7-23-2024 10:00 AM

Analytic Properties of Quantum States on Manifolds

Manimugdha Saikia, *The University of Western Ontario*

Supervisor: Barron, Tatyana, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Mathematics

Abstract

The principal objective of this study is to investigate how the Kähler geometry of a classical phase space influences the quantum information aspects of the quantum Hilbert space obtained from geometric quantization and vice versa. We associated states with subsets of a product of two integral Kähler manifolds using a quantum line bundle in a particular manner. We proved that the states associated this way are separable when the subset is a finite union of products. We presented an asymptotic result for the average entropy over all the pure states on the Hilbert space $H^0(M_1, L_1^{\otimes N}) \otimes H^0(M_2, L_2^{\otimes N})$, where $H^0(M_j, L_j^{\otimes N})$ is the space of holomorphic sections of the N-th tensor powers of hermitian ample line bundle L_j on compact complex manifolds M_j. The coefficients of this asymptotic expression capture certain topological and geometric properties of the manifold.

In another project related to quantum computing, we constructed an exact synthesis algorithm for quantum gates in the groups $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ and $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ over the multi-qutrit Clifford+T gate set with the help of ancilla.

Keywords: Geometric quantization, Kähler manifolds, pre-quantum line bundles, entropy of entanglement, entanglement of formation, separable quantum states, distillation of quantum states, qutrits, quantum circuit synthesis

Summary for Lay Audience

We live in a three-dimensional world where our everyday experiences and physical phenomena occur in geometric space. To understand these phenomena, physicists and mathematicians create mathematical frameworks. For example, Newtonian Mechanics describes how a particle's motion relates to the forces acting on it. A key focus in many scientific theories is understanding how changes in one quantity affect others. In this thesis, we explore how changes in a geometric space relate to concepts from quantum information theory.

The quantum world behaves in strange ways that classical physics can't explain. For instance, quantum particles can exist in multiple places at once, and particles can become entangled so that a change in one instantly affects the other, even across vast distances.

The location and properties of a quantum particle, or quantum state, are described by matrices, which are arrays of numbers. These matrices help us understand phenomena like entanglement. In our study, we take geometric objects known as Kähler manifolds and associate quantum states with them. We study properties related to the entanglement of these states versus the properties of the geometric objects.

In another project of a slightly different flavour, we construct circuits that can be used for computers that make use of quantum mechanics. The classical computers (the common computers that we see every day) use gates that manipulate the bits (0s and 1s) to execute an algorithm. However, the set of gates is very big. So, we select a small number of convenient gates that can be used (in a circuit) to generate any desirable gate. The quantum version of this process is even more complicated owing to the set of gates being infinite. To this end, we contributed by adding one more algorithm to tackle this process.

Co-Authorship Statement

This thesis contains both independent work and joint work. Sections 4.2 and 4.3 are the contents of the respective papers [BSaikia24] and [BSaikia23] co-authored with my supervisor Tatyana Barron. Section 4.4 is the content of the paper [Saikia24] of which I am the sole author. Tatyana Barron suggested an initial version of the problem and helped me by reading the paper [Saikia24]. Necessary modifications were made to the content of these papers so that they fit the context of this thesis.

Chapter 5 is based on the joint work [KSaikia+] with Amolak Ratan Kalra, Dinesh Valluri, Sam Winnick and Jon Yard. I contributed by solving 'Step 2' (extension of the analogue of Gray code construction to qudits) and 'Step 3' (see Figure 5.7) for the initial problem at hand, which is $n = 1$ of Theorem 5.4.1. Later I generalized the results of 'Step 1' to arbitrary n. The manuscript was under preparation at the time of writing the preliminary thesis. I wrote the version that appeared in this thesis with a few modifications suggested by Dinesh Valluri.

The authors in each of these papers are listed in alphabetical order of their last name.

Acknowlegements

I would like to express my deepest gratitude to my supervisor Tatyana Barron. Her unwavering support, insightful discussions and constant encouragement kept me motivated throughout my PhD journey. She was always available to meet and discuss math. Besides that, she is also a nice and exceptionally warm person.

