QUANTUM MAGIC SQUARES IN VIEW OF BIRKHOFF-VON NEUMANN THEOREM

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

SUNAY DOĞAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
MATHEMATICS

AUGUST 2024

Approval of the thesis:

QUANTUM MAGIC SQUARES IN VIEW OF BIRKHOFF-VON NEUMANN THEOREM

submitted by **SUNAY DOĞAN** in partial fulfillment of the requirements for the degree of **Master of Science in Mathematics Department, Middle East Technical University** by,

Prof. Dr. Naci Emre Altun
Dean, Graduate School of **Natural and Applied Sciences** ____________

Prof. Dr. Hasan Taşeli
Head of Department, **Mathematics** ____________

Assoc. Prof. Dr. Semra Öztürk
Supervisor, **Mathematics, METU** ____________

Examining Committee Members:

Prof. Dr. Songül Kaya Merdan
Department of Mathematics, METU ____________

Assoc. Prof. Dr. Semra Öztürk
Department of Mathematics, METU ____________

Assist. Prof. Dr. Serdar Ay
Department of Mathematics, Atılım University ____________

Date: 23.08.2024

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: Sunay Doğan

Signature :

ABSTRACT

QUANTUM MAGIC SQUARES IN VIEW OF BIRKHOFF-VON NEUMANN THEOREM

Doğan, Sunay
M.S., Department of Mathematics
Supervisor: Assoc. Prof. Dr. Semra Öztürk

August 2024, 67 pages

Quantum magic squares are generalizations of doubly stochastic matrices to arbitrary, possibly non-commutative algebras, more specifically C^*-algebras. Birkhoff-von Neumann Theorem states that every doubly stochastic matrix is a convex combination of permutation matrices. One inevitable question is whether a quantum magic square is a convex combinations of quantum permutation matrices. It has been proven by Cuevas, Drescher, and Netzer that the generalization of the Birkhoff-von Neumann Theorem in the quantum setting is not true in general. A quantum magic square is a convex combination of Arveson extreme points but not necessarily a convex combination of quantum permutation matrices. Additionally, the relationships between different subsets of quantum magic squares, including their inclusion properties, have been studied in this context.

Keywords: quantum magic squares, quantum permutation matrices, semi-classical magic squares, Birkhoff-von Neumann Theorem, Arveson extreme points

ÖZ

BİRKHOFF-VON NEUMANN TEOREMİ BAĞLAMINDA KUANTUM SİHİRLİ KARELER

Doğan, Sunay
Yüksek Lisans, Matematik Bölümü
Tez Yöneticisi: Doç. Dr. Semra Öztürk

Ağustos 2024 , 67 sayfa

Kuantum sihirli kareler, çift stokastik matrislerin değişmeli olmayabilen herhangi bir cebire, özellikle bir C* cebirine genelleştirilmesidir. Birkhoff-von Neumann Teoremi her çift stokastik matrisin permütasyon matrislerinin dışbükey kombinasyonu şeklinde yazılabildiğini ifade eder. Bu durumda ortaya çıkan kaçınılmaz soru her kuantum sihirli karenin kuantum permütasyon matrislerinin dışbükey kombinasyonu şeklinde yazılıp yazılamayacağıdır. Birkhoff-von Neumann Teoremi'nin kuantum sihirli kareler için her zaman doğru olmadığı Cuevas, Drescher ve Netzer, tarafından kanıtlanmıştır. Bir kuantum sihirli kare her zaman Arveson ekstrem noktaların bir dışbükey kombinasyonu olmasına rağmen, kuantum permütasyon matrislerin bir dışbükey kombinasyonu olmak zorunda değildir. Ek olarak, kuantum sihirli karelerin farklı alt kümeleri, özellikle bunlar arasındaki altküme ilişkileri, incelenmiştir.

Anahtar Kelimeler: kuantum sihirli kareler, kuantum permütasyon matrisleri, yarıklasik sihirli kareler, Birkhoff-von Neumann Teoremi, Arveson ekstrem noktalar

To my family

ACKNOWLEDGMENTS

I owe deep gratitude to my advisor Assoc. Prof. Dr. Semra Öztürk whose insightful guidance has been invaluable throughout my undergraduate and graduate studies. Her expertise and support have been instrumental in the preparation of this thesis.

Heartfelt thanks are extended to Prof. Zafer Gedik for his invaluable assistance and expertise in reviewing the sections of my thesis related to quantum information.

I would also like to thank the Scientific and Technological Research Council of Turkey (TÜBİTAK) for their financial support of this thesis through the BİDEB National Graduate Scholarship Programme for M.Sc. (2210-A).

I am deeply grateful to my colleagues for fostering an environment that allowed me to dedicate the necessary time and effort to this work. Their encouragement and collaboration have been immensely appreciated.

Finally, my deepest thanks go to my mother Hatice Doğan, my father Süleyman Özgür Doğan and my brother Serkan Doğan for their unwavering encouragement and dedication. Their love and support have been my greatest source of strength.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF SYMBOLS

$\mathbb{N}$	The set of natural numbers, *i.e.*, $\{1, 2, 3, ...\}$
$[n]$	The set of natural numbers from 1 to n, *i.e.*, $\{1, 2, \ldots, n\}$
$\mathbb{R}$	The set of real numbers
$\mathbb{R}_{\geq 0}$	The set of non-negative real numbers
$\mathbb{C}$	The set of complex numbers
$\mathbb{T}$	The set of points on the unit circle in $\mathbb{C}$
$\mathcal{D}$	The set of points on the unit disc in $\mathbb{C}$
$\mathcal{H}$	Hilbert space
$\mathcal{B}(\mathcal{H})$	Bounded linear maps over a Hilbert space $\mathcal{H}$
$\text{Mat}_n(V)$	$n \times n$ matrices over a vector space V
$\text{Her}_n(V)$	$n \times n$ Hermitian matrices over a vector space V
$\text{Psd}_n(V)$	$n \times n$ positive semi-definite matrices over a vector space V
$mconv(S)$	Matrix convex hull of a set S
S_{her}	Hermitian elements of a set S in a **C***-algebra
S^+	Positive elements of a set S in a **C***-algebra
$\mathcal{A}^{-1}$	Invertible elements of a subalgebra $\mathcal{A}$ of a **C***-algebra
$\mathcal{M}_n^s$	Quantum magic squares with exterior size n and interior size s
$\mathcal{P}_n^s$	Quantum permutation matrices with exterior size n and interior size s
$\mathcal{CP}_n^s$	Commuting quantum permutation matrices with exterior size n and interior size s
$\mathcal{S}_n^s$	Semi-classical magic squares with exterior size n and interior size s

$\mathcal{R}_n^n$	Rank 1 quantum magic squares with size n
Lat_n^q	Quantum Latin squares with size n
Lat_n^e	Easy quantum Latin squares with size n
POVML_n	Quantum magic squares with size n generated by a classical Latin square and a POVM (positive operator valued measure)
PVML_n	Quantum magic squares with size n generated by a classical Latin square and a PVM (projective valued measure)
$\mathfrak{A}_S$	Arveson extreme points of a set S

CHAPTER 1

INTRODUCTION

Magic squares are square matrices with non-negative real entries such that each row, column, and both diagonals sum to a constant number which is called the magic constant. When the restriction on the diagonals is removed, they are called semi-magic squares. This thesis aims to study the main results of [1] and [2]. We will refer semi-magic squares as magic squares throughout the thesis as in [1] and [2].

Doubly stochastic (bistochastic) matrices are matrices with non-negative real entries whose rows and columns sum to 1. In this sense, they can be viewed as special types of semi-magic squares. Doubly stochastic matrices have applications in many areas of mathematics and science. For example, Hartfield and Spellman used doubly stochastic matrices to understand connectivity of graphs [3] while Louck demonstrated their use as transition probabilities in quantum mechanics [4].

In his 1946 paper [5], Garret Birkhoff proved that every doubly stochastic matrix is a convex combination of permutation matrices. A permutation matrix is a special type of doubly stochastic matrix whose entries consist of 0 and 1. In 1953, John von Neumann referred to Birkhoff's theorem in his paper on game theory and optimization [6] and provided a more direct proof. As a result, the theorem became known as Birkhoff-von Neumann Theorem. This theorem is utilized not only in game theory and optimization but also in various other fields, including statistics [7] and quantum computing [8].

The early 20th century marked a revolutionary period in physics, with the development of quantum mechanics offering a fascinating and counterintuitive view of the universe. A new and still not clearly defined term "quantum mathematics" emerged and it is used to describe any branch of mathematics related to quantum physics [9].

In quantum mechanics, measurable properties of a particle like its position, speed, spin etc., are called observables and they are represented by Hermitian operators on the space of square integrable functions on $\mathbb{R}^3$ ($L^2(\mathbb{R}^3)$) [10]. Werner Heisenberg's Uncertainty Principle asserts that commutators of certain observables are non-zero, making non-commutativity a fundamental aspect of quantum mathematics. Consequently, from the 1930s onward, the theories of $\mathbf{C}^*$-algebras and von Neumann algebras were developed for quantum (non-commutative) analysis [9].

As quantum mathematics evolved, many new mathematical concepts emerged, such as quantum groups, quantum symmetries, quantum permutations, and quantum magic squares. These quantum magic squares can be regarded as a quantum generalization of doubly stochastic matrices. One natural question is whether the Birkhoff-von Neumann Theorem (Theorem 2.1.2) is true in the quantum setting. It will be proven that a quantum magic square is a convex combination of Arveson extreme points but not necessarily a convex combination of quantum permutation matrices (Theorem 4.2.3). In addition, the relationships between different subsets of quantum magic squares, especially their inclusion properties will be studied in this context as summarized in Table 5.1. These will be the main focus of this thesis.

To provide a comprehensive understanding of quantum magic squares, this work is structured as follows. Chapter 2 lays the groundwork by offering essential preliminary definitions. Section 2.1 defines magic squares, Latin squares, and doubly stochastic matrices, and presents a proof of the Birkhoff-von Neumann Theorem 2.1.2. Since the entries of quantum magic squares are positive elements of $\mathbf{C}^*$-algebras, Section 2.2 delves into $\mathbf{C}^*$-algebras, spectral theory, and the properties of positive elements within these algebras. Section 2.3 introduces operator systems, which are a more flexible generalization of $\mathbf{C}^*$-algebras.

Chapter 3 introduces the set of quantum magic squares and its various subsets. Section 3.1 defines quantum magic squares, quantum permutation matrices, and semi-classical magic squares. In Section 3.2, quantum Latin squares are introduced, and it is demonstrated that each quantum Latin square can be converted into a quantum magic square. Additionally, it is shown that certain magic squares can be derived from classical Latin squares. Section 3.3 provides a definition of magic operator systems and introduces the smallest and largest magic operator systems. These definitions are essential for proving Theorem 3.3.1, which asserts the existence of magic squares that are not semi-classical. This result will be later utilized to disprove the Birkhoff-von Neumann Theorem 2.1.2 in the quantum setting.

Chapter 4, building on the work of Cuevas, Drescher, and Netzer [2], is dedicated to disproving the Birkhoff-von Neumann Theorem for quantum magic squares. Section 4.1 explores matrix convexity, demonstrating that while the set of quantum magic squares is matrix convex, that is closed under convex combinations with matrix coefficients, the set of quantum permutation matrices is not. The matrix convex hull of quantum permutation matrices is a subset of quantum magic squares. Section 4.2 establishes that this subset relation is proper, indicating the existence of quantum magic squares that lie outside the matrix convex hull of quantum permutation matrices.

In Chapter 5, some further discussions related to quantum magic squares were provided. Drawing on the principal theorems from the work of Cuevas, Netzer and Valentiner-Branth [1], Section 5.1 examines the relationships between various subsets of quantum magic squares. Quantum magic squares have applications in quantum information. In Section 5.2 relations between magic squares and quantum information will be discussed following the work of Blum, Nechita and Schmidt [11].

Chapter 6 will serve as the concluding chapter. A brief summary and some open problems related to quantum magic squares will be provided.

CHAPTER 2

PRELIMINARIES

2.1 Magic Squares and Birkhoff - von Neumann Theorem

A magic square M is an $n \times n$ matrix whose cells contain non-negative real numbers such that the sum of each of its rows, columns, main diagonal and anti-diagonal are equal to the same number which is called the *magic constant* of M [1]. If the constraints on the diagonals are left out it is called a *semi-magic square*. Consistent with our main references, namely [1] and [2], we will employ the term "magic squares" interchangeably with "semi-magic squares" throughout this thesis.

Definition 2.1.1. A *(semi) magic square* is an $n \times n$ square matrix $M = (m_{ij})_{i,j \in [n]}$ where $m_{ij} \in \mathbb{R}_{\geq 0}$ such that

$$\sum_{k=1}^{n} m_{ik} = \sum_{k=1}^{n} m_{kj} = c$$

where $c \in \mathbb{R}$ is constant. The number c is called the *magic constant* of M. When $c = 1$, M is called a *doubly stochastic matrix*.

Example 2.1.1. Let $M = \begin{bmatrix} 1 & 3 & 2 & 8 \\ 2 & 4 & 7 & 1 \\ 8 & 2 & 1 & 3 \\ 3 & 5 & 4 & 2 \end{bmatrix}$. The matrix M has non-negative entries and each of its rows and columns sum to 14. Therefore, M is a (semi) magic square whose magic constant is 14.

Definition 2.1.2. A *Latin square of order n* is an $n \times n$ square matrix which is filled with numbers from 1 to n such that each number appears exactly once in each row and each column.

Example 2.1.2. Let $L = \begin{bmatrix} 1 & 3 & 2 & 4 \\ 4 & 1 & 3 & 2 \\ 2 & 4 & 1 & 3 \\ 3 & 2 & 4 & 1 \end{bmatrix}$. The matrix L contains numbers $\{1, 2, 3, 4\}$ exactly once in each column and each row. Therefore L is a Latin square.

Proposition 2.1.1. Every matrix which is a Latin square is also a (semi) magic square.

Proof. Any row or column of a Latin square L whose order is n contain numbers $\{1, ..., n\}$ exactly once. Therefore, sum of any row or column is $c = \sum_{i=1}^{n} i$. Hence, L is a magic square with magic constant c. □

Remark 2.1.1. Every non-zero magic square can be converted into a doubly stochastic matrix by simply dividing each of its entries by the magic constant.

Definition 2.1.3. Let V be a vector space over $\mathbb{C}$. A convex combination of a set of distinct points $\{v_1, ..., v_n\} \subseteq V$ is a linear combination $\sum\limits_{i\in[n]} c_i v_i$ where each coefficient $c_i \in \mathbb{R}_{\geq 0}$ is a non-negative real scalar and $\sum\limits_{i\in[n]} c_i = 1$. A subset of V is called a *convex set* if it is closed under convex combinations.

In Chapter 4, a generalization of convexity notion will be defined for matrices, Definition 4.1.1, which plays a crucial role in disproving Birkhoff-von Neumann Theorem 2.1.2 in the quantum setting.

Definition 2.1.4. Suppose $D = (d_{ij})_{i,j\in[n]}$ is an $n \times n$ doubly stochastic matrix. Then, $\forall i, j \in [n]$ it satisfies the following constraints:

1. $\sum\limits_{i=1}^{n} d_{ij} = \sum\limits_{j=1}^{n} d_{ij} = 1$
2. $d_{ij} \in \mathbb{R}_{\geq 0}$.

Every matrix in $\text{Mat}_n(\mathbb{R})$ can be considered as a point in $\mathbb{R}^{n^2}$. Regarding D as a point in $\mathbb{R}^{n^2}$, each d_{ij} can be viewed as the $[n(i-1)+j]$-th coordinate of the point D. The above constraints form *the Birkhoff polytope* $\mathcal{B}_n$, a bounded convex set of $n \times n$ doubly stochastic matrices in $\mathbb{R}^{n^2}$.

Definition 2.1.5. Let S be a convex set in $\mathbb{C}^n$ (*i.e.*, each element of S can be written as a combination of other elements of S with non-negative real coefficients adding up to 1.) and let $p \in S$. Then, p is called an *extreme point* of S if for any distinct $x, y \in S$ and for any $0 < \lambda < 1$, $p \neq \lambda x + (1 - \lambda)y$.

Theorem 2.1.1 (Krein-Milman)**.** Let S be a bounded, convex subset of a locally convex Hausdorff vector space and E be the set of its extreme points. Then, E is not empty and the smallest convex set which contains E is the set S. In other words, every element of S can be written as a convex combination of elements of E.

Proof. See the Theorem in [12]. □

Theorem 2.1.2 (Birkhoff - von Neumann)**.** Extreme points of the Birkhoff polytope $\mathcal{B}_n$ are permutation matrices, *i.e.*, every doubly stochastic matrix is a convex combination of permutation matrices.

Proof. The following builds upon the proof introduced by Hurlbert in [13].

A point $p = (p_1, ..., p_n) \in \mathbb{R}^n$ is called *integral* or *lattice point* if $p_i \in \mathbb{Z}$ for all $i \in [n]$. The aim is to show that every extreme point of $\mathcal{B}_n$ is an integral point, hence a permutation matrix, by using contrapositive.

Let $b = (b_{ij})_{i,j} \in \mathcal{B}_n$ be a point from the Birkhoff polytope. Suppose b is not an integral point. Then there exists $b_{i_1 j_1}$ such that $0 < b_{i_1 j_1} < 1$. Starting with this coordinate let us construct a finite sequence with distinct terms. Because of constraint (1) in Definition 2.1.4, there exists another coordinate $b_{i_1 j_2}$ of the point b such that $0 < b_{i_1 j_2} < 1$. Similarly there exists $b_{i_2 j_2}$ such that $0 < b_{i_2 j_2} < 1$ and so on. Since there are only n^2-many coordinates, the sequence will terminate after some term. Among this type of sequences, a sequence with the fewest terms, *i.e.*, one of the shortest ones, will be chosen.

If the sequence is the shortest then its number of terms is even and $(i_k, j_k) = (i_1, j_1)$ for some index k. In order to show this, assume the number of terms is odd, that is $(i_k, j_{k+1}) = (i_1, j_1)$. This means $b_{i_k j_{k+1}}$, $b_{i_1 j_1}$, and $b_{i_1 j_2}$ are all in the same row. If this is the case, the term $b_{i_1j_2}$ can be removed and a shorter sequence is constructed by starting with $b_{i_2j_2}$ instead of $b_{i_1j_1}$. This is a contradiction.

Let us take the minimum element of this set, $\epsilon_0 = \min\{b_{i_1j_1}, b_{i_1j_2}, ..., b_{i_{k-1}j_k}\}$. For any $0 < \epsilon < \epsilon_0$, define $b^+(\epsilon)$ as the point such that the value of $b_{i_sj_s}$ is increased by ϵ and the value of $b_{i_sj_{s+1}}$ is decreased by ϵ for all $1 \leq s \leq k-1$. Then, since the length of the sequence is even, in each row and column $+\epsilon$ and $-\epsilon$ cancel out. Additionally, both $b_{i_sj_s} + \epsilon > 0$ and $b_{i_sj_{s+1}} - \epsilon > 0$ is satisfied for any index s. Hence, $b^+(\epsilon) \in \mathcal{B}_n$. Similarly, $b^-(\epsilon)$ can be defined such that the value of $b_{i_sj_s}$ is decreased and the value of $b_{i_sj_{s+1}}$ is increased by ϵ for all $1 \leq s \leq k-1$. Then, $b^-(\epsilon) \in \mathcal{B}_n$.

The point b can be written as $b = \frac{1}{2}b^-(\epsilon) + \frac{1}{2}b^+(\epsilon)$. Therefore, b is not an extreme point. This implies that every extreme point of $\mathcal{B}_n$ is integral hence, a permutation matrix. □

2.2 A Brief Overview of C*-algebras

In Chapter 3, quantum magic squares will be defined over the positive elements of **C***-algebras. Therefore, this section aims to introduce **C***-algebras, *-homomorphisms and positive elements of **C***-algebras, while proving some fundamental results. The primary references for this section include [14], [15] and [16].

