annalen*, *104*(1), 570–578.

[81] Vourdas, A. (2004). Quantum systems with finite Hilbert space. *Reports on Progress in Physics*, *67*(3), 267.

[82] Walgate, J., Short, A. J., Hardy, L., & Vedral, V. (2000). Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, *85*(23), 4972.

[83] Wang, C., Yuan, J., Yang, Y., & Mu, G. (2021). Local unitary classification of generalized Bell state sets in $\mathbb{C}^5 \otimes \mathbb{C}^5$. *Journal of Mathematical Physics*, *62*(3), 032203.

[84] Wang, Y.-L., Li, M.-S., Zheng, Z.-J., & Fei, S.-M. (2016). On small set of one-way LOCC indistinguishability of maximally entangled states. *Quantum Information Processing*, *15*, 1661–1668.

[85] Wang, Y., Hu, Z., Sanders, B. C., & Kais, S. (2020). Qudits and high-dimensional quantum computing. *Frontiers in Physics*, *8*, 589504.

[86] Wang, Z.-W., Zhou, X.-F., Huang, Y.-F., Zhang, Y.-S., Ren, X.-F., & Guo, G.-C. (2006). Experimental entanglement distillation of two-qubit mixed states under local operations. *Physical Review Letters*, *96*(22), 220505.

[87] Weyl, H. (1927). Quantenmechanik und gruppentheorie. *Zeitschrift für Physik*, *46*(1), 1–46.

[88] Weyl, H. (1950). *The theory of groups and quantum mechanics*. Courier Corporation.

[89] Wigren, T. (2015). The Cauchy-Schwarz inequality: Proofs and applications in various spaces. *Mathematics*.

[90] Wootters, W. K. (1986). Quantum mechanics without probability amplitudes. *Foundations of Physics*, *16*(4), 391–405.

[91] Wootters, W. K., & Fields, B. D. (1989). Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, *191*(2), 363–381.

[92] Wu, H.-H., & Wu, S. (2009). Various proofs of the Cauchy-Schwarz inequality. *Octogon Mathematical Magazine*, *17*(1), 221–229.

[93] Yang, Y.-H., Wang, C.-H., Yuan, J.-T., Wu, X., & Zuo, H.-J. (2018). Local distinguishability of generalized Bell states. *Quantum Information Processing*, *17*, 1–12.

[94] Yang, Y.-H., Yan, R.-Y., Wang, X.-L., Yuan, J.-T., & Zuo, H.-J. (2021). Novel method for one-way local distinguishability of generalized bell states in arbitrary dimension. *Journal of Physics A: Mathematical and Theoretical*, *55*(1), 015301.

[95] Young, N. (1988). *An introduction to Hilbert space*. Cambridge University Press.

[96] Yuan, J.-T., Wang, C.-H., Yang, Y.-H., & Geng, S.-J. (2019). Constructions of one-way LOCC indistinguishable sets of generalized Bell states. *Quantum Information Processing*, *18*, 1–15.

[97] Yuan, J.-T., Yang, Y.-H., & Wang, C.-H. (2020). Constructions of locally distinguishable sets of maximally entangled states which require two-way LOCC. *Journal of Physics A: Mathematical and Theoretical*, *53*(50), 505304.

[98] Yuan, J.-T., Yang, Y.-H., & Wang, C.-H. (2022). Finding out all locally indistinguishable sets of generalized Bell states. *Quantum*, *6*, 763.

[99] Zhang, Z.-C., Wen, Q.-Y., Gao, F., Tian, G.-J., & Cao, T.-Q. (2014). One-way LOCC indistinguishability of maximally entangled states. *Quantum Information Processing*, *13*, 795–804.