I extend my appreciation to the members of my examination committee for their excellent questions and comments.

The PhD journey is a tough one to undertake without a few friends there to support. I am truly grateful for friends like Gayatri Saharia and Rohan Sen, who stood by me during tough times. I want to thank Sayantan Roy Choudhury for his valuable math discussions and suggestions. I also want to thank all my friends and colleagues from the Department of Mathematics for their support throughout, with special mention to Priya Bucha Jain, Oussama Hamza, and Alejandro Santacruz.

Last but not least, I am thankful to my parents and family for their encouragement and support throughout my life. My father, despite the limited knowledge and resources at his disposal, instilled in me a sense of curiosity that has been the driving force behind my academic pursuits.

Contents

List of Figures

Chapter 1

Introduction

The work presented in this thesis is in the broad area of Differential Geometry and Quantum Information Theory. Broadly, the work here can be split into two sets of projects. The first set of projects deals with the interplay between manifolds and quantum information theory. The study of the interplay between geometric structures and analytic objects arising from these structures emerges in many different ways in mathematics. Geometric quantization, due to the work of Kostant, Souriau and Kirillov [Sou67; Kos70], is a general mathematical framework for defining a quantum theory (modelled using a Hilbert space) corresponding to a given classical theory (modelled using a symplectic manifold). This provides a framework to investigate various quantum information-theoretic aspects of this Hilbert space and possible relationships with the corresponding manifolds.

The second set of projects is purely in the area of quantum information theory and quantum computing. In one of our ongoing projects, we study the problem of distillability of NPT (non-positive partial transposition) states. This problem concerns where NPT states can be distilled into maximally entangled states [HRŽ20]. Loosely, the concept of distillation of a quantum state relates to the capacity to extract useful entanglement present in the state from a large number of copies of the state.

The other project in the area of quantum information theory concerns the synthesis of quantum circuits. Similar to the circuit model of computation in the classical realm, we have a circuit model of computation in the quantum realm as well. The gates in quantum computations are unitary operators on a suitable quantum Hilbert space and so the set of quantum gates is of infinite cardinality. For a practical quantum computer, we should be able to at least approximately decompose all gates in terms of some finite amount of special gates. To this end, the idea is to first choose an appropriate dense group inside the group of all unitaries (called *approximate synthesis*) and then try to decompose elements of the dense group exactly into a word in a finite set of unitaries (called *exact synthesis*).

This thesis contains 5 chapters in total. Chapter 1 is an introductory chapter briefly outlining the different projects carried out towards this thesis and outlining the organization of the thesis.

Chapter 2 is mostly an introductory chapter to quantum information theory and serves the purposes of fixing notations and developing various basic concepts in the area. This chapter is included in this thesis to make it more self-contained. One may refer to the books [NC10] and [BZ06] for a more comprehensive and detailed treatment of the subject. In Section 2.1, we introduce the basic briefly introduce the basics of quantum information theory. In Section 2.2, we briefly summarize the famous Dirac Bra-ket notations that are commonly used in quantum mechanics. Section 2.3 provides the necessary basic definitions related to pure and mixed quantum states and the geometry of quantum states.

In Section 2.4, we provide the mathematical formalism related to entanglement, when there are only two particles involved. Entanglement is a fascinating phenomenon in quantum physics where the interactions between two or more particles become intertwined in such a manner that the state of one particle is intricately connected to the states of the other particles involved. The state space of a closed quantum system is modelled using a Hilbert space $\mathcal{H}$, known as the quantum Hilbert space. The quantum Hilbert space for a system involving two particles is the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ of two quantum Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, one for each of the particles. The amount of correlation between the particles involved in entanglement can vary depending on the shared state of particles. This leads to quantifying the amount of entanglement. Various measures quantify the extent of entanglement and they are used for the needed purposes. One of the most famous quantities to measure this, for pure states, is the entropy of entanglement.