2.2.1 C*-algebras

Definition 2.2.1. A complex vector space $\mathcal{B}$ with a norm $||.||$ is called a *Banach space* if it is complete with respect to the norm. A Banach space $\mathcal{B}$ with an associative and distributive multiplication function in which $||xy|| \leq ||x||||y||$ holds for any $x, y \in \mathcal{B}$ is called a *Banach algebra*.

Example 2.2.1. For some natural number $1 \leq p < \infty$, the p-norm is defined for any element $x = (x_1, ..., x_n) \in \mathbb{C}^n$ as $||x||_p = (|x_1|^p + ... + |x_n|^p)^{\frac{1}{p}}$. As in Example 5.2 of [17], the vector space $\mathbb{C}^n$ for some $n \in \mathbb{N}$ with the p-norm is a Banach space. Then with the usual multiplication function on $\mathbb{C}^n$ it can be shown that

$$\begin{aligned}\|x\|_p\|y\|_p = (|x_1|^p + ... + |x_n|^p)^{\frac{1}{p}}(|y_1|^p + ... + |y_n|^p)^{\frac{1}{p}} &= (\sum_{i,j\in[n]} |x_i y_j|^p)^{\frac{1}{p}} \\ &\geq (\sum_{i\in[n]} |x_i y_i|^p)^{\frac{1}{p}} \\ &= \|xy\|_p\end{aligned}$$

Since for any $x, y \in \mathbb{C}^n$ this holds, $\mathbb{C}^n$ is also a Banach algebra.

Definition 2.2.2. A *Hilbert space* $\mathcal{H}$ is a complete inner product space with inner product $\langle \cdot, \cdot \rangle$ on which the norm is defined by $\|h\| = \sqrt{\langle h, h \rangle}$ for any $h \in \mathcal{H}$.

Remark 2.2.1. Every Hilbert space is also a Banach space on which the norm is defined by the inner product.

Lemma 2.2.1. The set of bounded linear operators on a Hilbert space $\mathcal{H}$, which is denoted by $B(\mathcal{H})$, is a Banach algebra.

Proof. The set $B(\mathcal{H})$ is a vector space. Define the norm as the operator norm so that if $T \in B(\mathcal{H})$ then its norm is $\|T\| = \sup_{\|x\|\leq 1} \|T(x)\|$.

In order to show $B(\mathcal{H})$ is a Banach space it is needed to prove that $B(\mathcal{H})$ is complete. For any Cauchy sequence $\{T_n\}_{n\in\mathbb{N}}$

$$\lim_{n\to\infty} \|T_n - T_{n+1}\| = \lim_{n\to\infty} \|T_n - T_{n+1}\|\|x\| = \lim_{n\to\infty} \|T_n(x) - T_{n+1}(x)\| = 0$$

implies that $\{T_n(x)\}_{n\in\mathbb{N}}$ is also Cauchy for any $x \in \mathcal{H}$. This means that there exists linear operator $T \in \mathcal{H}$ such that $\lim_{n\to\infty} T_n(x) = T(x)$. Also, since $\{T_n\}_{n\in\mathbb{N}}$ is Cauchy for any $m \in \mathbb{N}$ there exists $M \geq 0$ such that if $n \geq m$ then $T_n \leq M$. Hence,

$$\|T(x)\| = \|\lim_{n\to\infty} T_n(x)\| \leq \lim_{n\to\infty} \|T_n(x)\| \leq \lim_{n\to\infty} M\|x\| = M\|x\|$$

proves that T is bounded. Then,

$$\lim_{n\to\infty} \|T_n - T\| = \lim_{n\to\infty} (\sup_{\|x\|\leq 1} \|T_n(x) - T(x)\|) = 0$$

implies that the limit of the sequence $\{T_n\}_{n\in\mathbb{N}}$ is T, and $T \in B(\mathcal{H})$. Therefore, $B(\mathcal{H})$ is complete.

Let $T, S \in B(\mathcal{H})$. Then,

$$\|ST\| = \sup_{\|x\|\leq 1} \|ST(x)\| \leq \|S\| \sup_{\|x\|\leq 1} \|T(x)\| = \|S\|\|T\|$$

holds.

Hence, $B(\mathcal{H})$ is a Banach algebra. □

Theorem 2.2.1. Let $\mathcal{H}$ be a Hilbert space (finite or infinite dimensional) and $\{e_i\}_{i\in I}$ be a set of its orthonormal basis. Then any bounded operator $P \in B(\mathcal{H})$ can be identified with a matrix $M = (m_{ij})_{i,j} \in \mathrm{Mat}_I(\mathbb{C})$ (multiplication in $\mathrm{Mat}_I(\mathbb{C})$ is not always defined when $|I| = \infty$ and such matrices are called infinite matrices) such that $m_{ij} = \langle Pe_j, e_i\rangle$ and $Px = Mx$ for any $x \in \mathcal{H}$.

Proof. Define a map $\phi : B(\mathcal{H}) \to \mathrm{Mat}_I(\mathbb{C})$ such that $\phi(P) = M = (m_{ij})_{i,j}$ such that $m_{ij} = \langle Pe_j, e_i\rangle$. As stated in the proof Theorem 2.15 in [14] this is a linear map whose kernel is $\{0\}$. Hence, ϕ is injective. If $x = \sum_{j\in I} x_j e_j \in \mathbb{C}$ then

$$Mx = \sum_{i\in I}(\sum_{j\in I} m_{ij}x_j)e_i = \sum_{i\in I}(\sum_{j\in I}\langle Pe_j, e_i\rangle x_j)e_i = \sum_{i\in I}(Px)_i e_i = Px.$$

Therefore, $B(\mathcal{H}) \subset \mathrm{Mat}_I(\mathbb{C})$. □

Corollary 2.2.1. If $\mathcal{H} = \mathbb{C}^n$ for some $n \in \mathbb{N}$ then $B(\mathcal{H})$ and $\mathrm{Mat}_n(\mathbb{C})$ are isomorphic as algebras. Therefore, for any bounded operator $P \in B(\mathcal{H})$ there exists a matrix $M \in \mathrm{Mat}_n(\mathbb{C})$ such that $Px = Mx$ for any $x \in \mathbb{C}^n$.

Proof. By Theorem 2.2.1 there exists an injective map $\phi : B(\mathbb{C}^n) \to \mathrm{Mat}_n(\mathbb{C})$. In order to show surjectivity consider any matrix $M = (m_{ij})_{i,j} \in \mathrm{Mat}_n(\mathbb{C})$. Then $\|M\| = \sqrt{\lambda_{max}} < \infty$ where λ_{max} is the greatest eigenvalue of matrix MM^* (spectral norm). Hence, ϕ is bijective. □

Definition 2.2.3. An *involution* is a map $*: \mathcal{B} \to \mathcal{B}$ on a complex Banach algebra $\mathcal{B}$ such that

- $(c_1 x + c_2 y)^* = \overline{c_1} x^* + \overline{c_2} y^*$
- $(xy)^* = y^* x^*$
- $(x^*)^* = x$

for any $c_1, c_2 \in \mathbb{C}$, $x, y \in \mathcal{B}$ where $\overline{c}$ denotes the conjugate of a complex number $c \in \mathbb{C}$. The element $x^* \in \mathcal{B}$ is called the *adjoint* of x.

Definition 2.2.4. A complex Banach algebra $\mathcal{B}$ together with an involution, $*$, which satisfies $\|xx^*\| = \|x\|^2$ for any $x \in \mathcal{B}$ is called a **C***-*algebra*.

Example 2.2.2. The set $B(\mathcal{H})$ of bounded operators on a Hilbert space with the operator norm is a Banach algebra by Lemma 2.2.1. Let $\mathcal{H} = \mathbb{C}^n$ for some $n \in \mathbb{N}$. According to Corollary 2.2.1 this implies that $\text{Mat}_n(\mathbb{C})$ is a Banach algebra where I_n is the unit element.

Define $*$ as the conjugate transpose of matrices. Then for any $A, B \in \text{Mat}_n(\mathbb{C})$ and any two scalars $c_1, c_2 \in \mathbb{C}$

- $(c_1 A + c_2 B)^* = (c_1 A)^* + (c_2 B)^* = \overline{c_1} A^* + \overline{c_2} B^*$
- $(AB)^* = B^* A^*$
- $(A^*)^* = A$

holds. Therefore, by Definition 2.2.3 $*$ is an involution.

Let $A \in \text{Mat}_n(\mathbb{C})$ be an arbitrary matrix, then the equivalence $\|AA^*\|_2 = \|A\|_2^2$ can be easily deduced since operator norm is equivalent to the spectral norm (square root of the greatest eigenvalue of AA^*) in finite dimensions.

Hence, $\text{Mat}_n(\mathbb{C})$ with conjugate transpose as the involution is a unital **C***-algebra.

Example 2.2.3. Suppose that $\mathcal{A}$ and $\mathcal{B}$ are two **C***-algebras. Then, their direct sum $\mathcal{A} \oplus \mathcal{B} = \{(a, b) \mid a \in \mathcal{A}, b \in \mathcal{B}\}$ is also a **C***-algebra where the associated norm is defined by $\|(a, b)\| = \max\{\|a\|, \|b\|\}$ as stated in [16].

Definition 2.2.5. A bijective map $\psi : \mathcal{A} \to \mathcal{B}$ between two $\mathbf{C}^*$-algebras is called $*$-*isomorphism* if it is an isomorphism and it satisfies $\psi(a^*) = \psi(a)^*$. If there exists such a map between $\mathcal{A}$ and $\mathcal{B}$ then they are called $*$-*isomorphic*.

Theorem 2.2.2 (Gelfand-Naimark)**.** Every $\mathbf{C}^*$-algebra is isometrically *-isomorphic to a norm-closed subalgebra of $B(\mathcal{H})$ for some Hilbert space $\mathcal{H}$.

Proof. See Theorem 11.18 in [18]. □

Corollary 2.2.2. Let $\mathcal{A}$ be a finite dimensional $\mathbf{C}^*$-algebra. Then, there exist a $*$-isomorphism, $n \in \mathbb{N}$ and $c_1, ..., c_n \in \mathbb{N}$ such that

$$\mathcal{A} \cong \mathrm{Mat}_{c_1}(\mathbb{C}) \oplus \mathrm{Mat}_{c_2}(\mathbb{C}) \oplus \cdots \oplus \mathrm{Mat}_{c_n}(\mathbb{C}).$$

Proof. Since every finite dimensional Hilbert space is isomorphic to a subset of $\mathbb{C}^n$ Corollary 2.2.1 and Gelfand-Neimark Theorem 2.2.2 asserts that $\mathcal{A} \subset \mathrm{Mat}_n(\mathbb{C})$ for some finite $n \in \mathbb{N}$. Then, Theorem 5.10 in [14] proves the corollary. □

Definition 2.2.6. Let $\mathcal{A}$ be a $\mathbf{C}^*$-algebra, $1_{\mathcal{A}}$ its unit element and $a, p, u, n \in \mathcal{A}$. Then,

- The element a is called *Hermitian (self-adjoint)* if $a = a^*$
- The element u is called *unitary* if $uu^* = u^*u = 1_{\mathcal{A}}$
- The element p is called *projection* if $p^2 = p^* = p$.
- The element n is called *normal* if $nn^* = n^*n$.

2.2.2 Spectral Theory

Definition 2.2.7. Let $a \in \mathcal{A}$ be an element of a $\mathbf{C}^*$-algebra $\mathcal{A}$. Then the *spectrum* of a, denoted by $\sigma(a)$, is defined by $\sigma(a) = \{\lambda \in \mathbb{C} \mid a - \lambda \notin \mathcal{A}^{-1}\}$ where $\mathcal{A}^{-1} \subseteq \mathcal{A}$ is the set of invertible elements of $\mathcal{A}$.

Example 2.2.4. The spectrum of any square matrix is the set of its eigenvalues. Consider the set of square matrices $\mathrm{Mat}_n(\mathbb{C})$. Then the set of its invertible elements is

$\mathrm{GL}_n(\mathbb{C}) = \{M \in \mathrm{Mat}_n(\mathbb{C}) \mid \det(M) \neq 0\}$. If $A \in \mathrm{Mat}_n(\mathbb{C})$ is an arbitrary element then,

$$\begin{aligned}\sigma(A) &= \{\lambda \in \mathbb{C} \mid A - \lambda I_n \notin \mathrm{GL}_n(\mathbb{C})\} \\ &= \{\lambda \in \mathbb{C} \mid \det(A - \lambda I_n) = 0\}.\end{aligned}$$

Hence, the spectrum of the matrix A is the set of its eigenvalues.

Proposition 2.2.1. Let $a, b \in \mathcal{A}$ be two elements of a $\mathbf{C}^*$-algebra. Then the following holds: $\sigma(ab) - \{0\} = \sigma(ba) - \{0\}$.

Proof. Suppose $ab - \lambda$ is invertible for some $0 \neq \lambda \in \mathbb{C}$. Then $(ba - \lambda)$ is also invertible with the inverse $(ba-\lambda)^{-1} = \lambda^{-1}b(ab-\lambda)^{-1}a-\lambda^{-1}$. Similarly, $ba-\lambda$ being invertibe implies $ab - \lambda$ to be invertible. Therefore, $\sigma(ab) - \{0\} = \sigma(ba) - \{0\}$. □

Definition 2.2.8. The *spectral radius* $r(a)$ of an element $a \in \mathcal{A}$ of a $\mathbf{C}^*$-algebra is defined if $\sigma(a) \neq \emptyset$. Then $r(a) = sup\{|\lambda| \mid \lambda \in \sigma(a)\}$.

Proposition 2.2.2. Let $\mathcal{A}$ be a $\mathbf{C}^*$-algebra. The spectrum of any element $a \in \mathcal{A}$ is non-empty, compact and on the disc centered at 0 with radius $\|a\|$.

Proof. Suppose $a \in \mathcal{A}$ and $\sigma(a) = \emptyset$. Define a function $\phi : \mathbb{C} \to \mathbb{C}$ and let $f \in \mathcal{A}^*$ be a linear functional on the dual of $\mathcal{A}$ such that $\phi(\lambda) = f((a-\lambda)^{-1})$. Since spectrum of a is empty f is well-defined. The function ϕ is entire by Proposition 3.4 of [14]. The limit $\lim\limits_{\lambda\to\infty} \phi(a) = 0$ implies ϕ is bounded. Hence, by Liouvilles's theorem ϕ is constant and equal to 0. However this is a contradiction. Therefore, $\sigma(a) \neq \emptyset$.

Let $\lambda \in \sigma(a)$ such that $\|\lambda\| > \|a\|$. Then, $\|\frac{a}{\lambda}\| < 1$. However this means that $a - \lambda$ is invertible by the Neumann Series Theorem which contradicts with the fact that $\lambda \in \sigma(a)$. Therefore, $\forall\, \lambda \in \sigma(a),\ \|\lambda\| \leq \|a\|$.

Let $t \notin \sigma(a)$, hence $a - t \in \mathcal{A}^{-1}$. The set of invertible elements $\mathcal{A}^{-1}$ is open by Lemma 1.3.1 of [16]. This implies that for a sufficienty small $\epsilon > 0$, $a - t - \epsilon \in \mathcal{A}^{-1}$. Therefore, $(t + \epsilon) \notin \sigma(a)$. This proves that $\sigma(a)$ is closed. Since $\sigma(a)$ is closed and bounded it is compact. □

Theorem 2.2.3. Let $a \in \mathcal{A}$ be an element of a $\mathbf{C}^*$-algebra. Then its spectral radius is the limit $r(a) = \lim_{n\to\infty} \|a^n\|^{\frac{1}{n}} \leq \|a\|$.

Proof. See Theorem 3.20 in [14] □

Theorem 2.2.4. If $\mathcal{A}$ is a $\mathbf{C}^*$-algebra and $a \in \mathcal{A}$ is Hermitian, then $r(a) = \|a\|$.

Proof. Let a be a Hermitian element. Then $\|a^2\| = \|aa^*\| = \|a\|^2$. Therefore, by induction on k, $\|a^{2^k}\| = \|a\|^{2^k}$ for any $k \in \mathbb{N}$. Consider the sequence $s_n = \|a^n\|^{\frac{1}{n}}$. The spectral radius is $r(a) = \lim_{n\to\infty} s_n$ by Theorem 2.2.3. Let $s_{n_k} = \|a^{2^k}\|^{\frac{1}{2^k}} = \|a\|$ be a subsequence. Then, $\lim_{k\to\infty} s_{n_k} = \lim_{k\to\infty} (\|a\|^{2^k})^{\frac{1}{2^k}} = \|a\|$ implies that $r(a) = \|a\|$. □

Corollary 2.2.3. For a Hermitian element $a \in \mathcal{A}$ of a $\mathbf{C}^*$-algebra if $a^n = 0$, then $a = 0$.

Proof. Since $a^n = 0$, $a^k = 0$ for any $k \geq n$. By theorem 2.2.3 and Theorem 2.2.4 $r(a) = \lim_{n\to\infty} \|a^n\|^{\frac{1}{n}} = \|a\| = 0$ implies that $a = 0$. □

Lemma 2.2.2. Let $P \in \mathbb{C}[x]$ be a complex polynomial and $\mathcal{A}$ be a $\mathbf{C}^*$-algebra. Then $P(\sigma(a)) = \sigma(P(a))$ for any $a \in \mathcal{A}$.

Proof. Let $c \in \mathbb{C}$ be an arbitrary complex scalar. Since $\mathbb{C}$ is algebraically closed $P(x) - c = k(x - r_1)(x - r_2)...(x - r_n)$.

Observe that

$$\begin{aligned} c \notin \sigma(P(a)) &\iff P(a) - c \in \mathcal{A}^{-1} \text{ is invertible} \\ &\iff a - r_i \text{ is invertible for each } i \in [n] \\ &\iff r_i \notin \sigma(a) \\ &\iff c \notin P(\sigma(a)) \end{aligned}$$

Hence, $P(\sigma(a)) = \sigma(P(a))$. □

Theorem 2.2.5. Let f be a rational function on $\mathbb{C}$ and $a \in \mathcal{A}$ be an element of a **C***-algebra. If the poles of the function f is outside of $\sigma(a)$ then $\sigma(f(a)) = f(\sigma(a))$.

Proof. Let $f(z) = \frac{P(z)}{Q(z)}$ and define $F(z) = P(z) - \lambda Q(z)$ for any $\lambda \in \mathbb{C}$. The following is true: $\lambda \in \sigma(f(a))$ if and only if $F(a) \notin \mathcal{A}^{-1}$. Then

$$\begin{aligned} F(a) \notin \mathcal{A}^{-1} &\iff 0 \in \sigma(F(a)) = \{k \in \mathbb{C} \mid F(a) - k \notin \mathcal{A}^{-1}\} \\ &\iff 0 \in F(\sigma(a)) = \{F(k) \in \mathbb{C} \mid a - k \notin \mathcal{A}^{-1}\} \text{ (by Lemma 2.2.2)} \\ &\iff \exists \mu \in \sigma(a) \text{ such that } F(\mu) = P(\mu) - \lambda Q(\mu) = 0 \\ &\iff \lambda \in f(\sigma(a)). \end{aligned}$$

□

Theorem 2.2.6. Let $a \in \mathcal{A}$ be a normal element of a **C***-algebra. If $f \in C(\sigma(a))$ then $f(\sigma(a)) = \sigma(f(a))$ where $C(\sigma(a))$ is the set of complex valued, continuous functions on $\sigma(a)$.

Proof. See Theorem 3.23 in [14]. □

Theorem 2.2.7. Let $u \in \mathcal{A}$ be a unitary element of a **C***-algebra $\mathcal{A}$. Then its spectrum $\sigma(u)$ is on the unit circle $\mathbb{T}$.

Proof. The element u being unitary means $u = u^* = u^{-1}$. Therefore, its norm is $\|u\| = \sqrt{\|u\|\|u^*\|} = \sqrt{\|u\|\|u^{-1}\|} = 1 = \|u^{-1}\|$. By Proposition 2.2.2, the spectrum $\sigma(u)$ is on the unit disc $\mathcal{D}$. Theorem 2.2.5 implies that $\sigma(u^{-1}) = \sigma(u)^{-1} = \sigma(u^*)$. Hence, the spectrum $\sigma(u)$ consist of elements λ such that $\overline{\lambda} = \lambda^{-1}$ and this implies that $\|\lambda\| = 1$. □

Theorem 2.2.8. Let $a \in \mathcal{A}$ be a Hermitian element of a **C***-algebra $\mathcal{A}$. Then the spectrum $\sigma(a)$ is a set of real numbers.