The concept of entropy of entanglement serves as a valuable tool not only for quantifying the degree of entanglement within a system but also for distinguishing between two key categories of states: separable states (those lacking entanglement) and maximally entangled states. The value of entropy of entanglement is in the range from 0 to $\ln d$, where d represents the smaller dimension of the two Hilbert spaces involved. At the lower end, an entropy of 0 indicates a separable state, while at the upper limit, an entropy of $\ln d$ signifies a state of maximal entanglement, where the particles' quantum states are fully intertwined.

The entanglement of formation extends the concept of entropy of entanglement to mixed states. Mixed states are represented as convex combinations of pure states, inspiring the definition of entanglement of formation. However, because the convex decomposition isn't unique, the definition incorporates an infimum to make it well-defined. In Section 2.4.2, inspired by the convex roof construction in [Uhl10], we provide proof that this infimum is indeed a minimum. Similar to the entropy of entanglement, entanglement of formation ranges from 0 to $\ln d$, distinguishing between separable states and maximally entangled states. However, due to the inclusion of the minimum in its definition, this quantity is harder to compute.

In fact, for mixed states, even the task of determining whether a state is entangled or not is also not easy. There are various criteria to test the separability of mixed states, one of the simplest being the Peres-Horodecki criterion (detailed in Section 2.5.1). The Peres-Horodecki criterion provides a sufficient condition for a state to be entangled using the "non-positivity" of the partial transpose of a state. It also serves as a necessary condition for entanglement in quantum systems of dimensions $2 \otimes 2$ and $2 \otimes 3$ (or $3 \otimes 2$), but fails to become a necessary condition in higher dimensions.

In Section 2.5, an ongoing project related to the distillability of quantum states is introduced. The main result in this section is Theorem 2.5.18. In this result, we constructed a family of non-distillable states based on the operator Schmidt rank. In a broad sense, the distillability of a quantum state means the capacity to extract a maximally entangled state from a substantial number of copies of that state using local operations and classical communications (LOCC), as detailed in Section 2.5.2. Over the years, physicists and mathematicians have made several advances and come up with some partial results based on different criteria such as rank, operator Schmidt rank, matrix rank of the states etc. Yet, a complete solution to this problem seems hard. There is also an equivalent formulation of this problem in the language of C^*-algebras [DiV+00; Cla05].

Chapter 3 serves as an introductory chapter providing background in Complex Differential Geometry and doesn't present any new results. It covers definitions and establishes notations related to symplectic manifolds, Kähler manifolds, and hermitian line bundles.

Chapter 4 contains many new results in this thesis, which deals with the first set of projects that we mentioned earlier. We briefly introduce the concept of quantization in Section 4.1. Briefly, a symplectic manifold (M, ω) is said to be pre-quantizable if there exists a hermitian line bundle $L \to M$ satisfying certain conditions. Once we have a pre-quantizable line bundle, there are various different versions of geometric quantization based on the choice of polarization. For Kähler manifold, there is a standard method of geometric quantization that yields $H^0(M, L)$, the space of holomorphic sections of the line bundle $L \to M$, as the corresponding Hilbert space.

For $j \in \{1, 2\}$, let M_j be a compact Kähler manifold and $L_j \to M_j$ be a pre-quantum line bundle. Then for each $N \in \mathbb{N}$, the line bundle $L_1^N \boxtimes L_2^N \to M_1 \times M_2$ becomes a pre-quantum line bundle, leading to the quantum Hilbert space $H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N)$. For large N, this space is isomorphic to the tensor product $H^0(M_1, L_1^N) \otimes H^0(M_2, L_2^N)$ of two quantum Hilbert spaces and so we have a framework to talk about entanglement. For notational convenience, we denote $\mathcal{H}_A = H^0(M_1, L_1^N)$ and $\mathcal{H}_B = H^0(M_2, L_2^N)$. Within this framework, various quantum information theoretic aspects arising from entanglement can be explored. The work presented in Sections 4.2, 4.3 and 4.4 deal with these quantum Hilbert spaces.

The study of asymptotics plays an important role in many areas of mathematics. Asymptotics coming from tensor powers of line bundles provide many interesting results and invariants. For instance, the coefficients of the asymptotic expansion of the Bergman kernel encode certain geometric information about the manifold and the line bundle [MM00]. In [BPU95], the authors associated a sequence of quantum states ρ_N with Lagrangian submanifold Λ and showed that certain local geometric properties of the Λ are captured by the asymptotic properties of ρ_N.

A natural question is to compute the average entropy of entanglement over the set of all pure states in the quantum Hilbert space $H^0(M_1, L_1^N) \otimes H^0(M_2, L_2^N)$ and see the parameters on which the asymptotic expression depends. This motivated us for the contents of Section 4.2. It contains the work of the paper [BSaikia24]. The proof of this result is based on an expression for the expected value of the entropy of entanglement for a tensor product of two finite-dimensional Hilbert spaces and an asymptotic Hirzebruch–Riemann–Roch Theorem for ample line bundles. The contributions of Section 4.2 are summarized in Theorems 4.2.1, 4.2.4 and 4.2.6.

Section 4.3 contains the work of the paper [BSaikia23]. The theme of the section centers on the exploration of the interplay between geometry and analysis. We aim to associate an analytic construct, derived from the Hilbert space $H^0(M_1, L_1^N) \otimes H^0(M_2, L_2^N)$ using concepts from quantum information theory, such as entanglement entropy, negativity, or entanglement of formation, with a subset of M (denoted Λ). As a guiding example, we focus on $M = \mathbb{CP}^1$ equipped with the Fubini-Study metric, where L represents the hyperplane bundle, and $\Lambda = S^1$ embedded antidiagonally as specified in Theorem 4.3.1. The theorem serves as an initial step, laying the groundwork for generalizing this statement to other M and Λ.

Section 4.4 contains the work of the paper [Saikia24]. In this section, we associate quantum states with subsets of a product of two compact connected Kähler manifolds M_1 and M_2 having pre-quantum line bundles. To associate the quantum state with the subset Λ of $M_1 \times M_2$, we use the map $\mathcal{R}_\Lambda$ that restricts holomorphic sections of the quantum line bundle over the product of the two Kähler manifolds to the subset (see Equation 4.33). At first, in Proposition 4.4.3, we present a description of the kernel of $\mathcal{R}_\Lambda$ when $\Lambda = \Lambda_1 \times \Lambda_2$ and one of Λ_1 or Λ_2 is a singleton set. This is, then, extended to any product subset Λ (see Proposition 4.4.6). With the help of these propositions, we present a description of the kernel of this restriction map when the subset is a finite union of products. This in turn shows that the quantum states associated with the finite union of products are separable. Finally, for every pure state and certain mixed state, we construct subsets of $M_1 \times M_2$ such that the states associated with these subsets are the original states, to begin with. The contributions of this section are summarized in Theorems 4.4.7, 4.4.10 and 4.4.11 and Corollary 4.4.9.

Chapter 5 contains the work of the paper [KSaikia+]. Similar to classical computers using circuits to manipulate the basic units of classical computations known as bits, quantum computers use quantum circuits to manipulate the basic units of quantum computation known as qudits. The counterpart of classical Boolean gates in quantum computing is quantum gates. Quantum gates are unitary operators on the quantum Hilbert space $(\mathbb{C}^d)^{\otimes n}$ of a system of n-qudits. The group $\mathcal{U}_{d^n}(\mathbb{C})$ of quantum gates is infinite, but for a practical quantum computer, we can make an architecture that can implement only implement finitely many quantum gates. The next best thing would be to find a finite set that can generate a group which is dense in $\mathcal{U}_{d^n}(\mathbb{C})$. The process of choosing such a finite set (known as a universal gate set) and decomposing a unitary as a word in this finite set is roughly what we mean by quantum circuit synthesis. In this chapter, we present two algorithms to make circuits corresponding to unitaries with elements in two different important number rings over the multi-qutrit Clifford+T gate set.