Proof. Let $a \in \mathcal{A}$ be a Hermitian element of a **C***-algebra. Define a Möbius transformation $f(z) = \frac{z+ir}{z-ir}$ where $r \in \mathbb{R}$ is a sufficiently large number such that $f(a)$ is well-defined. Then,

$$f(a)^* = \left(\frac{a+ir}{a-ir}\right)^* = \frac{a-ir}{a+ir} = \left(\frac{a+ir}{a-ir}\right)^{-1} = f(a)^{-1}$$

implies that $f(a)$ is unitary. Therefore, $\sigma(f(a)) \subset \mathbb{T}$ by Theorem 2.2.7. Using Theorem 2.2.5 we obtain $f(\sigma(a)) \subset \mathbb{T}$ and $\sigma(a) \subset f^{-1}(\mathbb{T}) = \mathbb{R}$. □

Corollary 2.2.4. Let $A \in \text{Mat}_n(\mathbb{C})$ be a Hermitian matrix. Then, $A = U^*DU$ where $U, D \in \text{Mat}_n(\mathbb{C})$ are a unitary matrix and a diagonal matrix respectively.

Proof. The matrix A has real eigenvalues by Theorem 2.2.8. Assume v_i, v_j are eigenvectors corresponding to eigenvalues λ_i, λ_j respectively. Then,

$$\lambda_i\langle v_i, v_j\rangle = \langle \lambda_i v_i, v_j\rangle = \langle Av_i, v_j\rangle = \langle v_i, A^*v_j\rangle = \langle v_i, \lambda_j v_j\rangle = \lambda_j\langle v_i, v_j\rangle$$

Then $\lambda_i \neq \lambda_j$ implies that v_i and v_j are orthogonal. Therefore, for distinct eigenvalues corresponding eigenspaces are orthogonal.

In order to show that A is diagonalizable it is needed to prove by induction that the algebraic and geometric multiplicities (m_a and m_g resp.) are the same for all eigenvalues. If $m_a(\lambda_i) = 1$ then $m_g(\lambda_i) = 1$ as well for all i. Therefore, assume $m_a(\lambda_i) = k > 1$ for some i and let v_i be a corresponding unit eigenvector such that $Av_i = \lambda_i v_i$. Then, let $\{v_i, w_1, ..., w_{n-1}\}$ be an orthonormal basis for $\mathbb{C}^n$. This implies that for any $v \in \langle v_i\rangle^\perp$

$$v_i^*Av = (Av_i)^*v = (\lambda_i v_i)^*v = \lambda_i(v_i^*v) = 0.$$

Hence, $\langle v_i\rangle^\perp$ is invariant under A. Define the unitary matrix $U = \begin{bmatrix} v_i & w_1 & \cdots & w_{n-1}\end{bmatrix}$. Then,

$$U^*AU = \left[\begin{array}{c|ccc} \lambda_i & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right]$$

Since U^*AU is a Hermitian matrix, A' is also Hermitian such that $m_a(\lambda_i) = k - 1$. This proves that A is diagonalizable where the diagonal matrix contains the eigenvalues of A in the diagonal. □

2.2.3 Positive Elements of C*-algebras

Definition 2.2.9. A Hermitian element $a \in \mathcal{A}$ of a **C***-algebra is called *positive* if $\sigma(a) \subseteq [0, \infty)$. The set of positive elements of $\mathcal{A}$ is denoted by $\mathcal{A}^+$.

The set $\mathcal{A}^+$ of a **C***-algebra $\mathcal{A}$ defines a partial order on Hermitian elements, $\mathcal{A}_{Her}$, of $\mathcal{A}$.

Definition 2.2.10. Let $\mathcal{A}_{Her}$ be the Hermitian elements of a **C***-algebra $\mathcal{A}$. Define a partial order "$\leq$" on $\mathcal{A}_{Her}$ by $a \leq b$ provided that $b - a \in \mathcal{A}^+$ for $a, b \in \mathcal{A}_{Her}$. Conversely, $a > b$ implies that $b - a \notin \mathcal{A}^+$.

Definition 2.2.11. The positive elements of $\mathrm{Mat}_n(\mathbb{C})$ are *positive semi-definite* matrices which are the $n \times n$ Hermitian matrices such that all of its eigenvalues (in other words, its spectrum) are real, non-negative numbers. A matrix $A \in \mathrm{Mat}_n(\mathbb{C})$ is called *positive definite* if all of its eigenvalues are strictly greater than 0.

Example 2.2.5. The matrix

$$A = \begin{bmatrix} 4 & 1+i & 2-i \\ 1-i & 3 & i \\ 2+i & -i & 5 \end{bmatrix}$$

is Hermitian and its eigenvalues are positive real numbers. Hence, A is a positive semi-definite (also positive definite) matrix.

Lemma 2.2.3. Let $\mathcal{A}$ be a **C***-algebra and $a \in \mathcal{A}$ is an Hermitian element. Then $a \in \mathcal{A}^+$ if and only if $\|a - k\| \leq k$ for any real number $k \geq \|a\|$.

Proof. The element $a \in \mathcal{A}$ being Hermitian implies that the spectrum is a subset of real numbers such that $\sigma(a) \subset [-k, k]$ by Theorem 2.2.8. In addition, Theorem 2.2.4 ensures that $\|a - k\| = r(a - k) = \sup_{\lambda \in \sigma(a)} (|\lambda - k|) = \sup_{\lambda \in \sigma(a)} (k - \lambda)$. Therefore, the inequality holds if $0 \leq \lambda \in \sigma(a)$. □

Theorem 4.2.2 from [15] provides some fundamental results of positive elements of $\mathbf{C}^*$-algebras which is stated as Theorem 2.2.9 below.

Theorem 2.2.9. Let $\mathcal{A}$ be a $\mathbf{C}^*$-algebra and $\mathcal{A}^+ \subset \mathcal{A}$ be the set of its positive elements. Then

i. $\mathcal{A}^+$ is closed in $\mathcal{A}$.

ii. If $a, b \in \mathcal{A}^+$ then $a + b \in \mathcal{A}^+$.

iii. $ka \in \mathcal{A}^+$ where $a \in \mathcal{A}$, $k \in \mathbb{R}_{\geq 0}$.

iv. If $a, -a \in \mathcal{A}^+$ then $a = 0$.

Proof. Let $\mathcal{A}$ be a $\mathbf{C}^*$-algebra and $\mathcal{A}^+ \subseteq \mathcal{A}$ be the set of its positive elements.

i. Let $\{a_i\}_{i\in\mathbb{N}}$ be a sequence on $\mathcal{A}^+$ whose limit is a. The elements of this sequence satisfies the inequalty $\|a_i - \|a\|\| \leq \|a\|$ for all $i \in \mathbb{N}$ by Lemma 2.2.3. Then, $\lim_{i\to\infty} \|a_i - \|a\|\| = \|a - \|a\|\| \leq \|a\|$ implies a is positive.

ii. Let $a, b \in \mathcal{A}^+$. Then $\|a - \|a\|\| \leq \|a\|$ and $\|b - \|b\|\| \leq \|b\|$. This implies that $\|(a + b) - (\|a\| + \|b\|)\| \leq \|a\| + \|b\|$. Taking $k = \|a\| + \|b\|$ in Lemma 2.2.3 it can be concluded that $a + b \in \mathcal{A}^+$.

iii. If a is a positive element its spectrum is $\sigma(a) = \{\lambda \in \mathbb{R}_{\geq 0} \mid a - \lambda \notin \mathcal{A}^{-1}\}$. Then by multiplying each element with a real number $k \geq 0$ it is obtained the set $k\sigma(a) = \{k\lambda \in \mathbb{R}_{\geq 0} \mid a - \lambda \notin \mathcal{A}^{-1}\} = \{t \in \mathbb{R}_{\geq 0} \mid ka - t \notin \mathcal{A}^{-1}\} = \sigma(ka)$ as a consequence of Lemma 2.2.2.

iv. Since a is positive $\sigma(a) \subset [0, \|a\|]$ by Proposition 2.2.2 and $\sigma(-a) \subset [-\|a\|, 0]$ by Lemma 2.2.2. Then $\sigma(a) = \{0\}$ implies that $r(a) = 0$ and by Theorem 2.2.4 $\|a\| = r(a) = 0$. Hence, $a = 0$. □

Lemma 2.2.4. If $a \in \mathcal{A}$ is an element of a $\mathbf{C}^*$-algebra and $-aa^*$ is positive, then $a = 0$.

Proof. Suppose $-aa^*$ is positive. The element a can be written as $a = b + ic$ where $b = \frac{a+a^*}{2}$ and $c = \frac{a-a^*}{2i}$ such that both b and c are Hermitian. Since spectra of b and c are on the real line both b^2 and c^2 are positive. Also, by Proposition 2.2.1 $\sigma(-aa^*) \subseteq \sigma(-a^*a) \cup \{0\} \subseteq \mathbb{R}_{\geq 0}$. Hence, $-a^*a$ is positive. Then,

$$a^*a + aa^* = (b - ic)(b + ic) + (b + ic)(b - ic) = 2b^2 + 2c^2$$

implies that $aa^* = 2b^2 + 2c^2 - a^*a$. Theorem 2.2.9 implies that aa^* is positive and since both aa^* and $-aa^*$ are positive $aa^* = 0$. Therefore, $a = 0$. □

Theorem 2.2.10. Let $a \in \mathcal{A}$ be an element of a **C***-algebra. Then the following are equivalent:

1. The element a is positive.
2. There exists a unique element $b \in \mathcal{A}^+$ such that $a = b^2$.
3. There exists an element $c \in \mathcal{A}$ such that $a = cc^*$.

Proof. In order to show that $(1) \implies (2)$, suppose $a \in \mathcal{A}$ is a positive element. Therefore, $\sigma(a) \subset [0, \|a\|]$. Define $f \in C(\sigma(a))$ as $f(x) = x^{\frac{1}{2}}$. Take $b = f(a)$. By Theorem 2.2.6 $f(\sigma(a)) = \sigma(f(a))$ hence b is positive.

Proving $(2) \implies (3)$ is trivial since if b is positive then it is Hermitian by definition. Therefore, by taking $c = b$ the equality $a = b^2 = cc^*$ holds.

For $(3) \implies (1)$, let $a = cc^*$ for some $c \in \mathcal{A}$. Then $a^* = (cc^*)^* = cc^* = a$ implies that a is Hermitian. Therefore, a can be decomposed into positive a^+, a^- respectively as proved in Theorem 4.2.3 (iii) of [15] such that $a = a^+ - a^-$ and $a^+a^- = a^-a^+ = 0$.

Define $d = ca^-$. Then

$$dd^* = (ca^-)(ca^-)^* = a^-c^*ca^- = a^-(a^+ - a^-)a^- = -(a^-)^3$$

$-dd^* = (a^-)^3$ is positive since a^- is positive. Then Lemma 2.2.4 implies that $d = 0$ and $(a^-)^3 = 0$. By Corollary 2.2.2 $a^- = 0$. Hence, $a = a^+$. □

Corollary 2.2.5. The following are equivalent:

1. $A \in \mathrm{Mat}_n(\mathbb{C})$ is a positive semi-definite matrix,
2. A is similar to a diagonal matrix with real, non-negative entries,
3. $A = BB^*$ for a positive semi-definite matrix $B \in \mathrm{Mat}_n(\mathbb{C})$,
4. $z^*Az \geq 0$ for all $z \in \mathbb{C}^n$.

Proof. Since A is positive semi-definite it is a Hermitian matrix. Therefore, for some unitary matrix U and a diagonal matrix D, which contains eigenvalues of A in the diagonal, $A = U^*DU$ by Corollary 2.2.4. Therefore, $(1) \implies (2)$ is trivial.

Let $A = P^{-1}DP$ where D is a diagonal matrix with real, non-negative entries and P be an invertible matrix. Consider the matrix $B = P^{-1}\sqrt{D}P$ which is positive semi-definite since it is similar to a diagonal matrix with real, non-zero entries. Therefore, it is Hermitian. Hence, $BB^* = B^2 = P^{-1}\sqrt{D}PP^{-1}\sqrt{D}P = P^{-1}DP = A$ proves that $(2) \implies (3)$.

Let $A = BB^*$. Then $z^*Az = z^*BB^*z = (B^*z)^*(B^*z) = \|B^*z\|^2 \geq 0$ for any $z \in \mathbb{C}^n$ proves $(3) \implies (4)$.

In order to prove that $(4) \implies (1)$, let λ be an eigenvalue and v_λ is the corresponding eigenvector of A. Then, $Av_\lambda = \lambda v_\lambda \implies v_\lambda^* A v_\lambda = \lambda v_\lambda^* v_\lambda = \lambda\|v_\lambda\|^2 \geq 0$ and $\lambda \geq 0$. Therefore, A is positive semi-definite. □

2.3 Operator Systems

The Gelfand-Naimark Theorem 2.2.2 asserts that any *-homomorphism between two **C***-algebras is also an isometry (distance preserving transformation). This inherent rigidity in classifying **C***-algebras has led operator algebraists to seek a more flexible framework which led to the development of the more general concept of *operator systems*, as discussed in [19]. Operator systems relax this rigid algebraic structure of **C***-algebras hence provide a broader context for study and application.

Operator systems are unital subspaces of the space of bounded linear maps over a Hilbert space, $B(\mathcal{H})$, that are closed under involution but not necessarily under multiplication. The theory of operator systems heavily relies on order structures, emphasizing positive elements and completely positive maps, which serve as the natural morphisms within this framework. This approach preserves the system's order and maintains the norm, ensuring that essential properties like size and spectral characteristics are conserved.

In Theorem 4.4 of their paper dated 1977 [20], Choi and Effros proved that a matrix-ordered complex vector space (Definition 2.3.7) which contain a positive cone and satisfy some additional properties is completely order-isomorphic to an operator system (see Theorem 2.3.1). This result established a foundational bridge between abstract algebraic structures and concrete operator systems, enabling the extension of many classical results to this broader context.

Definition 2.3.1. Let $B(\mathcal{H})$ be the set of bounded, linear operators on a Hilbert space $\mathcal{H}$ and $* : B(\mathcal{H}) \to B(\mathcal{H})$ be the involution. A subspace $S \subseteq B(\mathcal{H})$ is an *operator system* if it satisfies:

1. $1_{B(\mathcal{H})} \in S$,
2. $x \in S \iff x^* \in S$.

C*-algebras are operator systems that additionally satisfy a norm condition involving the product of an element and its adjoint ($\|xx^*\| = \|x\|^2$ for any element of x). In this sense, operator systems can be viewed as a generalization of **C***-algebras.

Definition 2.3.2. Let V be a complex vector space. Then a subset $\mathcal{C} \subset V$ is called a *cone* if $\alpha x \in \mathcal{C}$ for any $x \in \mathcal{C}$, $\alpha \in \mathbb{R}_{>0}$ and $x_1 + x_2 \in \mathcal{C}$ if $x_1, x_2 \in \mathcal{C}$. In addition, $\mathcal{C}$ is called

- *convex* if $\lambda x + (1 - \lambda) y \in \mathcal{C}$ for any $x, y \in \mathcal{C}$ and $\lambda \in [0, 1]$,
- *salient* if $0 \neq x \in \mathcal{C}$ implies $-x \notin \mathcal{C}$,
- *pointed* if $0 \in \mathcal{C}$ and $x, -x \in \mathcal{C}$ implies $x = 0$,

- *generating* if any element of V can be written as a difference of two elements in $\mathcal{C}$, *i.e.*, $V = \mathcal{C} - \mathcal{C} = \{c_1 - c_2 \mid c_1, c_2 \in \mathcal{C}\}$.

Definition 2.3.3. Let $\mathcal{C} \subset V$ be a cone in a complex vector space and $c \in \mathcal{C}$ be a non-zero element. The element c is called an *extreme ray* if it cannot be decomposed as a non-negative linear combination of elements of $\mathcal{C} - \{c\}$ with real coefficients.

Moreover, a cone is called *simplicial (simplex)* if it is the span of its extreme rays and the number of extreme rays is equal to its dimension.

Example 2.3.1. Consider $V = \mathbb{C}^2$ and $\{(1,0),(i,1)\}$ are two linearly independent vectors in V. Then the set $\{\lambda_1(1,0) + \lambda_2(i,1) \mid \lambda_1, \lambda_2 \in \mathbb{R}_{\geq 0}\}$ is a simplicial cone and $(1,0)$ and $(i,1)$ are its extreme rays.

Definition 2.3.4. A cone is called *proper* if it is convex, pointed, generating and topologically closed.

Remark 2.3.1. A proper cone $\mathcal{C}$ on a vector space V induces a partial ordering on V such that $a \leq b \iff b - a \in \mathcal{C}$. According to this partial order, any element of V is positive if and only if it is in $\mathcal{C}$. Therefore, a proper cone is also called a *positive cone*.

Example 2.3.2. Let $\mathcal{A}$ be a $\mathbf{C}^*$-algebra and $\mathcal{A}^+$ denotes the set of its positive elements. Then, closedness, convexity and pointedness of $\mathcal{A}^+$ immediately follows from Theorem 2.2.9. In order to show that $\mathcal{A}^+$ is generating, consider any $a \in \mathcal{A}_{her}$ the set of Hermitian elements of $\mathcal{A}$. Then there exist $a^+, a^- \in \mathcal{A}^+$ such that $a^+a^* = a^-a^+ = 0$ and $a = a^+ - a^-$ which was proved in Theorem 4.2.3 of [15]. Hence $\mathcal{A}$ is a proper cone.

Definition 2.3.5. Let V be a partially ordered, complex vector space. A self-adjoint element $e \in V$ is called an *order unit* if for every self-adjoint $x \in V$ there exists $r \in \mathbb{R}_{>0}$ such that $x \leq re$.

Moreover, an order unit e is called *Archimedean* if for all $r > 0$ and a self-adjoint $x \in V$, $0 \leq re + x$ implies $x \geq 0$.

Example 2.3.3. The set $\mathrm{Mat}_n(\mathbb{C})$ is a partially ordered, complex vector space. For an arbitrary Hermitian matrix $H \in \mathrm{Her}_n(\mathbb{C})$, Corollary 2.2.4 asserts that $H = U^*DU$ for a unitary matrix U and a diagonal matrix D which contains eigenvalues of H in the diagonal. Let, λ_{max} be the greatest eigenvalue of H and define $r = |\lambda_{max}| + 1$. Then, $rI_n - H = U^*(rI_n - D)U$ is positive semi-definite implies that $H \leq rI_n$. Therefore I_n is an order unit of $\mathrm{Mat}_n(\mathbb{C})$.

In order to show that I_n is an Archimedean order unit, let $H = U^*DU$ be an arbitrary Hermitian matrix and suppose $0 \leq rI_n + H$ is true for all $r > 0$. Then,

$$\begin{aligned} 0 \leq rI_n + H &\implies 0 \leq U^*(rI_n + D)U \\ &\implies 0 \leq U^*(rI_n + \lambda_{min} I_n)U \\ &\implies 0 \leq r + \lambda_{min} \\ &\implies 0 \leq \lim_{r \to 0}(r + \lambda_{min}) = \lambda_{min}. \end{aligned}$$

Hence, H is a positive semi-definite matrix. Therefore, I_n is an Archimedean order unit.

Definition 2.3.6. Let V and W be two partially ordered, complex vector spaces. A bijection $\phi : V \to W$ which satisfies $v > 0 \iff \phi(v) > 0$ for any $v \in V$ is called an *order isomorphism*.

Definition 2.3.7. Let V be a complex vector space and $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ be a sequence of proper cones where $\mathcal{C}_n \subset \mathrm{Her}_n(V)$ for all $n \in \mathbb{N}$. Then the pair $(V, \{\mathcal{C}_n\}_{n \in \mathbb{N}})$ is called a *matrix ordered vector space* if $A^*\mathcal{C}_n A \subset \mathcal{C}_m$ for any $n, m \in \mathbb{N}$ and for any $A \in \mathrm{Mat}_{n \times m}(V)$.

Example 2.3.4. Let $\mathrm{Psd}_n(\mathbb{C}) \subset \mathrm{Her}_n(\mathbb{C})$ be the set of $n \times n$ positive semi-definite matrices. According to Theorem 2.2.9, $\mathrm{Psd}_n(\mathbb{C})$ is a proper cone.

Let $A \in \mathrm{Mat}_{n \times m}(\mathbb{C})$ and $P \in \mathrm{Psd}_n(\mathbb{C})$. Consider z^*A^*PAz for an arbitrary $z \in \mathbb{C}^m$ and define $y = Az \in \mathbb{C}^n$. Then, $z^*(A^*PA)z = y^*Py \geq 0$ by Corollary 2.2.5 and therefore (A^*PA) is also a positive semi-definite matrix. Hence, $A^*PA \in \mathrm{Psd}_m(\mathbb{C})$ which proves that $(\mathbb{C}, \{\mathrm{Psd}(\mathbb{C})\}_{n \in \mathbb{N}})$ is a matrix ordered vector space.

Definition 2.3.8. Let $(V, \{\mathcal{C}_n\}_{n\in\mathbb{N}})$ be a matrix ordered, complex vector space. A self-adjoint element $e \in V$ is called a *matrix order unit* if for every $n \in \mathbb{N}$ and for any matrix $A \in \text{Her}_n(V)$, there exists $r \in \mathbb{R}_{>0}$ such that $re_n - A \in \mathcal{C}_n$ where $e_n = e \otimes I_n$.

Moreover, a matrix order unit is called *Archimedean* if for any $A \in \text{Her}_n(V)$ and for all $r > 0$, $re_n - A \in \mathcal{C}_n$ implies $A \in \mathcal{C}_n$.

Therefore, a matrix order unit serves as an order unit not just for elements of V, but also for matrices over V.

Definition 2.3.9. Let $(V, \{\mathcal{C}_n^V\}_{n\in\mathbb{N}})$ and $(W, \{\mathcal{C}_n^W\}_{n\in\mathbb{N}})$ be two matrix ordered, complex vector spaces. A linear map $\phi : V \to W$ is called a *complete order isomorphism* if

1. ϕ is an order isomorphism between V and W and
2. ϕ induces an order isomorphism $\phi_n : \text{Mat}_n(V) \to \text{Mat}_n(W)$ for each $n \in \mathbb{N}$ defined by applying ϕ entrywise, *i.e.*, $\phi_n(\mathcal{C}_n^V) = \mathcal{C}_n^W$.

Remark 2.3.2. A complete order isomorphism preserves the order structure both at the level of individual elements and at the level of matrices.

Theorem 2.3.1 (Choi-Effros)**.** A matrix ordered, complex vector space V with an Archimedean matrix order unit $e \in V$ is completely order isomorphic to an operator system S in which e is mapped to 1_S.

Proof. See Theorem 4.4 in [20]. □

In the light of Choi-Effros Theorem, abstract operator systems can be defined. An abstract operator system extends the concept of an operator system by not explicitly referencing operators on a Hilbert space. This abstract definition simplifies the key features of operator systems, making it easier to study them in a wider, more general context.

Definition 2.3.10 (Abstract Operator System)**.** Let V be a complex vector space and $\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ be a sequence of proper cones such that $\mathcal{C}_n \subset \text{Her}_n(V)$. Then $\mathcal{C} = \bigcup_{n\in\mathbb{N}} \mathcal{C}_n$ is an *abstract operator system* if

1. $A \in \mathcal{C}_n,\ V \in \text{Mat}_{n\times m}(\mathbb{C}) \implies V^*AV \in \mathcal{C}_m$, or equivalently $(V, \{\mathcal{C}_n\}_{n\in\mathbb{N}})$ is a matrix ordered vector space

2. V has an Archimedean matrix order unit $e \in \mathcal{C}_1$.

It can be observed that an abstract operator system on a vector space is not necessarily unique since it depends on the choice of the sequence of proper cones.

Definition 2.3.11. Let V be a complex vector space and $\mathcal{C}_1^{ph} \subset \text{Her}_1(V) \subset \mathbb{R}^d$ be a proper cone where $d \in \mathbb{N}$. Define

$$\mathcal{C}_n^{ph} = \{\ (P_1, P_2, ..., P_d) \in \text{Her}_n(\mathbb{C})^d \mid \forall v \in V^n,\ (vP_1v^*, ..., vP_dv^*) \in \mathcal{C}_1^{ph}\}$$

for some $n \in \mathbb{N}$ and

$$\mathcal{C}^{max} = \bigcup_{n\in\mathbb{N}} \mathcal{C}_n^{ph}.$$

The vector space $\mathcal{C}^{max}$ is the *largest operator system* on V by [21].

Definition 2.3.12. Let V be a complex vector space and $\mathcal{C}_1^{pt} \subset \text{Her}_1(V) \subset \mathbb{R}^d$ be a proper cone where $d \in \mathbb{N}$. Define $\mathcal{C}_n^{pt} = \{\sum(c \otimes P) \mid c \in \mathcal{C}_1^{pt}, P \in \text{Psd}_n(\mathbb{C})\}$ for some $n \in \mathbb{N}$ and

$$\mathcal{C}^{min} = \bigcup_{n\in\mathbb{N}} \mathcal{C}_n^{pt}.$$

The vector space $\mathcal{C}^{min}$ is *the smallest operator system* on V by Lemma 4.1 in [21].

Remark 2.3.3. The largest operator system extending a proper cone $\mathcal{C}_1 \subset V$ contains all the other operator systems on V extending $\mathcal{C}_1$ and similarly the smallest one is contained in all the other operator systems on V extending $\mathcal{C}_1$.

Theorem 2.3.2. Let V be a complex vector space, $\mathcal{C}_1 \subset \text{Her}_1(V)$ be a proper cone and $\mathcal{C}^{min}$ and $\mathcal{C}^{max}$ be the smallest and largest operator systems on V extending $\mathcal{C}_1$. If $\mathcal{C}_1$ is not a simplicial cone then $\mathcal{C}^{min} \subsetneq \mathcal{C}^{max}$.

Proof. See the proof of Theorem 1 in [22] and also [23]. □

CHAPTER 3

QUANTUM MAGIC SQUARES

In this chapter, the concept of magic squares will be expanded to include their quantum versions, which are obtained by changing the underlying algebra from real numbers to $\mathbf{C}^*$-algebras, as studied in our main references [2] and [1]. In addition, distinct types of quantum magic squares, along with their interrelations as established in the mentioned literature, will be presented. Lastly, the magic cone will be defined, the smallest and largest magic operator systems extending the magic cone will be given.

3.1 Quantum Magic Squares

Definition 3.1.1. Let $\mathcal{A}$ be a $\mathbf{C}^*$-algebra. Let $\mathcal{A}^+$ denote positive elements of $\mathcal{A}$. A matrix $M \in \mathrm{Mat}_n(\mathcal{A}^+)$ is called a *quantum magic square* if the sum of each row and column is $1_{\mathcal{A}}$, the identity element of $\mathcal{A}$.

Remark 3.1.1. It is stated in Corollary 2.2.2 that every finite dimensional $\mathbf{C}^*$-algebra can be written as a direct sum of matrices. Hence, in this and the following chapters the underlying algebra will be taken as $\mathrm{Mat}_s(\mathbb{C})$ for some $s \in \mathbb{N}$. Then, the positive semi-definite matrices, $\mathrm{Psd}_s(\mathbb{C})$, will serve as the non-negative elements of this algebra.

Definition 3.1.2. Let $M \in \mathrm{Mat}_n(\mathrm{Psd}_s(\mathbb{C}))$ be a quantum magic square. The numbers n and s are called the *external* and *internal* size of M respectively. The set of all quantum magic squares with external size n and internal size s is denoted by $\mathcal{M}_n^s$. The set of all $n \times n$ quantum magic squares is denoted by $\mathcal{M}_n = \bigcup_{s \in \mathbb{N}} \mathcal{M}_n^s$.

Example 3.1.1. Consider the matrix

$$M = \begin{bmatrix} \begin{pmatrix} 0.75 & 0.25 \\ 0.25 & 0.25 \end{pmatrix} & \begin{pmatrix} 0.25 & -0.25 \\ -0.25 & 0.75 \end{pmatrix} \\ \begin{pmatrix} 0.25 & -0.25 \\ -0.25 & 0.75 \end{pmatrix} & \begin{pmatrix} 0.75 & 0.25 \\ 0.25 & 0.25 \end{pmatrix} \end{bmatrix}$$

which is a quantum magic square, *i.e.*, $M \in \mathcal{M}_2^2(\mathbb{C})$, since its entries are positive semi-definite matrices and each row and column sum to I_2.

Definition 3.1.3. A *Positive Operator Valued Measure (POVM)* is a set of positive semi-definite matrices $\{A_1, ..., A_n\}$ of $\text{Mat}_s(\mathbb{C})$ such that $\sum_{i=1}^{n} A_i = I_s$. If all A_i's are also projections then the set is called *Projective Valued Measure (PVM).*

Remark 3.1.2. A matrix $M \in \text{Mat}_n(\text{Psd}_s(\mathbb{C}))$ is a quantum magic square if and only if every row and column of M forms a POVM.

Remark 3.1.3. Let $M \in \mathcal{M}_n^1 \subset \text{Mat}_n(\mathbb{R})$ be a quantum magic square with internal size is 1. Then M is a *doubly stochastic matrix* in the classical sense.

Remark 3.1.4. Let $M \in \mathcal{M}_1^s \subset \text{Psd}_s(\mathbb{C})$ be a quantum magic square with external size 1. Then M is the $s \times s$ identity matrix, *i.e.*, $\mathcal{M}_1^s = \{I_s\}$.

Remark 3.1.5. Let $M \in \mathcal{M}_2^s$ be a quantum magic square. Then M can be decomposed as the following:

$$M = \begin{bmatrix} A & I_s - A \\ I_s - A & A \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes A + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes I_s - A.$$

where A and $I_s - A$ are positive semi-definite matrices.

Definition 3.1.4. Let $P = (p_{ij})_{i,j} \in \mathcal{M}_n^s$ be a quantum magic square. P is called a *quantum permutation matrix* if each p_{ij} is a projection (i.e $p_{ij}^2 = p_{ij}^* = p_{ij}$). The set of all quantum permutation matrices with exterior size n and interior size s is denoted by $\mathcal{P}_n^s$ and the set of all $n \times n$ quantum permutation matrices is denoted by $\mathcal{P}_n = \bigcup_{s \in \mathbb{N}} \mathcal{P}_n^s$.

Remark 3.1.6. A quantum magic square $P \in \mathcal{M}_n^s$ is a quantum permutation matrix if and only if each of its rows and columns form a PVM.

Lemma 3.1.1. Let $(p_{ij})_{i,j\in[n]} \in \mathcal{P}_n^s$ be a quantum permutation matrix. Then the following holds

$$p_{ik}p_{jk} = p_{ki}p_{kj} = 0$$

for any $i, j, k \in [n]$ such that $i \neq j$.

Proof. The proof follows from [9]. Take $P = (p_{ij})_{i,j} \in \mathcal{P}_n^s$. Since P is a quantum permutation matrix $p_{ij} = p_{ij}^2 = p_{ij}^*$ and $\sum_{i\in[n]} p_{ij} = I_s$. Therefore, for a fixed k,

$$\begin{aligned}\sum_{i\in[n],i\neq j} (p_{ik}p_{jk})^*(p_{ik}p_{jk}) &= \sum_{i\in[n]} (p_{ik}p_{jk})^*(p_{ik}p_{jk}) - p_{jk} \\ &= \sum_{i\in[n]} p_{jk}p_{ik}p_{jk} - p_{jk} \\ &= p_{jk} - p_{jk} = 0.\end{aligned}$$

Sum of positive semi-definite elements being 0 implies that each summad is 0 by Theorem 2.2.9, therefore $(p_{ik}p_{jk})^*(p_{ik}p_{jk}) = 0$. Hence, $p_{ik}p_{jk} = 0$ for any $i \neq j$. Similarly, it can be shown that $p_{ki}p_{kj} = 0$. □

Proposition 3.1.1. Let $I_n^s \in \mathrm{Mat}_n(\mathrm{Mat}_s(\mathbb{C}))$ be the identity matrix and $P \in \mathcal{P}_n^s$ be an arbitrary quantum permutation matrix. Then $PP^* = P^*P = I_n^s$, *i.e.*, P is unitary.

Proof. Define $Q = (q_{ij})_{i,j\in[n]} = PP^*$. Then,

$$q_{ij} = \sum_{k\in[n]} p_{ik}p_{jk}^* = \sum_{k\in[n]} p_{ik}p_{jk}.$$

If $i \neq j$, then $q_{ij} = 0$ by Lemma 3.1.1.

Conversely, if $i = j$

$$q_{ii} = \sum_{k\in[n]} p_{ik}p_{ik}^* = \sum_{k\in[n]} p_{ik} = I_s$$

Therefore, $PP^* = I_n^s$. Similarly, it can be shown that $P^*P = I_n^s$. □

Lemma 3.1.2. All the entries of a quantum permutation matrix $P = (p_{ij})_{i,j\in[n]} \in \mathcal{P}_n^s$ commute for $n \leq 3$.

Proof. Similar to the proof of Lemma 2.5 from [9], each case can be examined separately. The cases $n = 1$ and $n = 2$ are trivial. It follows from Remark 3.1.4 that $\mathcal{P}_1^s = I_s$. For $n = 2$, Remark 3.1.5 ensures that $p_{11} = p_{22} = A$ and $p_{12} = p_{21} = I_s - A$ for some $A \in \mathrm{Psd}_s(\mathbb{C})$. Hence, all entries of P commute.

In case of $n = 3$, consider p_{ij} and p_{kl}. If $i = k$ or $j = l$ or both holds, then $p_{ij}p_{kl} = 0$ by Lemma 3.1.1. Therefore, assume that $i \neq k$ and $j \neq l$. Then there exist $q \in [3]$ such that $q \neq j$ and $q \neq l$. This implies that $p_{kj} + p_{kl} + p_{kq} = p_{ij} + p_{il} + p_{iq} = I_s$. Therefore,

$$\begin{aligned} p_{ij}p_{kl}p_{iq} &= p_{ij}(p_{kj} + p_{kl} + p_{kq})p_{iq} = p_{ij}p_{iq} = 0, \\ p_{ij}p_{kl}p_{il} &= p_{ij}(p_{kj} + p_{kl} + p_{kq})p_{il} = p_{ij}p_{il} = 0 \end{aligned}$$

and

$$\begin{aligned} p_{ij}p_{kl} &= p_{ij}p_{kl}(p_{ij} + p_{il} + p_{iq}) \\ &= p_{ij}p_{kl}p_{ij} \\ &= (p_{ij}p_{kl}p_{ij})^* \\ &= (p_{ij}p_{kl})^* \\ &= p_{kl}p_{ij} \end{aligned}$$

□

The following example shows that in case where $n \geq 4$ the entries of $P \in \mathcal{P}_n^s$ need not commute.

Example 3.1.2. Let $A, B, I_s - A, I_s - B \in \mathrm{Psd}_s(\mathbb{C})$ such that $AB \neq BA$. Define

$$P = \left[\begin{array}{cc|cc} A & I_s - A & \multicolumn{2}{c}{\multirow{2}{*}{(0)}} \\ I_s - A & A & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{(0)}} & B & I_s - B \\ & & I_s - B & B \end{array}\right].$$

In particular, let $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $B = \frac{1}{2}\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Then the matrices A, B, $I_2 - A$ and $I_2 - B$ are projections. Therefore, $P \in \mathcal{P}_4^2$ is a quantum permutation matrix.

Definition 3.1.5. Let $P \in \mathcal{P}_n^s$. If $p_{ij}p_{kl} = p_{kl}p_{ij}$ for any $i, j, k, l \in [n]$ then P is a *commuting quantum permutation matrix*. The set of all commuting quantum permutation matrices with exterior size n and interior size s is denoted by $\mathcal{CP}_n^s$ and the set of $n \times n$ commuting quantum permutation matrices is denoted by $\mathcal{CP}_n = \bigcup_{s\in\mathbb{N}} \mathcal{CP}_n^s$.

Remark 3.1.7. For $n \leq 3$, commuting quantum permutation matrices and quantum permutation matrices coincide by Lemma 3.1.2, *i.e.*, $\mathcal{CP}_n^s = \mathcal{P}_n^s$

Definition 3.1.6. A quantum magic square $S \in \mathcal{M}_n^s$ is called *semi-classical* if there exists a POVM $\{Q_\pi\}_{\pi\in S_n}$ such that

$$\mathcal{S} = \sum_{\pi\in S_n} P_\pi \otimes Q_\pi$$

where $\{P_\pi\}_{\pi\in S_n}$ are the permutation matrices. The set of semi-classical magic squares with external size n and internal size s will be denoted by $\mathcal{S}_n^s$ and the set of all $n \times n$ semi-classical magic squares is denoted by $\mathcal{S}_n = \bigcup_{s\in\mathbb{N}} \mathcal{S}_n^s$.

Example 3.1.3. Let $S \in \mathcal{M}_2^3$ be defined as follows;

$$S = \begin{bmatrix} \begin{pmatrix} 0.2 & -0.01 & 0.01 \\ -0.01 & 0.3 & 0.01 \\ 0.01 & 0.01 & 0.9 \end{pmatrix} & \begin{pmatrix} 0.8 & 0.01 & -0.01 \\ 0.01 & 0.7 & -0.01 \\ -0.01 & -0.01 & 0.1 \end{pmatrix} \\ \begin{pmatrix} 0.8 & 0.01 & -0.01 \\ 0.01 & 0.7 & -0.01 \\ -0.01 & -0.01 & 0.1 \end{pmatrix} & \begin{pmatrix} 0.2 & -0.01 & 0.01 \\ -0.01 & 0.3 & 0.01 \\ 0.01 & 0.01 & 0.9 \end{pmatrix} \end{bmatrix}$$

Since each entry of S is a 3×3 positive semi-definite matrix and their sum in each row and column is the identity matrix I_3, the matrix S is indeed a quantum magic square. Observe that S can be decomposed as

$$S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{pmatrix} 0.2 & -0.01 & 0.01 \\ -0.01 & 0.3 & 0.01 \\ 0.01 & 0.01 & 0.9 \end{pmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{pmatrix} 0.8 & 0.01 & -0.01 \\ 0.01 & 0.7 & -0.01 \\ -0.01 & -0.01 & 0.1 \end{pmatrix}.$$

Hence, S is a semi-classical magic square.

Lemma 3.1.3. Quantum magic squares with exterior size $n \leq 2$ are semi-classical, *i.e.*, $\mathcal{S}_n^s = \mathcal{M}_n^s$ for $n \leq 2$.

Proof. Directly follows from Remarks 3.1.4 and 3.1.5. $\square$

The following lemma originated from Remark (4-ii) in [2] provides a method of checking whether a quantum magic square is semi-classical.

Lemma 3.1.4. Let $S \in \mathcal{M}_n^s$ and $\rho : S_n \to [n!]$ be a bijection. Define the matrices

$$B := \left[\begin{array}{c|c|c} \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & & \\ \hline & (0) & \\ \hline & & (0) \end{array}\right], \quad C_{ij} := \left[\begin{array}{c|c|c} (0) & & \\ \hline & (0) & \\ \hline & & \begin{smallmatrix} (0) & E_{ij} \\ E_{ij}^t & (0) \end{smallmatrix} \end{array}\right] \quad \text{and}$$

$$D_\pi := \left[\begin{array}{c|c|c} \begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix} & & \\ \hline & E_{\rho(\pi)\rho(\pi)} & \\ \hline & & \begin{smallmatrix} (0) & -P_\pi \\ -P_\pi^t & (0) \end{smallmatrix} \end{array}\right]$$

where $\{E_{ij}\}_{i,j}$ is the canonical basis of $\mathrm{Mat}_k(\mathbb{C})$ and $k = n$ for matrices C_{ij} and $k = n!$ for matrices D_π. Then, S is a semi-classical magic square if there exist $Q_{\pi_1}, ..., Q_{\pi_{n!}}$ where $\pi_i \in S_n$ such that the matrix

$$A = B \otimes I_s + \sum_{i,j=1}^{n} C_{ij} \otimes S_{ij} + \sum_{\pi \in S_n} D_\pi \otimes Q_\pi \tag{3.1}$$

is a positive semi-definite element of $\mathrm{Mat}_{n!+2n+2}(\mathrm{Mat}_s(\mathbb{C}))$.

Proof. The matrix A in Equation (3.1) is of the form

$$A = \left[\begin{array}{c|c|c} \left(\begin{smallmatrix} 0 & X \\ X^t & 0 \end{smallmatrix}\right) & (0) & (0) \\ \hline (0) & Y & (0) \\ \hline (0) & (0) & \left(\begin{smallmatrix} 0 & Z \\ Z^t & 0 \end{smallmatrix}\right) \end{array}\right] \text{ where } Y = \begin{pmatrix} Q_{\pi_1} & 0 & \dots & 0 \\ 0 & Q_{\pi_2} & \dots & 0 \\ \vdots & \vdots & & 0 \\ 0 & 0 & \dots & Q_{\pi_{n!}} \end{pmatrix},$$

$X = I_s - \sum Q_\pi$ and $Z = S - \sum P_\pi \otimes Q_\pi$.

If S is a semi-classical magic square then $S = \sum\limits_{\pi \in S_n} P_\pi \otimes Q_\pi$ such that Q_π's are positive semi-definite and sum to I_s. Then, $X = Z = 0$ and Y is a positive semi-definite matrix. Hence, A is a positive semi-definite matrix.

Conversely, assume that there exist matrices $\{Q_\pi\}_{\pi \in S_n}$ which make A positive semi-definite. This implies that $\left(\begin{smallmatrix} 0 & X \\ X^t & 0 \end{smallmatrix}\right)$, (Y) and $\left(\begin{smallmatrix} 0 & Z \\ Z^t & 0 \end{smallmatrix}\right)$ are positive semi-definite. Then, $X = Z = 0$ (by Theroem 1.20 of [24]). The matrix Y being positive semi-definite means all the Q_π's are positive semi-definite matrices. Hence, S is a semi-classical magic square. □

In Section 3.3 it will be proved that there are quantum magic squares which are not semi-classical.

3.2 Quantum Latin Squares

A classical Latin square of order $n \in \mathbb{N}$ is an $n \times n$ matrix such that every row and column contains numbers from 1 to n exactly once. It is trivial to see that classical Latin squares are also classical magic squares with magic constant $\frac{n(n+1)}{2}$. In the quantum version, the entries $\{1, ..., n\}$ are replaced by vectors $\{v_1, ..., v_n\}$ where for each $i \in [n]$, $v_i \in \mathbb{C}^n$ such that each row and column is an orthonormal basis of $\mathbb{C}^n$.

Definition 3.2.1. Let $L \in \text{Mat}_n(\mathbb{C}^n)$. A matrix L is called a *quantum Latin square* if every row and every column of L is an orthonormal basis of $\mathbb{C}^n$. The set of quantum Latin squares is denoted by $\text{Lat}_n^q(\mathbb{C})$.

Example 3.2.1. Consider the matrix $L = (l_{ij})_{i,j \in [n]} \in \text{Mat}_4(\mathbb{C}^4)$

$$L = \begin{bmatrix} (1,0,0,0) & (0,1,0,0) & (0,0,1,0) & (0,0,0,1) \\ (0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0) & (\frac{i}{\sqrt{5}}, 0, 0, \frac{2}{\sqrt{5}}) & (\frac{2}{\sqrt{5}}, 0, 0, \frac{-i}{\sqrt{5}}) & (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0) \\ (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0) & (\frac{2}{\sqrt{5}}, 0, 0, \frac{-i}{\sqrt{5}}) & (\frac{i}{\sqrt{5}}, 0, 0, \frac{2}{\sqrt{5}}) & (0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0) \\ (0,0,0,1) & (0,0,1,0) & (0,1,0,0) & (1,0,0,0) \end{bmatrix}.$$

Each row and column of L is an orthonormal basis of $\mathbb{C}^4$. Hence, L is a quantum Latin square.

Remark 3.2.1. Two quantum Latin squares are considered to be equivalent if their corresponding bases differ only by a complex phase factor ($e^{i\theta}$ for $\theta \in [0, 2\pi)$) in each entry.

Definition 3.2.2. A Latin square $L \in \text{Lat}_n^q(\mathbb{C})$ is called an *easy* quantum Latin square if it is formed by exactly one orthonormal basis of $\mathbb{C}^n$. In other words, all the entries of L belong to the orthonormal basis set $\{v_1, ..., v_n\}$ where $v_i \in \mathbb{C}^q$. The set of easy quantum Latin squares is denoted by $\text{Lat}_n^e(\mathbb{C})$.

Remark 3.2.2. Since the Latin square L in Example 3.2.1 contains four different orhonormal bases of $\mathbb{C}^n$ it is not an easy quantum Latin square.

Remark 3.2.3. Given an orthonormal basis $\{v_1, ..., v_n\}$ of $\mathbb{C}^n$ and a classical $n \times n$ Latin square with entries $\{1, ..., n\}$, an easy quantum Latin square can be formed by replacing i with v_i for all $i \in [n]$.

Example 3.2.2. The set $\{(1,0,0,0), (0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0), (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0), (0,0,0,1)\}$ form an orthonormal basis for $\mathbb{C}^4$. Then the matrix

$$L = \begin{bmatrix} (1,0,0,0) & (0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0) & (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0) & (0,0,0,1) \\ (0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0) & (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0) & (0,0,0,1) & (1,0,0,0) \\ (0,0,0,1) & (1,0,0,0) & (0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0) & (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0) \\ (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0) & (0,0,0,1) & (1,0,0,0) & (0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0) \end{bmatrix}$$

is an easy quantum Latin square.

Definition 3.2.3. Let $\mathcal{R}_n^s = \{(m_{ij})_{i,j\in[n]} \in \mathcal{M}_n^s \mid \text{rank}(m_{ij}) = 1,\ \forall i,j \in [n])\}$. The set $\mathcal{R}_n^s$ is the set of *rank 1 quantum magic squares*.

Remark 3.2.4. For $s > n$, $\mathcal{R}_n^s = \emptyset$ since n-many $s \times s$ matrices with rank 1 never add up to I_s.

Remark 3.2.5. Every element R of $\mathcal{R}_n^n$ is a positive semi-definite matrix of rank 1. Hence, there exists a unit vector $v_{ij} \in \mathbb{C}^n$ such that $R = v_{ij}^* v_{ij}$ by Theorem 2.2.10. Therefore, $R^2 = R^* = R$ implies that elements of $\mathcal{R}_n^n$ are quantum permutation matrices, *i.e.*, $\mathcal{R}_n^n \subset \mathcal{P}_n^n$.

Proposition 3.2.1. There exists an injective map $\phi : \text{Lat}_n^q(\mathbb{C}) \to \mathcal{R}_n^n$ for any $n \in \mathbb{N}$.

Proof. Define $\phi : \text{Lat}_n^q(\mathbb{C}) \to \mathcal{R}_n^n$ as follows:

$$\phi\left(\begin{bmatrix} v_{11} & \dots & v_{1n} \\ \vdots & & \vdots \\ v_{n1} & \dots & v_{nn} \end{bmatrix}\right) = \begin{bmatrix} v_{11}^* v_{11} & \dots & v_{1n}^* v_{1n} \\ \vdots & & \vdots \\ v_{n1}^* v_{n1} & \dots & v_{nn}^* v_{nn} \end{bmatrix}$$

For any $i, j \in [n]$, $v_{ij}^* v_{ij}$ is an $n \times n$ positive semi-definite matrix with rank 1. Since $\{v_{ij}\}$ in each row and column are orthonormal $\sum_{k=1}^{n} v_{kj}^* v_{kj} = \sum_{k=1}^{n} v_{ik}^* v_{ik} = I_n$ implies that $\phi(L) \in \mathcal{R}_n^n$ for any $L \in Lat_n^q$. ☐

Remark 3.2.6. By Proposition 3.2.1 quantum Latin squares can be identified with the corresponding quantum magic squares in $\mathcal{R}_n^n$. Therefore,

$$\text{Lat}_n^e(\mathbb{C}) \subseteq \text{Lat}_n^q(\mathbb{C}) \subseteq \mathcal{R}_n^n \subseteq \mathcal{P}_n^n \subseteq \mathcal{M}_n^n.$$

Remark 3.2.7. If v and w are orthogonal vectors in $\mathbb{C}^e$, then

$$v^*(vw^*)w = (v^*v)(w^*w) = (w^*w)(v^*v) = w^*(wv^*)v = 0.$$

Since all distinct entries of an easy quantum Latin square are orthogonal to each other, they commute. Hence,

$$\text{Lat}_n^e(\mathbb{C}) \subseteq \mathcal{CP}_n^n.$$

Theorem 3.2.1. Easy quantum Latin squares are semi-classical, *i.e.*, $Lat_n^e \subseteq \mathcal{S}_n^n$. Moreover, $\mathcal{R}_n^n \bigcap \mathcal{S}_n^n \subseteq Lat_n^e$, hence $Lat_n^e = \mathcal{R}_n^n \bigcap \mathcal{S}_n^n$.

Proof. Let $M \in Lat_n^e$ be an easy quantum Latin square. Proposition 3.2.1 and Remark 3.2.7 indicates that $M \in \mathcal{R}_n^n \bigcap \mathcal{CP}_n^n$. Since $\mathcal{CP}_n^n \subset \mathcal{S}_n^n$ by Theorem 4.2.1, $M \in \mathcal{R}_n^n \bigcap \mathcal{S}_n^n$.

Conversely, let $M \in \mathcal{R}_n^n \bigcap \mathcal{S}_n^n$ be a rank 1 semi-classical magic square. Therefore M satisfies that $M = \sum_{\pi \in S_n} P_\pi \otimes Q_\pi$ where each Q_π is a positive semi-definite matrix with rank at most 1 and $\sum_{\pi \in S_n} Q_\pi = I_n$. Mirroring the argument in the proof of Theorem 11 in [1], it will be shown that there exists an orthonormal basis of $\mathbb{C}^n$ which forms M.

Define the set of permutations $\Pi_{ij} = \{(P_\pi)_{ij} = 1 \mid \pi \in S_n\}$. If $\pi, \bar{\pi} \in \Pi_{ij}$ then Q_π and $Q_{\bar{\pi}}$ are linearly dependent matrices since M_{ij} has rank 1 implies that rank of $\sum_{\pi \in \Pi_{ij}} Q_\pi$ is also 1 for any $i, j \in [n]$. Since each row and column of M sum to the identity matrix there exist at least one $\pi \in \Pi_{ij}$ such that $Q_\pi \neq 0$. For each $i \in [n]$ choose $\pi_i \in \Pi_{i1}$ where $Q_{\pi_i} \neq 0$. The entries M_{i1} and M_{j1} are linearly independent if $i \neq j$ because otherwise their sum would also be a rank 1 matrix. Therefore, the sum of the first column would have rank at most $n-1$ implying that it cannot be the $n \times n$ identity matrix. Therefore, we can infer Q_{π_i} and Q_{π_j} are linearly independent if $i \neq j$. Then, any set Π_{kl} cannot contain more than one element of the set $\{\pi_1, ..., \pi_n\}$. Since there must be a permutation π_i such that $\pi_i(l) = k$, each Π_{kl} includes precisely one π_i from this set.

Let $\pi \in S_n - \{\pi_1, ...\pi_n\}$ be a permutation such that $\pi \in \Pi_{l1}$ and $\pi \neq \pi_l$. Then $Q_\pi \in span(Q_{\pi_l})$. There exists $j \in [n]$ such that $\pi(j) \neq \pi_l(j)$. This means $\pi \in \Pi_{\pi(j)j}$ and $\pi_l \notin \Pi_{\pi(j)j}$. Let us take $\pi_i \in \Pi_{\pi(j)j}$. Then $Q_\pi \in span(Q_{\pi_l}) \bigcap span(Q_{\pi_i}) = \{0\}$. Therefore, $Q_\pi = 0$ for any $\pi \in S_n - \{\pi_1, ...\pi_n\}$. Hence, $M = \sum_{i \in [n]} P_{\pi_i} \otimes Q_{\pi_i}$ where Q_π's are linearly independent, rank 1 matrices. This implies that for any $i \in [n]$, there exists a unit vector q_i such that $Q_{\pi_i} = q_i^* q_i$ and $\{q_1, ..., q_n\}$ is an orthonormal basis of $\mathbb{C}^n$. Thus, M is an easy quantum Latin square. □

Definition 3.2.4. For a classical Latin square $L = (l_{ij})_{i,j\in[n]}$ and a POVM (or PVM) $\{Q_i\}_{i\in[n]}$, let $\phi : [n] \to \{Q_i\}_{i\in[n]}$ be the map such that $\phi(i) = Q_i$ for all $i \in [n]$. Then, a magic square can be obtained by applying ϕ entrywise to L. The set of magic squares constructed in this way is denoted by POVML_n^s (or PVML_n^s).

Example 3.2.3. Let L be a Latin square such that $L = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}$ and consider matrices

$$Q_1 = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Q_2 = \frac{1}{3}\begin{pmatrix} 1 & 0.5 & 0 \\ 0.5 & 1 & 0.5 \\ 0 & 0.5 & 1 \end{pmatrix} \quad \text{and} \quad Q_3 = \frac{1}{3}\begin{pmatrix} 1 & -0.5 & 0 \\ -0.5 & 1 & -0.5 \\ 0 & -0.5 & 1 \end{pmatrix}$$

which form a POVM. Then

$$L' = \frac{1}{3}\begin{bmatrix} \begin{pmatrix} 1 & 0.5 & 0 \\ 0.5 & 1 & 0.5 \\ 0 & 0.5 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & -0.5 & 0 \\ -0.5 & 1 & -0.5 \\ 0 & -0.5 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & -0.5 & 0 \\ -0.5 & 1 & -0.5 \\ 0 & -0.5 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0.5 & 0 \\ 0.5 & 1 & 0.5 \\ 0 & 0.5 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & -0.5 & 0 \\ -0.5 & 1 & -0.5 \\ 0 & -0.5 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0.5 & 0 \\ 0.5 & 1 & 0.5 \\ 0 & 0.5 & 1 \end{pmatrix} \end{bmatrix}$$

is an element of POVML_3^3.

Proposition 3.2.2. Elements of POVML_n^s are semi-classical magic squares and elements of PVML_n^s are commuting elements of POVML_n^s i.e., $\text{POVML}_n^s \subseteq \mathcal{S}_n^s$ and $\text{PVML}_n^s \subseteq \text{POVML}_n^s \cap \mathcal{CP}_n^s$.

Proof. Consider an element $S \in \text{POVML}_n^s$. Let $L = (l_{ij})_{i,j\in[n]}$ be the classical Latin square and $\{Q_k\}_{k\in[n]}$ be the POVM that generate S. Define the permutation matrix $P_{\pi_k} = (p_{ij}^k)_{i,j\in[n]}$ corresponding to Q_k for some $k \in [n]$ as follows:

$$p_{ij}^k = \begin{cases} 1 & \text{if } \; l_{ij} = k \\ 0 & \text{otherwise} \end{cases}$$

Therefore, $S = \sum_{k\in[n]} P_{\pi_k} \otimes Q_k$ hence S is semi-classical.

If $\{Q_k\}_{k\in[n]}$ is a PVM, then for each $i \in [n]$, Q_i is a projection which implies that $\text{PVML}_n^s \subset \text{POVML}_n^s \cap \mathcal{P}_n^s$. Lemma 3.1.1 proves that elements of $\{Q_k\}_{k\in[n]}$ are orthogonal, hence they commute. Therefore, $\text{PVML}_n^s \subset \text{POVML}_n^s \cap \mathcal{CP}_n^s$. $\square$

3.3 Smallest and Largest Magic Operator Systems

In this section the magic cone will be defined and smallest and largest operator systems extending the magic cone will be given. The aim of this chapter is to prove that there are quantum magic squares which are not semiclassical for $n \geq 3$.

Recall that the definition of a cone and a proper cone is given in Definition 2.3.2 and 2.3.4 respectively.

Proposition 3.3.1. Define $V^s \subseteq \text{Mat}_s(\mathbb{C})$ as the vector space of $s \times s$ matrices with constant row and column sum where the involution * is entrywise conjugation. Let $\mathcal{C}^s \subset (V^s \cap \text{Her}_s(\mathbb{C}))$ be the subset of real, Hermitian matrices with non-negative entries. Then $\mathcal{C}^s$ is a proper cone.

Proof. It can easily be proven that $\mathcal{C}^s$ is a cone since $\lambda\mathcal{C}^s \subset \mathcal{C}^s$ for any $\lambda \geq 0$. The cone $\mathcal{C}^s$ is closed under non-negative scaling and addition therefore, it is convex and containing zero matrix implies that it is also pointed. Since V^s is the vector space of matrices with constant row and column sum each $v \in V^s$ can be written as $v = c_1 - c_2$ for some $c_1, c_2 \in \mathcal{C}^s$ which implies that $\mathcal{C}^s$ is generating. In addition, Hermitian matrices are topologically closed implies that $\mathcal{C}^s$ is also topologically closed. Hence, $\mathcal{C}^s$ is a proper cone. □

Definition 3.3.1. The cone $\mathcal{C}^s$ in Proposition 3.3.1 is called *the magic cone*.

Lemma 3.3.1. Let $V^s \subset \text{Mat}_s(\mathbb{C})$ be the set of matrices with constant row and column sums where the involution is entrywise conjugation and $V^s_{her} = V^s \cap \text{Her}_s(\mathbb{C})$. Then V^s is spanned over $\mathbb{C}$ by permutation matrices and V^s_{her} is spanned over $\mathbb{R}$ by permutation matrices, *i.e.*,

$$V^s = \text{span}_{\mathbb{C}}\{P^1_s\} \text{ and } V^s_{her} = \text{span}_{\mathbb{R}}\{P^1_s\}$$

Proof. The following proof is originated from Lemma 2.29 in [25].

Assume $A = (a_{ij})_{i,j} \in V^s_{her}$ such that $a_{ij} \geq 0$ for all $i, j \in [s]$. Therefore, A is a magic square with magic constant $c \geq 0$. If $c = 0$, then A is the zero matrix. Assume

$c > 0$. In this case $A' = \frac{1}{c}A$ is a doubly stochastic matrix hence A' is spanned by permutation matrices over $\mathbb{R}$ by Birkhoff-von Neumann Theorem 2.1.2. On the other hand, if there exists $i, j \in [s]$ such that $a_{ij} < 0$, take $m = \min\{a_{ij}\}_{i,j \in [s]}$ and define a new matrix $M = A + |m|J$ where J is the all ones matrix. Then M is spanned by permutation matrices. This implies A is also spanned by permutation matrices. Hence, $A = M - |m|J \in \text{span}_{\mathbb{R}}\{P_s^1\}$.

Conversely, $\sum_{\pi \in S_s} \lambda_\pi P_\pi$ where $\lambda_\pi \in \mathbb{R}$ and $P_\pi \in \{P_s^1\}$ is a magic square with magic constant $\sum_{\pi \in S_n} \lambda_\pi$ hence an element of V_{her}^s.

In order to show that V^s is spanned over $\mathbb{C}$ by permutation matrices take an arbitrary matrix $A \in (V^s - V_{her}^s)$. Then $A = \text{Re}(A) + i\text{Im}(A)$ where $\text{Re}(A)$ and $\text{Im}(A)$ represents the real and imaginary parts of A respectively. Therefore, if the constant rows and columns sum is $c_1 + ic_2$ then rows and columns sum of $\text{Re}(A)$ is constant and equal to c_1. Similarly, the constant sum of $\text{Im}(A)$ is equal to c_2. Hence, $\text{Re}(A)$ and $\text{Im}(A)$ are in V_{her}^s. Since $\text{Re}(A)$ and $\text{Im}(A)$ are spanned over $\mathbb{R}$ by permutation matrices, $A \in \text{span}_{\mathbb{C}}\{P_s^1\}$. □

Remark 3.3.1. In an $s \times s$ square matrix whose row and column sums is a constant number c, one can arbitrarily select $(s-1)$ entries in a row (or column) and the remaining entry is determined by c. Hence, $\dim_{\mathbb{C}}(V^s) = \dim_{\mathbb{R}}(V_{her}^s) = (s-1)^2 + 1$ by Lemma 9 (ii) of [2].

Lemma 3.3.2. The matrix J is an Archimedean matrix order unit on the magic cone $\mathcal{C}^s$ over V^s.

Proof. The all ones matrix J is in the magic cone $\mathcal{C}^s$ by definition. Let $A = (a_{ij})_{i,j \in [s]}$ be an arbitrary real, Hermitian matrix with constant row and column sum $c \geq 0$. The matrix $rJ - A$ is a Hermitian matrix with non-negative entries whose row and column sums are $sr - c$ where $r = \max\{|a_{ij}|\}_{i,j,\in[s]}$. Hence, $rJ - A \in \mathcal{C}^s$ implies that J is an order unit. If $A = (A_1, ..., A_{n^2}) \in (V_{her}^s)^{n^2} \simeq \text{Her}_n(V_{her}^s)$ for some $n \in \mathbb{N}$, then r can be choosen as $r = \max\{r_{A_1}, ..., r_{A_{n^2}}\}$ such that r_{A_i}'s are defined as above. Therefore, $r(J \otimes I_n) - A \in \mathcal{C}_n^s$. Hence, J is a matrix order unit.

In order to show that is Archimedean let $A = (a_{ij}) \in V_{her}^s$ such that $rJ - A \in \mathcal{C}^s$

for all $r > 0$. If $a_{ij} < 0$ for some $i, j \in [s]$ then chosing $0 < r < |a_{ij}|$ implies that $(rJ - A)_{ij} \leq 0$ which contradicts with the assumption that $rJ - A \in \mathcal{C}^s$ for all $r > 0$. A similar argument can be produced for higher matrix orders as well. Hence, J is an Archimedean matrix order unit. $\square$

Remark 3.3.2. The largest operator system on $V^s \subset \mathrm{Mat}_s(\mathbb{C})$ extending the magic cone $\mathcal{C}^s = \mathfrak{L}_1^s \subset V_{her}^s \subset \mathbb{R}^{s^2}$ is the set $\mathfrak{L}^s = \bigcup_{n\in\mathbb{N}} \mathfrak{L}_n^s$ such that

$$\mathfrak{L}_n^s = \{(P_1, ..., P_{s^2}) \in \mathrm{Her}_n(\mathbb{C})^{s^2} \mid \forall v \in \mathbb{C}^n, \ \ (vP_1v^*, ..., vP_{s^2}v^*) \in \mathfrak{L}_1^s\}$$

by Definition 2.3.11.

Remark 3.3.3. The smallest operator system on $V^s \subset \mathrm{Mat}_s(\mathbb{C})$ extending the magic cone $\mathcal{C}^s = \mathfrak{S}_1^s$ is the set $\mathfrak{S}^s = \bigcup_{n\in\mathbb{N}} \mathfrak{S}_n^s$ such that

$$\begin{aligned}
\mathfrak{S}_n^s &= \{\sum(c \otimes P) \mid c \in \mathfrak{S}_1^s, \ \ P \in \mathrm{Psd}_n(\mathbb{C})\} \\
&= \{\sum(\sum_{\pi\in S_n}(\lambda_\pi P_\pi) \otimes P) \mid \lambda_\pi \in \mathbb{R}, \ \ P \in \mathrm{Psd}_n(\mathbb{C})\} \text{ by Lemma 3.3.1} \\
&= \{\sum_{\pi\in S_n} P_\pi \otimes \sum(\lambda_\pi P) \mid \lambda_\pi \in \mathbb{R}, \ \ P \in \mathrm{Psd}_n(\mathbb{C})\} \\
&= \{\sum_{\pi\in S_n} P_\pi \otimes Q_\pi \mid Q_\pi \in \mathrm{Psd}_n(\mathbb{C})\}
\end{aligned}$$

by Definition 2.3.12.

Remark 3.3.4. The set of magic squares $\mathcal{M}_n^s$ is a proper subset of $\mathfrak{L}_n^s$. If an element of $\mathcal{M}_n^s$ is also an element of $\mathfrak{S}_n^s$ then it is semi-classical, *i.e.*, $\mathcal{S}_n^s = \mathcal{M}_n^s \cap \mathfrak{S}_n^s$.

Lemma 3.3.3. The magic cone $\mathcal{C}^s$ is not simplicial for $s > 3$.

Proof. The magic cone $\mathcal{C}^s$ has $(s-1)^2 + 1$ dimensions by Remark 3.3.1. The permutation matrices are extreme rays of $\mathcal{C}^s$. However $s! > (s-1)^2 + 1$ for $s \geq 3$ implies that $\mathcal{C}^s$ is not simplicial for $s > 3$ by Definition 2.3.3. $\square$

The following theorem is Corollary (15-i) in [2]

Theorem 3.3.1. For $s \geq 2$ and $n \geq 3$, there are quantum magic squares which are not semi-classical *i.e.*, $\mathcal{S}_n^s \subsetneq \mathcal{M}_n^s$.

Proof. Remark 2.3.2 ensures that $(\mathfrak{L}_n^s - \mathfrak{S}_n^s) \neq \emptyset$ for $n \geq 3$. Then, there exists a positive semi-definite matrix $M = (m_{ij})_{i,j} \in (\mathfrak{L}_n^s - \mathfrak{S}_n^s)$ whose row and columns sums are $\sum\limits_{i\in[n]} m_{ij} = \sum\limits_{j\in[n]} m_{ij}$. This implies that there exists an invertible matrix $v \in \mathrm{Mat}_n(\mathbb{C})$ such that $v^*Mv = I_s$ by Corollary 2.2.5. Define a quantum magic square M' as $M' = (I_n \otimes v)^* M (I_n \otimes v)$. Since M is not a semi-classical magic square by Remark 3.3.4 then $M' \notin \mathcal{S}_n^s$. □

CHAPTER 4

LIMITATIONS OF BIRKHOFF-VON NEUMANN THEOREM

4.1 Matrix Convex Hull

Let V be a vector space over $\mathbb{C}$. As defined in Definition 2.1.3 a convex combination of a set of distinct points $\{v_1, ..., v_n\} \subseteq V$ is a linear combination $\sum\limits_{i \in [n]} c_i v_i$ where each coefficient $c_i \in \mathbb{R}_{\geq 0}$ is a non-negative real scalar and $\sum\limits_{i \in [n]} c_i = 1$. A subset of V is called a *convex set* if it is closed under convex combinations.

Similarly, as per Definition 1.1 in [26], a matrix convex combination of a set of matrices $\{A^{(1)}, ..., A^{(n)}\}$, where $A^{(i)} \in \text{Mat}_{s_i}(\mathbb{C})$ which may vary in size, is defined as a linear combination $\sum\limits_{i \in [n]} V_i^* A^{(i)} V_i$ where V_i's are $s_i \times t$ rectangular matrices over $\mathbb{C}$ and $\sum\limits_{i \in [n]} V_i^* V_i = I_t$. A set of matrices is called *matrix convex* if it remains closed under matrix convex combinations. Matrix convexity provides a dimension-free, hence stronger, version of convexity. Unlike classical convexity, which is defined in a fixed dimensional Euclidean space, a matrix convex set can include matrices of varying sizes [27].

In the next section matrix convexity will be used to prove that Birkhoff-von Neumann Theorem 2.1.2, which states that every doubly stochastic matrix is a convex combination of permutation matrices, fails for quantum magic squares in general.

Definition 4.1.1. Let $R_s \subseteq \text{Mat}_n(\text{Her}_s(\mathbb{C}))$ for any $s \in \mathbb{N}$ and define $R = \bigcup_{s\in\mathbb{N}} R_s$. The set R is called *matrix convex* if

$$\sum_{i\in[r]} v_i^* A^{(i)} v_i \in R_t$$

holds for all $r, t \geq 1$, for all $A^{(i)} \in R_{s_i}$ and for any $v_i \in \text{Mat}_{s_i,t}(\mathbb{C})$ where $\sum_i v_i^* v_i = I_t$. The matrix multiplication $v_i^* \cdot v_i$ is defined entrywise.

Definition 4.1.2. The intersection of all matrix convex supersets of a set R is called its *matrix convex hull* and it is denoted by $mconv(R)$.

Example 4.1.1. Consider the set of $n \times n$ quantum magic squares $\mathcal{M}_n = \bigcup_{s\in\mathbb{N}} \mathcal{M}_n^s$. Choose arbitrary $M^1 \in \mathcal{M}_n^{s_1}, ..., M^r \in \mathcal{M}_n^{s_r}$ and let $\{v_i\}_{i\in[r]}$ be $s_i \times t$ rectangular matrices such that $\sum_{i=1}^r v_i^* v_i = I_t$. Then,

$$\sum_{i=1}^r v_i^* M^i v_i = \begin{bmatrix} \sum_{i=1}^r v_i^* M_{11}^i v_i & \cdots & \sum_{i=1}^r v_i^* M_{1n}^i v_i \\ \vdots & & \vdots \\ \sum_{i=1}^r v_i^* M_{n1}^i v_i & \cdots & \sum_{i=1}^r v_i^* M_{nn}^i v_i \end{bmatrix}.$$

Let us take an arbitrary k^{th} row and calculate the sum,

$$\begin{aligned} \sum_{i=1}^r v_i^* M_{k1}^i v_i + \cdots + \sum_{i=1}^r v_i^* M_{kn}^i v_i &= \sum_{i=1}^r v_i^* (\sum_{j=1}^n M_{kj}^i) v_i \\ &= \sum_{i=1}^r v_i^* I_{s_i} v_i \\ &= I_t \end{aligned}$$

Similarly for any column sum we obtain the identity matrix I_t. Therefore,

$$\sum_{i=1}^r v_i^* M^i v_i \in \mathcal{M}_n^t \subset \mathcal{M}_n$$

implies that $\mathcal{M}_n$ is matrix convex.

Example 4.1.2. Consider the (commuting) quantum permutation matrices $P_1 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, $P_2 = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ in $\mathcal{P}_2^1$ and matrices $v_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}$, $v_2 = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}$ such that $v_1^* v_1 + v_2^* v_2 = I_1$. Then,

$$v_1^* P_1 v_1 + v_2^* P_2 v_2 = \begin{bmatrix} \frac{1}{2} \end{bmatrix} \notin \mathcal{P}_1^1.$$

Hence the set of quantum permutation matrices $\mathcal{P}_n$ is not matrix convex.

Remark 4.1.1. The set of quantum permutation matrices $\mathcal{P}_n$ and the set of commuting quantum permutation matrices $\mathcal{CP}_n$ are not matrix convex for $n \geq 2$. Therefore, when $n \geq 2$

$$mconv(\mathcal{CP}_n) \subseteq mconv(\mathcal{P}_n) \subseteq \mathcal{M}_n.$$

If $n \leq 2$ then $mconv(\mathcal{CP}_n) = mconv(\mathcal{P}_n)$ by 3.1.4 and 3.1.5.

Remark 4.1.2. Let $R = \bigcup_{s\in\mathbb{N}} R_s$ where $R_s \subseteq \text{Mat}_n(\text{Her}_s(\mathbb{C}))$. If the set of $R = \bigcup_{s\in\mathbb{N}} R_s$ is matrix convex then R_s is matrix convex for each $s \in \mathbb{N}$. However, the converse is not always true.

Remark 4.1.3. Intersection of matrix convex sets is also matrix convex.

4.2 Limitations of Birkhoff-von Neumann Theorem

In this chapter, based on the work of Cuevas et al. [2] we will prove the subset relation $mconv(\mathcal{P}_n) \subsetneq \mathcal{M}_n$, highlighting the presence of magic squares that are not contained within the matrix convex hull of quantum permutation matrices. This observation implies that the generalization of Birkhoff-von Neumann Theorem 2.1.2 to quantum magic squares is not possible.

Lemma 4.2.1. Consider $\mathbf{C}^*$-algebra $\mathbb{C}^{S_n} = \{f \mid f : S_n \to \mathbb{C}\}$. For any matrix $M \in mconv(\mathcal{CP}_n)$ there exists a positive, unital, linear map $\phi : \mathbb{C}^{S_n} \to \text{Mat}_n(\mathbb{C})$ such that $\phi(f_{ij}) = M_{ij}$ for $i, j \in [n]$ where $f_{ij} \in \mathbb{C}^{S_n}$ is defined by

$$f_{ij}(\pi) = \begin{cases} 1 & \pi(i) = j \\ 0 & otherwise \end{cases} \quad \text{for } i, j \in [n].$$

Proof. Let $M = (M_{ij})_{i,j} \in mconv(\mathcal{CP}_n)$. Therefore, $M_{ij} = v^* u_{ij} v$ for some matrix $v \in \text{Mat}_{t,s}(\mathbb{C})$ such that $v^*v = I_s$ and $(u_{ij})_{i,j\in[n]} \in \mathcal{CP}_n$.

Define a map $\psi : \mathbb{C}^{S_n} \to \text{Mat}_n(\mathbb{C})$ by

$$\psi(f) = \sum_{\pi\in S_n} (f(\pi) \prod_{k=1}^{n} u_{k\pi(k)}).$$

Then, it can be easily shown that ψ is linear:

$$\begin{aligned}
\psi(\lambda f + g) &= \sum_{\pi\in S_n} ((\lambda f + g)(\pi) \prod_{k=1}^{n} u_{k\pi(k)}) \\
&= \sum_{\pi\in S_n} (\lambda f(\pi) \prod_{k=1}^{n} u_{k\pi(k)}) + \sum_{\pi\in S_n} (g(\pi) \prod_{k=1}^{n} u_{k\pi(k)}) \\
&= \lambda \sum_{\pi\in S_n} (f(\pi) \prod_{k=1}^{n} u_{k\pi(k)}) + \sum_{\pi\in S_n} (g(\pi) \prod_{k=1}^{n} u_{k\pi(k)}) \\
&= \lambda\psi(f) + \psi(g).
\end{aligned}$$

Any positive element $g \in \mathbb{C}^{S_n}$ is of the form $g = ff^*$ for some $f \in \mathbb{C}^{S_n}$ by Theorem 2.2.10. Therefore,

$$\begin{aligned}
\psi(ff^*) &= \sum_{\pi\in S_n} ((ff^*)(\pi) \prod_{k=1}^{n} u_{k\pi(k)}) \\
&= \sum_{\pi\in S_n} (f(\pi)f^*(\pi) \prod_{k=1}^{n} u_{k\pi(k)}) \\
&= \sum_{\pi\in S_n} (f(\pi)f^*(\pi) \prod_{k=1}^{n} u_{k\pi(k)}^2) \\
&= \sum_{\pi\in S_n} (f(\pi) \prod_{k=1}^{n} u_{k\pi(k)}) \sum_{\pi\in S_n} (f^*(\pi) \prod_{k=1}^{n} u_{k\pi(k)}^*) \\
&= \psi(f)(\psi(f))^* \geq 0
\end{aligned}$$

concludes that ψ is a positive map.

In order to show that ψ is unital take the unit of $\mathbb{C}^{S_n}$ which is $f_1 : S_n \to 1$. The unit f_1 must go to the unit of $\text{Mat}_n(\mathbb{C})$ under ψ. Then,

$$\begin{aligned}\psi(f_1) &= \sum_{\pi \in S_n} \prod_{k=1}^{n} u_{k\pi(k)} \\ &= \sum_{\tau_1=1}^{n} \cdots \sum_{\tau_n=1}^{n} \prod_{k=1}^{n} u_{k\tau_k} \\ &= \prod_{k=1}^{n} \sum_{\tau=1}^{n} u_{k\tau} = I_n\end{aligned}$$

implies ψ is unital.

Let us show that $u_{ij} = \psi(f_{ij})$. Since $f_{ij} = 1$ for all $\pi \in S_n$ such that $\pi(i) = j$ and 0 otherwise,

$$\psi(f_{ij}) = u_{ij} \sum_{\pi \in S_{n-1}} \prod_{k=1}^{n} u_{k\pi(k)} = u_{ij} \prod_{k=1}^{n-1} \sum_{\tau=1}^{n} u_{k\tau} = u_{ij}.$$

Then, define $\phi(f_{ij}) = v^* \psi(f_{ij}) v = v^* u_{ij} v = M_{ij}$ for $i, j \in [n]$. □

Theorem 4.2.1. Matrix convex hull of commuting quantum permutation matrices is equal to the set of semi-classical magic squares, *i.e.*, $mconv(\mathcal{CP}_n) = \mathcal{S}_n$.

Proof. Let $S \in \mathcal{S}_n^s$. Then, $S = \sum_{\pi \in S_n} P_\pi \otimes Q_\pi$ where P_π's are permutation matrices and Q_π's form a POVM. Then for any Q_π there exist $v_\pi \in \text{Mat}_s(\mathbb{C})$ such that $v_\pi^* v_\pi = Q_\pi$.

Let us define

$$u = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & & \vdots \\ u_{n1} & u_{n2} & \cdots & u_{nn} \end{bmatrix} \text{ such that } u_{ij} = \begin{bmatrix} P_{(\pi_1)_{ij}} & 0 & \cdots & 0 \\ 0 & P_{(\pi_2)_{ij}} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & P_{(\pi_{n!})_{ij}} \end{bmatrix}.$$

Therefore, $u \in \mathcal{CP}_n$.

Take $v = \begin{bmatrix} v_{\pi_1} \\ v_{\pi_2} \\ \vdots \\ v_{\pi_{n!}} \end{bmatrix}$, so that $v^*v = I_s$. Then, $v^*u_{ij}v = S_{ij}$. Hence, $\mathcal{S}_n \subseteq mconv(\mathcal{CP}_n)$.

On the other hand, assume $S \in mconv(\mathcal{CP}_n)$. Let the function $\delta_{\pi_i} \in \mathbb{C}^{S_n}$ be the characteristic function of $\pi_i \in S_n$. Since $\delta_{\pi_i} \geq 0$ for all $\pi \in S_n$, using the map ϕ from Lemma 4.2.1 we get $\phi(\delta\pi_i) \geq 0$ and $\sum_{\pi \in S_n} \phi(\delta\pi_i) = I_s$. Let us define $Q_\pi = \phi(\delta_\pi)$.

$$\begin{aligned} S = (S_{ij})_{i,j} &= \sum_{i,j=1}^{n} (E_{ij} \otimes S_{ij}) \\ &= (1 \otimes \phi)(\sum_{i,j=1}^{n} E_{ij} \otimes f_{ij}) \\ &= (1 \otimes \phi)(\sum_{\pi \in S_n} P_\pi \otimes \delta_\pi) \\ &= \sum_{\pi \in S_n} P_\pi \otimes Q_\pi \end{aligned}$$

Therefore, S is a semiclassical magic square. This implies $\mathcal{S}_n = mconv(\mathcal{CP}_n)$. □

Corollary 4.2.1. Matrix convex hull of commuting quantum pemutation matrices is a proper subset of the set of magic squares for $s \geq 2$ and $n \geq 3$, *i.e.*, $mconv(\mathcal{CP}_n) \subsetneqq \mathcal{M}_n$.

Proof. The matrix convex hull $mconv(\mathcal{CP}_n)$ is equal to $\mathcal{S}_n$ by Theorem 4.2.1 and $\mathcal{S}_n^s \subsetneqq \mathcal{M}_n^s$ for $s \geq 2$, $n \geq 3$ by Theorem 3.3.1 imply that $mconv(\mathcal{CP}_n) \subsetneqq \mathcal{M}_n$. □

Lemma 4.2.2. Let $u \in \text{Mat}_s(\mathbb{C})$ be a projection, $w \in \text{Psd}_t(\mathbb{C})$ be a positive semi-definite matrix which satisfies $0 \leq w \leq I_t$ and $v \in \text{Mat}_{t,s}(\mathbb{C})$ an isometry such that $u = v^*wv$. Then, there is $p \in \text{Mat}_{t-s}(\mathbb{C})$ such that $w = u \oplus p$ and $0 \leq p \leq I_{t-s}$.

Proof. Since $v \in \text{Mat}_{s,t}(\mathbb{C})$ is an isometry and $u = v^* w v$, the matrix w can be decomposed as follows:

$$w = \begin{bmatrix} u & r \\ r^* & p \end{bmatrix}$$

for some $r \in \text{Mat}_{s,t-s}(\mathbb{C})$ and $p \in \text{Mat}_{t-s}(\mathbb{C})$. Then,

$$w^2 = \begin{bmatrix} u^2 + rr^* & ur + rp \\ r^*u + pr^* & r^*r + p^2 \end{bmatrix} = \begin{bmatrix} u + rr^* & ur + rp \\ r^*u + pr^* & r^*r + p^2 \end{bmatrix}.$$

Also, $0 \leq w \leq I_t$ implies $w^2 \leq w$. Therefore,

$$\begin{aligned} u + rr^* \leq u &\implies rr^* \leq 0 \\ &\implies r = 0 \end{aligned}$$

and we get $p^2 \leq p \implies 0 \leq p \leq I_{t-s}$. □

Corollary 4.2.2. For every $n \geq 4$ and $s \geq 2$ there are quantum permutation matrices which are not semi-classical, *i.e.*, $\mathcal{S}_n^s = mconv(\mathcal{CP}_n^s) \subsetneqq \mathcal{P}_n^s$.

Proof. Suppose $n \geq 4$ and $s \geq 2$. Let $U = (u_{ij})_{i,j} \in \mathcal{P}_n^s - \mathcal{CP}_n^s$ be a quantum permutation matrix which is not commuting. If U is a semi-classical magic square, then it is in the matrix convex hull of commuting quantum permutation matrices *i.e.*, $U \in mconv(\mathcal{CP}_n^s)$ by Theorem 4.2.1. This implies $u_{ij} = v^* w_{ij} v$ where $w_{ij} \in \mathcal{CP}_n^t$ and v is an isometry. Then, Lemma 4.2.2 proves that

$$w_{ij} = \begin{bmatrix} u_{ij} & 0 \\ 0 & p_{ij} \end{bmatrix}$$

for some $p_{ij} \in \text{Mat}_{t-s}(\mathbb{C})$. However, U is not a commuting quantum permutation matrix. Hence, $w_{ij} \notin \mathcal{CP}_n^t$ is a contradiction and U is not semi-classical. □

Definition 4.2.1. Let $C \in \text{Mat}_n(\text{Mat}_{s_1}(\mathbb{C}))$ and $D \in \text{Mat}_n(\text{Mat}_{s_2}(\mathbb{C}))$ such that $C = (c_{ij})_{i,j}$ and $D = (d_{ij})_{i,j}$. The matrix C is called a *compression* of D if there exists an isometric embedding $v : \text{Mat}_{s_2}(\mathbb{C}) \to \text{Mat}_{s_1}(\mathbb{C})$ such that $c_{ij} = v^* d_{ij} v$ for all $i, j \in [n]$. If C is a compression of D, then D is called a *dilation* of C.

Example 4.2.1. Let $C = (c_{ij})_{i,j\in[2]} = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$ and $D = (d_{ij})_{i,j\in[2]} = \left[\begin{smallmatrix} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) & \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \\ \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right) & \left(\begin{smallmatrix} 4 & 0 \\ 0 & 4 \end{smallmatrix}\right) \end{smallmatrix}\right]$. If $v = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, then $v^*v = 1$ implies that v is an isometry. Then,

$$c_{11} = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1 = v^* d_{11} v.$$

This is true for all $i, j \in [2]$. Hence, C is a compression of D and conversely, D is a dilation of C.

Definition 4.2.2. Let R be a matrix convex set and $A = (a_{ij})_{i,j\in[n]}$ is an element of R. A trivial dilation $(d_{ij})_{i,j\in[n]}$ of A is of the form

$$d_{ij} = \begin{bmatrix} a_{ij} & 0 \\ 0 & b_{ij} \end{bmatrix}$$

for some matrix (b_{ij}). The matrix A is called an *Arveson extreme point of* R if R does not include any non-trivial dilation of A. The set of Arveson extreme points of a set R is denoted by $\mathfrak{A}_R$.

Proposition 4.2.1. If $U \in \mathcal{P}_n$ is a quantum permutation matrix, then U is an Arveson extreme point of the set of quantum magic squares, $i.e.$, $\mathcal{P}_n \subseteq \mathfrak{A}_{\mathcal{M}_n}$.

Proof. Let $U = (u_{ij})_{i,j} \in \mathcal{P}_n$ be a quantum permutation matrix. Suppose U can be written as $u_{ij} = v^* m_{ij} v$ where $M = (m_{ij})_{i,j} \in \mathcal{M}_n$ is a quantum magic square and v is an isometry. Since the matrix M is a quantum magic square $0 \leq m_{ij} \leq I$ for all $i, j \in [n]$. Therefore, according to Lemma 4.2.2, $m_{ij} = u_{ij} \oplus p_{ij}$ for some matrix p_{ij}. Therefore, any dilation of U is trivial. Hence, U is an Arveson extreme point. □

Theorem 4.2.2. The set of quantum magic squares M_n is the matrix convex hull of its Arveson extreme points, $i.e.$, $mconv(\mathfrak{A}_{\mathcal{M}_n}) = \mathcal{M}_n$.

Proof. The matrix convex hull of Arveson extreme points of a free spectrahedron (a set of tuples of matrices satisfying a linear matrix inequality) is the full spectrahedron as proved in [28]. □

Theorem 4.2.2 can be regarded as a generalization of Birkhoff-von Neumann Theorem in terms of not quantum permutation matrices but Arveson extreme points.

Remark 4.2.1. There exists an Arveson extreme point of $\mathcal{M}_3^s$ which is not a quantum permutation matrix follows from Lemma 3.1.2, Corollary 4.2.1 and Proposition 4.2.2.

Remark 4.2.1 already shows that the Birkhoff-von Neumann Theorem fails for $n = 3$. So far we established the following inclusions

$$mconv(\mathcal{P}_3) \subsetneq \mathcal{M}_3 = mconv(\mathfrak{A}_{\mathcal{M}_3}).$$

In order to show that the above inclusion holds for all $n \geq 3$ the following construction, proven in [2], is needed to determine the membership of matrices in $mconv(\mathcal{P}_n)$. After this construction it will be proven that there are magic squares which do not satisfy this condition.

Construction. Let $M = (m_{ij})_{i,j\in[n]} \in \mathcal{M}_n^s$ be a quantum magic square. Define

$$\text{col}(M) = \sum_{i,j\in[n]} (e_i \otimes e_j \otimes m_{ij})$$

where $\{e_i\}_{i\in[n]}$ is the canonical basis of $\mathbb{C}^n$ and

$$\text{diag}(M) = \sum_{i,j\in[n]} (E_{ii} \otimes E_{jj} \otimes m_{ij})$$

where $\{E_{ij}\}_{i,j\in[n]}$ is the canonical basis of $\text{Mat}_n(\mathbb{C})$. Then $\text{col}(M)$ is the column matrix formed by aligning the entries of M to one column, and $\text{diag}(M)$ is the matrix formed by aligning entries of M to the main diagonal, both ordered lexicographically.

Define the map $\phi : \mathcal{M}_n^s \to \text{Mat}_n(\text{Mat}_s(\mathbb{C}))$ by $\phi(M) = \text{diag}(M) - \text{col}(M)\text{col}(M)^*$ and let $\mathcal{Z}_n$ denote the vector space of $n \times n$ matrices whose main diagonal is zero. Then,

$$\phi(M) = \begin{bmatrix} m_{11} - m_{11}^2 & -m_{11}m_{12} & \cdots & -m_{11}m_{nn} \\ -m_{12}m_{11} & m_{12} - m_{12}^2 & \cdots & -m_{12}m_{nn} \\ \vdots & \vdots & \cdots & \vdots \\ -m_{nn}m_{11} & -m_{nn}m_{12} & \cdots & m_{nn} - m_{nn}^2 \end{bmatrix}.$$

Proposition 4.2.2. For any quantum magic square $A \in mconv(\mathcal{P}_n^s)$ there exists a matrix $X \in (\mathcal{Z}_n \otimes \mathcal{Z}_n \otimes \text{Mat}_s(\mathbb{C}))_{her}$ such that $\phi(A) + X \geq 0$.

Proof. Since $A = (a_{ij})_{i,j}$ is in the matrix convex hull of quantum permutation matrices it can be decomposed as $a_{ij} = v^* u_{ij} v$ where $v \in \text{Mat}_{t,s}(\mathbb{C})$ is an isometry and $u_{ij} \in \text{Mat}_{t-s,s}$ is a projection such that

$$u_{ij} = \begin{bmatrix} a_{ij} & b_{ij}^* \\ b_{ij} & c_{ij} \end{bmatrix}.$$

Then $u_{ij}^2 = u_{ij}$ implies $b_{ij}^* b_{ij} = a_{ij} - a_{ij}^2$ and since $u_{ij} u_{ik} = u_{ij} u_{kj} = 0$ by Lemma 3.1.1, $b_{ij}^* b_{ik} = -a_{ij} a_{ik}$ and $b_{ij}^* b_{kj} = -a_{ij} a_{kj}$. Define the matrix $B = \begin{bmatrix} b_{11}^* & b_{12}^* & \cdots & b_{nn}^* \end{bmatrix}^T$ and choose $X = BB^* - \phi(A)$. It can easily be computed that the diagonal entries of X are $b_{ii}^* b_{ii} - (a_{ii} - a_{ii}^2) = 0$ and X is Hermitian. Hence, $\phi(A) + X = BB^* \geq 0$. □

Definition 4.2.3 (Moore-Penrose Inverse)**.** Let $A \in \text{Mat}_{m,n}(\mathbb{C})$ be a matrix. A matrix $A^\dagger$ is called *Moore-Penrose inverse* of the matrix A if $A^\dagger$ satisfies the following conditions:

1. $AA^\dagger A = A^\dagger$
2. $A^\dagger A A^\dagger = A$
3. $AA^\dagger = (A^\dagger A)^*$
4. $A^\dagger A = (AA^\dagger)^*$

Remark 4.2.2. Every matrix has a unique Moore-Penrose inverse [29].

Theorem 4.2.3. For $n \geq 3$, $mconv(\mathcal{P}_n) \subsetneq \mathcal{M}_n$.

Proof. The proof will use induction as in [2]. Consider the case when $n = 3$. Then, there exists an Arveson extreme point in $A \in \mathcal{M}_n$ such that A is not a quantum permutation matrix. The existence of A is already shown in Remark 4.2.1. It will be proven that if A satisfies the condition in Proposition 4.2.2, then it leads to a contradiction.

Since the matrix A is not a quantum permutation matrix then $a_{ij} - a_{ij}^2 \neq 0$ for some indices $i, j \in [3]$. Suppose that A satisfies the inequality $\phi(A) + X = BB^* \geq 0$ for an $X \in (\mathcal{Z}_n \otimes \mathcal{Z}_n \otimes \mathrm{Mat}_s(\mathbb{C}))_{her}$ and a matrix $B = (b_{ij})_{i,j}$. The proof of Proposition 4.2.2 shows that $b_{ij}^* b_{ij} = a_{ij} - a_{ij}^2 \neq 0$. Hence, there exists a vector $v \in \mathbb{C}^s$ such that $v^* b_{ij}^* b_{ij} v = 1$. On the other hand, since A is a quantum magic square

$$(b_{i1} + b_{i2} + b_{i3})^*(b_{i1} + b_{i2} + b_{i3}) = \sum_{k,l=1}^{3} b_{ik}^* b_{il} = \sum_{k=l=1}^{3} (a_{ik} - a_{ik}^2) + \sum_{\substack{k,l=1 \\ k \neq l}}^{3} -a_{ik}a_{il}$$
$$= \sum_{k,l=1}^{3} (\delta_{kl} a_{ik} - a_{ik}a_{il})$$
$$= \sum_{k=1}^{3} (a_{ik} - a_{ik} I_s) = 0.$$

This implies $(b_{i1} + b_{i2} + b_{i3}) = 0$. Similarly $(b_{1j} + b_{2j} + b_{3j}) = 0$.

Since a_{ij} is a positive semi-definite matrix, there exists $a_{ij}^{\frac{1}{2}}$. Now consider p_{ij} as the Moore-Penrose inverse of $a_{ij}^{\frac{1}{2}}$. By Definition 4.2.3, p_{ij} is Hermitian since $a_{ij}^{\frac{1}{2}}$ is Hermitian and $a_{ij}^{\frac{1}{2}} p_{ij} = p_{ij} a_{ij}^{\frac{1}{2}}$ is the orthogonal projection onto $\ker(a_{ij})^{\perp}$. Then, $b_{ij}^* b_{ij} = a_{ij} - a_{ij}^2$ implies that $b_{ij} p_{ij} a_{ij}^{\frac{1}{2}} = b_{ij}$.

Now define $A' = (a'_{ij})_{i,j \in [3]} \in \mathcal{M}_3^{s+1}$ as

$$a'_{ij} = \begin{bmatrix} a_{ij} & b_{ij} b_{11} v \\ v^* b_{11}^* b_{ij}^* & v^* b_{11}^* b_{ij}^* p_{ij}^2 b_{ij} b_{11} v + c_{ij}. \end{bmatrix}$$

where $c_{ij} \geq 0$ are real numbers. In order to show A' is indeed a magic square, it is needed to be checked that each entry is a positive semi definite matrix and each row and column sum is equal to I_{s+1}.

Let us check the positivity of the entries of A'. Each entry a'_{ij} can be written as

$$a'_{ij} = \begin{bmatrix} I_s \\ v^* b_{11}^* b_{ij} p_{ij}^2 \end{bmatrix} a_{ij} \begin{bmatrix} I_s & p_{ij}^2 b_{ij}^* b_{11} v \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & c_{ij} \end{bmatrix}$$

which is a positive semi-definite matrix.

The matrix A being a magic square implies that the upper left corner of a'_{ij}'s sum to I_s. Since $\sum_{i \in [3]} b_{ij} = \sum_{j \in [3]} b_{ij} = 0$, then the anti diagonal partititons of a'_{ij}'s sum to 0. It is only needed to be shown that

$$\sum_{i \in [3]} (v^* b_{11}^* b_{ij}^* v^* b_{11}^* b_{ij}^* p_{ij}^2 b_{ij} b_{11} v + c_{ij}) = \sum_{j \in [3]} (v^* b_{11}^* b_{ij}^* v^* b_{11}^* b_{ij}^* p_{ij}^2 b_{ij} b_{11} v + c_{ij}) = 1.$$

Therefore,

$$s_{i*} = \sum_{i\in[3]} v^* b_{11}^* b_{ij}^* v^* b_{11}^* b_{ij}^* p_{ij}^2 b_{ij} b_{11} v = \sum_{i\in[3]} (v^* b_{11}^* b_{ij} p_{ij})(v^* b_{11}^* b_{ij} p_{ij})^* \leq 1$$

$$s_{*j} = \sum_{j\in[3]} (v^* b_{11}^* b_{ij} p_{ij})(v^* b_{11}^* b_{ij} p_{ij}) \leq 1.$$

Let

$$s = \sum_{i\in[3]} (1 - s_{i*}) = \sum_{j\in[3]} (1 - s_{*j}) \geq 0.$$

Then, c_{ij}'s can be defined as

$$c_{ij} = \begin{cases} 0 & \text{if } s = 0 \\ \frac{(1-s_{i*})(1-s_{*j})}{s} & \text{otherwise.} \end{cases}$$

Therefore, A' is indeed a magic square and it is a dilation of A. However, $b_{ij} b_{11} v \neq 0$ implies that this is not a trivial dilation. This is a contradiction since A is an Arveson extreme point of M_3^s. This leads to the conclusion that the magic square A does not satisfy the inequality and it is not a member of the matrix convex hull of quantum permutation matrices, *i.e.*, $A \notin mconv(P_3^s)$.

By the induction hypothesis for $n \geq 3$ there exists an element $A \in \mathcal{M}_{n-1}$ such that $A \notin mconv(\mathcal{P}_{n-1})$. Consider $A' = \left[\begin{smallmatrix} A & 0 \\ 0 & I_s \end{smallmatrix}\right] \in \mathcal{M}_n^s$. Let $v = \left[\begin{smallmatrix} I_{n-1} \\ 0 \end{smallmatrix}\right] \in \text{Mat}_{n,n-1}(\mathbb{C})$ and $X' \in (\mathcal{Z}_n \otimes \mathcal{Z}_n \otimes \text{Mat}_s(\mathbb{C}))_{her}$ be arbitrary. Then,

$$\begin{aligned} X &= (v \otimes v \otimes I_s)^* X' (v \otimes v \otimes I_s) \in (\mathcal{Z}_{n-1} \otimes \mathcal{Z}_{n-1} \otimes \text{Mat}_s(\mathbb{C}))_{her} \\ &\implies (v \otimes v \otimes I_s)^* (\phi(A') + X')(v \otimes v \otimes I_s) = \phi(A) + X < 0 \\ &\implies \phi(A') + X' < 0 \text{ for any } X'. \end{aligned}$$

Therefore, for $n \geq 3$, $mconv(\mathcal{P}_n) \subsetneq \mathcal{M}_n$. □

Hence, $\mathcal{M}_n - mconv(\mathcal{P}_n) \neq \emptyset$ for $n \geq 3$ implies that the Birkhoff-von Neumann Theorem cannot be applied to quantum magic squares in general.

CHAPTER 5

FURTHER DISCUSSIONS

5.1 Relations Between Subsets of Quantum Magic Squares

In Chapter 3 various subsets of quantum magic squares are defined. In this section, emphasis is placed on the insights offered by Cuevas et.al. [1] with their work serving as the primary reference for the examination of the relationships among different subsets of quantum magic squares.

The following table shows all the previously defined subsets of quantum magic squares and their pairwise subset relations. Let set-r denote the set in the r^{th} row and set-c denote the set in the c^{th} column. Then, if the entry in r^{th} row and c^{th} column is

- 1 then set-c is a subset of set-r,
- 0 then subset relation between set-r and set-c is not defined.

Table 5.1: Subset relations between quantum magic squares

M_n	$\mathcal{S}_n$	$\mathfrak{A}_{\mathcal{M}_n}$	P_n	CP_n	POVML$_n$	PVML$_n$	R_n^n	Lat_n^q	Lat_n^e
$\mathcal{S}_n$	1	0	0	1	1	1	0	0	1
$\mathfrak{A}_{\mathcal{M}_n}$	0	1	1	1	0	1	1	1	1
P_n			1	1	0	1	1	1	1
CP_n				1	0	1	0	0	1
POVML$_n$					1	1	0	0	1
PVML$_n$						1	0	0	1
R_n^n							1	1	1
Lat_n^q								1	1
Lat_n^e									1

A Hasse diagram where the direction of the arrows indicate supersets can be used to visualize Table 5.1.

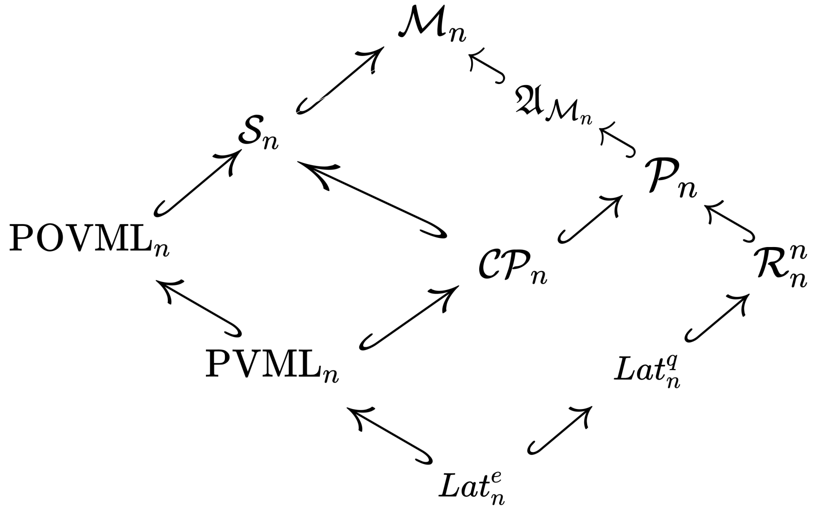

Figure 5.1: Subset relations of quantum magic squares from Figure 3 of [1]

Proposition 5.1.1. The matrix convex hull of easy Latin squares coincides with the matrix convex hull of commuting quantum permutation matrices which is the set of semi-classical magic squares, *i.e.*, $\mathcal{S}_n = mconv(\mathcal{CP}_n) = mconv(Lat_n^e)$.

Proof. The first equality follows from Theorem 4.2.1. The set of semi-classical magic squares is the matrix convex hull of quantum permutation matrices with interior size 1 deduced from Definition 3.1.6. Hence, $\mathcal{S}_n = mconv(P_n^1)$. Let $P \in \mathcal{P}_n^1$ be a permutation matrix. A Latin square L can be formed by replacing the 0 entries of P with numbers $\{2, ..., n\}$ suitably. If $\{v_1, ..., v_n\}$ is an orthonormal basis for $\mathbb{C}^n$, an easy Latin square $\tilde{L} \in Lat_n^e$ can be constructed by pairing each vector v_i with the number $i \in [n]$. Then, $P = v_1^* \tilde{L} v_1 \in mconv(Lat_n^e)$ implies $mconv(\mathcal{P}_n^1) \subseteq mconv(Lat_n^e)$. Since $Lat_n^e \subseteq \mathcal{S}_n = mconv(\mathcal{P}_n^1)$ by Theorem 3.2.1, $\mathcal{S}_n = mconv(\mathcal{CP}_n) = mconv(Lat_n^e)$. $\square$

Remark 5.1.1. By Figure 5.1 and Proposition 5.1.1 the following subset inequality

$$Lat_n^e \subset \text{PVML}_n \subset \text{POVML}_n \subset \mathcal{S}_n = mconv(Lat_n^e)$$

implies that $\mathcal{S}_n = mconv(\text{POVML}_n) = mconv(\text{PVML}_n)$.

Proposition 5.1.2. For $n \geq 4$ even, $mconv(Lat_n^e) \subsetneqq mconv(\mathcal{R}_n^n)$.

Proof. Following the proof in [1], let $v = \{v_1, ..., v_m\}$ and $w = \{w_1, ..., w_m\}$ be two orthonormal basis for $\mathbb{C}^m$ such that $v_k v_k^* w_k w_k^* \neq w_k w_k^* v_k v_k^*$ for some $k \in [m]$. Consider an arbitrary classical $m \times m$ Latin square L and $L_{ij} = k$ for indexes $i, j \in [m]$. Let $V, W \in \mathrm{Lat}_m^e$ be two quantum Latin squares generated by L and v, w respectively. Therefore,

$$P = V \oplus W = \begin{bmatrix} v_{L_{11}} v_{L_{11}}^* & \cdots & v_{L_{1n}} v_{L_{1n}}^* & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ v_{L_{n1}} v_{L_{n1}}^* & \cdots & v_{L_{nn}} v_{L_{nn}}^* & 0 & \cdots & 0 \\ 0 & \cdots & 0 & w_{L_{11}} w_{L_{11}}^* & \cdots & w_{L_{1n}} w_{L_{1n}}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & w_{L_{11}} w_{L_{11}}^* & \cdots & w_{L_{nn}} w_{L_{nn}}^* \end{bmatrix}$$

is a quantum permutation matrix. However, $P_{ij} P_{(n+i)(j+i)} \neq P_{(n+i)(j+i)} P_{ij}$ since $P_{ij} = v_k v_k^*$ and $P_{(n+i)(j+i)} = w_k w_k^*$. Take $n = 2m$. Hence, $P \notin \mathcal{CP}_n$ implies that $P \notin \mathcal{S}_n = mconv(Lat_n^e)$ by the proof of Corollary 4.2.2 and Proposition 5.1.1.

In order to prove that $P \in mconv(\mathcal{R}_n^n)$, define a map $l : \mathbb{C}^n \to \mathbb{C}^{2n}$ such that $l(v_i) = \left[\begin{smallmatrix} v_i \\ (0) \end{smallmatrix}\right]$ and $l(w_i) = \left[\begin{smallmatrix} w_i \\ (0) \end{smallmatrix}\right]$. This implies that the elements of $l(v)$ and $l(w)$ are still orthonormal but they do not cover the whole $\mathbb{C}^{2n}$. If the remaining orthonormal bases are selected as $\{e_1, ..., e_n\}$, then a matrix $C \in \mathcal{R}_n^n$ can be obtained as follows

$$C = \begin{bmatrix} l(V) & E \\ E & l(W) \end{bmatrix}$$

where E is an $n \times n$ easy quantum Latin square generated by L and $\{e_1, ...e_n\}$ for all $e_i \in [n]$. Then for $t = \left[\begin{smallmatrix} I_n \\ (0) \end{smallmatrix}\right]$, $t^* C t = V \oplus W = P$ implies that $P \in mconv(\mathcal{R}_n^n)$. Hence, $mconv(Lat_n^e) \subsetneqq mconv(\mathcal{R}_n^n)$. □

By the subset relations between matrix convex hulls of different subsets of quantum magic squares can be summarized in Figure 5.2.

$$
\begin{array}{c}
mconv(\mathfrak{A}_{\mathcal{M}_n}) = \mathcal{M}_n \\
\Big\uparrow \\
mconv(\mathcal{P}_n) \\
\Big\uparrow \\
mconv(\mathcal{R}_n^n) \\
\Big\uparrow \\
\mathcal{S}_n = mconv(\mathcal{CP}_n) = mconv(POVML_n) \\
= mconv(PVML_n) = mconv(Lat_n^e)
\end{array}
$$

Figure 5.2: Subset relations of matrix convex hulls from Figure 4 of [1]

5.2 An Application in Quantum Information

In classical physics, measurements are deterministic, and the order of measurements does not matter. Given the initial conditions of a system and the forces acting upon it, the future state of the system can be predicted with certainty. The act of measuring does not change the state of the system being measured. Physical quantities such as position, momentum, and velocity possess definite values at all times, and the measurement merely reveals these pre-existing values. Whether one measures position first and then velocity, or vice versa, the results remain consistent, and the system's state is unaffected by the measurement process.

In contrast, quantum mechanics is inherently probabilistic and the order of measurements plays a crucial role. The state of a quantum system is described by a wave function, which evolves deterministically according to the Schrödinger equation until a measurement is made. Before measurement, the system exists in a superposition of states, each with a certain probability amplitude. However, the act of measurement profoundly affects the system, causing the wave function to collapse to a particular outcome [30].

In quantum mechanics, measurements can be incompatible, meaning that the order in which measurements are performed can significantly affect the outcomes. This non-commutativity of measurements implies that performing measurement A followed by measurement B can yield different results than performing measurement B followed by measurement A [11].

A *qubit (quantum bit)* is analogous to a classical bit in computer science. However, unlike a classical bit, which can be either 0 or 1, a qubit can exist in a superposition of states. Quantum measurement is crucial in quantum information because it enables the extraction of information from quantum systems, influencing the state of the system and affecting the outcomes. Therefore, accurate and precise quantum measurements are essential for the implementation and reliability of quantum algorithms and protocols.

5.2.1 Birkhoff Body and Magic Squares

According to Blum et.al. [11] some problems in quantum information can be reduced to the problem of membership of the minimal matrix convex sets of certain polytopes. An example for such a problem is measurement compatibility. Blum et. al. proved that the membership in the matrix convex hull of the Birkhoff body (Definition 5.2.1) implies that the corresponding measurements are compatible with each other.

Consider the affine hyperplane $\mathbb{R}^{n^2}$ and center the Birkhoff Polytope (Definition 2.1.4) at $\frac{J}{n}$ where J is the all ones matrix. For every $n \times n$ doubly stochastic matrix, one can freely choose elements for only $n-1$ rows (or columns) and the remaining row (column) is determined automatically by these choices. Therefore, the Birkhoff polytope is an $(n-1)^2$-dimensional shape in this space. Then the Birkhoff body is defined as the compact, convex set in this $(n-1)^2$-dimensional subspace.

Definition 5.2.1. *The Birkhoff body* $\mathcal{B}_n$ for any $n \geq 2$, is the set of $(n-1)$ dimensional submatrices derived from n dimensional doubly stochastic matrices, shifted by $\frac{J_{n-1}}{n}$:

$$\mathcal{B}_n = \left\{ A^{(n-1)} - \frac{J_{n-1}}{n} \mid A \in \mathrm{Mat}_n(\mathbb{R}),\ \text{doubly stochastic} \right\} \subseteq \mathrm{Mat}_{n-1}(\mathbb{R})$$

where $A^{(n-1)}$ denotes the submatrix obtained by deleting the last row and last column of A.

Theorem 5.2.1. Let $(\mathcal{B}_n)_{max}$ and $(\mathcal{B}_n)_{min}$ are the maximal and minimal matrix convex sets of $\mathcal{B}_n$. If $A \in \text{Mat}_n(\text{Her}_s(\mathbb{C}))$ and $\tilde{A} \in \text{Mat}_{n-1}(\text{Her}_s(\mathbb{C}))$ is the corresponding truncated submatrix then,

- A is a quantum magic square if and only if $\tilde{A} \in (\mathcal{B}_n)_{max}$
- A is a semi-classical magic square if and only if $\tilde{A} \in (\mathcal{B}_n)_{min}$

Proof. See proof of Theorem 5.5 in [11] □

Quantum measurements can be described by a set of operators $\{M_1, ..., M_n\}$. This type of sets are already defined as POVMs (positive operator valued measure) in Definition 3.1.3. As stated previously in Remark 3.1.2 each row and column of a magic square form a POVM.

Proposition 5.2.1. POVMs that appear in rows and columns of a semi-classical magic square are compatible with each other.

Proof. See proof of Proposition 5.6 in [11] □

The converse argument for Proposition 5.2.1 is not true in general. In other words there are compatible POVMs which do not form semi-classical magic squares as shown as an example in Table 1 of [11].

CHAPTER 6

SYNOPSIS AND FUTURE RESEARCH CHALLENGES

In this thesis, we examined the relationship between classical magic squares, doubly stochastic matrices and their quantum counterparts, focusing on the limitations of generalizing the Birkhoff - von Neumann Theorem 2.1.2 to quantum magic squares.

In Chapter 2 we introduced classical magic squares as matrices with real, positive entries that satisfy a condition on all of their rows and columns and defined doubly stochastic matrices as a special subset of classical magic squares. Then we laid down some preliminary information about $\mathbf{C}^*$-algebras and operator systems.

In Chapter 3, we defined quantum magic squares as generalization of doubly stochastic matrices by replacing real, positive numbers with positive elements of a $\mathbf{C}^*$-algebra. Additionally, we discussed several subsets of quantum magic squares, including quantum permutation matrices and semi-classical magic squares.

In Chapter 4, we explained the notion of matrix convexity and matrix convex hulls. Using these concepts and following our main reference [2] we proved that the smallest matrix convex set containing the set of quantum permutation matrices is strictly contained in the set of quantum magic squares, which implies that the generalization of the Birkhoff-von Neumann Theorem is not possible.

In Chapter 5, we showed how subsets of quantum magic squares are related to each other and presented an application for the use of quantum magic squares in quantum information.

6.1 Some Open Questions

The introduction of quantum Latin squares by Musto and Vicary in 2016 [31] and quantum magic squares by Cuevas, Netzer, Drescher in 2020 [2] has opened up new frontiers in quantum mathematics. These advancements have unveiled a complex landscape, rich with potential applications in quantum information theory. Consequently, a multitude of open questions and research opportunities has emerged, inviting further exploration into the structural properties and broader implications of these quantum constructs.

6.1.1 Quantum Permutation Matrices

Some questions Weber provided about quantum permutation matrices in Section 3 of [9] are the following;

- Given two projections $p, q \in B(\mathcal{H})$ under what conditions can they be decomposed into projections $p = p_1 + p_2$ and $q = q_1 + q_2$ such that $p_1 \perp q_1$ and $p_2 \perp q_2$?
- Consider an $n \times m$ rectangular matrix such that $m > n$ and each entry is a projection such that each row sum to the identity matrix. Can we always find projections to fill the remaining rows such that the new square matrix is a quantum permutation matrix?
- Can we find a nice subclass of quantum permutation matrices that can be studied separately?
- Are there any subsets of quantum permutation matrices whose elements can act as building blocks for the entire set?

6.1.2 Quantum Sinkhorn Algorithm

For an arbitrary orthogonal matrix $M \in \mathrm{Mat}_n(\mathbb{R})$, one can transform M into a doubly stochastic matrix through an iterative normalization process. Start by dividing each element in every row by the sum of the elements in that row, ensuring each row sums to 1. Next, apply a similar normalization to the columns by dividing each element in every column by the sum of the elements in that column, ensuring each column sums to 1. Alternate between row and column normalization iteratively until the matrix converges to a state where both the rows and columns sum to 1, resulting in a doubly stochastic matrix. This iteration process is called the Sinkhorn algorithm. Nechita, Smith and Weber presented a Sinkhorn-like algorithm for quantum permutation matrices with the help of graphs in [32]. Weber ([9]) asks the following question:

- Does this Sinkhorn-like algorithm for quantum permutation matrices converge?

6.1.3 Quantum Sudoku (SudoQ)

A sudoku is a special type of a Latin square. It is an $n^2 \times n^2$ matrix where each row, each column and each $n \times n$ submatrix in its partitioned $n \times n$ grid contains numbers $\{1, ..., n^2\}$ exactly once. The well-known Sudoku puzzle involves completing a partially filled Sudoku grid to form a complete Sudoku.

A quantum sudoku (SudoQ), on the other hand, is the quantum counterpart of sudoku where each row, column and submatrix contain an orthonormal basis of $\mathbb{C}^{n^2}$. A quantum grid is a partially filled $n^2 \times n^2$ grid such that each entry is either a rank 1 orthogonal projection or 0 (to indicate emptiness).

Some conjectures related to SudoQ from [33] follow as:

- If a classical sudoku grid does not have any solutions then a SudoQ grid obtained from this classical sudoku grid (assigning numbers from 1 to n to distinct vectors of an orthonormal basis and replacing these numbers in the sudoku grid with the corresponding basis vectors) does not have any quantum solutions.
- If a classical sudoku grid has a unique solution then the corresponding SUDOQ grid does not have any additional quantum solution. In other words, the only solution is the classical solution whose entries replaced by the corresponding basis elements.

REFERENCES

[1] G. De las Cuevas, T. Netzer, and I. Valentiner-Branth, "Magic squares: Latin, semiclassical, and quantum," *Journal of Mathematical Physics*, vol. 64, no. 2, 2023.

[2] G. De las Cuevas, T. Drescher, and T. Netzer, "Quantum magic squares: Dilations and their limitations," *Journal of Mathematical Physics*, vol. 61, p. 111704, 11 2020.

[3] D. J. Hartfiel and J. W. Spellman, "A role for doubly stochastic matrices in graph theory," *Proceedings of the American Mathematical Society*, vol. 36, no. 2, pp. 389–394, 1972.

[4] J. D. Louck, "Doubly stochastic matrices in quantum mechanics," *Foundations of Physics*, vol. 27, pp. 1085–1104, Aug. 1997.

[5] G. Birkhoff, "Tres observaciones sobre el algebra lineal," *Revista Facultad de Ciencias Exactas, Puras y Aplicadas Universidad Nacional de Tucumán, Serie A (Matemáticas y Física Teórica)*, vol. 5, pp. 147–151, 1946.

[6] J. von Neumann, *A Certain Zero-sum Two-person Game Equivalent to the Optimal Assignment Problem*, pp. 5–12. Princeton: Princeton University Press, 1953.

[7] A. Dallakyan and M. Pourahmadi, "Learning bayesian networks through birkhoff polytope: A relaxation method," 07 2021.

[8] A. De Vos and S. De Baerdemacker, "A birkhoff connection between quantum circuits and linear classical reversible circuits," in *Reversible Computation* (M. K. Thomsen and M. Soeken, eds.), (Cham), pp. 23–33, Springer International Publishing, 2019.

[9] M. Weber, "Quantum permutation matrices," *Complex Anal. Oper. Theory*, vol. 17, no. 3, pp. Paper No. 37, 26, 2023.

[10] S. J. Gustafson and I. M. Sigal, *Mathematical Concepts of Quantum Mechanics*. Springer Cham, 3 ed., 2020.

[11] A. Bluhm, I. Nechita, and S. Schmidt, "Polytope compatibility - From quantum measurements to magic squares," *Journal of Mathematical Physics*, vol. 64, p. 122201, 12 2023.

[12] M. G. Krein and D. P. Milman, "On extreme points of regular convex sets," *Studia Mathematica*, vol. 9, pp. 133–138, 1940.

[13] G. H. Hurlbert, "A short proof of the Birkhoff-von Neumann Theorem," 2012.

[14] T. Banica, "Principles of operator algebras." working paper or preprint, June 2023.

[15] R. V. Kadison and J. R. Ringrose, "Chapter 4 elementary C^*-algebra theory," in *Elementary Theory*, vol. 100 of *Pure and Applied Mathematics*, pp. 236–303, Elsevier, 1983.

[16] I. F. Putnam, "Lecture notes on C^*-algebras," 2019.

[17] J. K. Hunter and B. Nachtergaele, *Applied Analysis*. World Scientific, 2001.

[18] W. Rudin, *Functional Analysis*. New York: McGraw-Hill, Inc., International Edition ed., 1991.

[19] G. Pisier, *Introduction to Operator Space Theory*. London Mathematical Society Lecture Note Series, Cambridge University Press, 2003.

[20] M.-D. Choi and E. G. Effros, "Injectivity and operator spaces," *Journal of Functional Analysis*, vol. 24, no. 2, pp. 156–209, 1977.

[21] T. Fritz, T. Netzer, and A. Thom, "Spectrahedral containment and operator systems with finite-dimensional realization," *SIAM Journal on Applied Algebra and Geometry*, vol. 1, no. 1, pp. 556–574, 2017.

[22] B. Huber and T. Netzer, "A note on non-commutative polytopes and polyhedra," 2019.

[23] V. I. Paulsen, I. G. Todorov, and M. Tomforde, "Operator system structures on ordered spaces," *Proceedings of the London Mathematical Society*, vol. 102, no. 1, pp. 25–49, 2011.

[24] R. A. Horn and F. Zhang, "Basic properties of the schur complement," in *The Schur Complement and Its Applications* (F. Zhang, ed.), pp. 17–46, Boston, MA: Springer US, 2005.

[25] I. Valentiner-Branth, "Quantum generalization of magic squares and latin squares," Master's thesis, University of Innsbruck, 2022.

[26] I. Klep and T. Štrekelj, "Facial structure of matrix convex sets," *Journal of Functional Analysis*, vol. 283, no. 7, p. 109601, 2022.

[27] T. L. Kriel, "An introduction to matrix convex sets and free spectrahedra," *Complex Analysis and Operator Theory*, vol. 13, pp. 3251–3335, Oct 2019.

[28] E. Evert and J. W. Helton, "Arveson extreme points span free spectrahedra," *Mathematische Annalen*, vol. 375, pp. 629–653, Oct 2019.

[29] O. M. Baksalary and G. Trenkler, "The Moore–Penrose inverse: a hundred years on a frontline of physics research," *The European Physical Journal H*, vol. 46, p. 9, Apr. 2021.

[30] S. Carroll, "Quantum mechanics," *Stanford Encyclopedia of Philosophy*, 2018. `https://plato.stanford.edu/entries/qm/`.

[31] B. Musto and J. Vicary, "Quantum latin squares and unitary error bases," 2016.

[32] S. S. Ion Nechita and M. Weber, "Sinkhorn algorithm for quantum permutation groups," *Experimental Mathematics*, vol. 32, no. 1, pp. 156–168, 2023.

[33] I. Nechita and J. Pillet, "Sudoq – a quantum variant of the popular game," 2020.