Section 5.1 is an introductory section to motivate the problem. Generally, the universal gate set is chosen on the basis of various factors, for instance, the ability to implement them physically in a fault-tolerant way and cost-effectively. A popular choice of universal gate set is the Clifford+T gate set. A few other proposed gate sets for the single-qutrit (3-level quantum system) case are Clifford+R and Clifford+$\mathcal{D}$. Cyclotomic number rings naturally appear for these gate sets and thus the problem of circuit synthesis involving these gates has an arithmetic flavour to it.

The exact synthesis algorithm for single-qubit (2-level quantum system) gates in $\mathcal{U}_2(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ over Clifford+T gate set was first shown in [KMM13] and later extended to the multi-qutrit case $\mathcal{U}_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ in [GS13]. For qutrits, there are already a few single-qutrit exact synthesis algorithms over Clifford+R, Clifford+$\mathcal{D}$ and Clifford+T [Boc+16; KVM23; EP24; Gla+22]. In this work, we extend to the multi-qutrit case and present an algorithm to exactly synthesize unitaries in $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ over the multi-qutrit Clifford+T (see Theorem 5.3.1). We further use the concept of Catalytic embedding to apply this algorithm to find an exact synthesis algorithm for unitaries in $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$.

We introduce the necessary concepts and fix notations in Section 5.2. We recall the definitions of a few important gate sets, some basic facts about the localized ring of cyclotomic integers $\mathbb{Z}[\frac{1}{p}, \zeta_{p^l}]$, definition of denominator exponents which plays a crucial role in the chapter. We also recall briefly the recently introduced concept of Catalytic embedding which plays a crucial role in the second main result of this chapter.

In Section 5.3, we prove the necessary lemmas and present the exact synthesis algorithm for unitaries in $\mathcal{U}_{3^{n+1}}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ (see Theorem 5.3.1). We follow the basic structure of the algorithm of [GS13]. The central idea behind the first step of decomposing a unitary in $\mathcal{U}_{3^{n+1}}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ hangs on dropping the smallest denominator exponent of a unit vector iteratively using appropriate 3-level unitaries (defined in Subsection 5.3.1) and converting the initial unit vector to one of the standard column vectors $|j\rangle$. In Subsection 5.3.2, we decompose these 3-level unitaries to controlled gates. We introduce the concept of extending the Gray code construction ([NC10, Section 4.5.2]) to the qutrit case. The final step is to implement these controlled gates over multi-qutrit Clifford+T using a borrowed ancilla [YW22; Gla+22].

In Section 5.4, we embed unitaries in $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ inside $\mathcal{U}_{3^{n+1}}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ using Catalytic embedding and apply Theorem 5.3.1 to prove Theorem 5.4.1. This result is a complete analogue of the main result of [GS13]. The contributions of this chapter are summarized in Theorems 5.3.1, 5.4.1 and Lemma 5.3.13.

Chapter 2

Quantum Information Theory

2.1 Introduction

Quantum mechanics is a mathematical framework to describe the behaviour of particles on a small scale and is built upon a few foundational postulates. A partial list of books to learn more about quantum mechanics and quantum information theory is [NC10; Wil13; BZ06]. Here, we shall briefly discuss the main three basic postulates of quantum mechanics: state-space, evolution and measurement postulates.

In quantum mechanics, the state space of a closed quantum system is modelled using a Hilbert space, called the Quantum Hilbert space $\mathcal{H}$ of the system. To describe the state of a system at any given moment, unit vectors in this Hilbert space are used. This postulate is also known as *State-space postulate*. The state space of a composite system is given by the tensor product of the state space of the individual systems. The evolution of a closed quantum system is described using a unitary operator acting on the quantum Hilbert space $\mathcal{H}$ of the system. This is known as the *evolution postulate*. The *measurement postulate* deals with when the closed system interacts with the environment. It roughly says that measurable quantities or observables are described using hermitian operators on $\mathcal{H}$. The state $|\psi\rangle$ being measured collapses to one of the eigenvectors of the hermitian operator with a probability that depends on $|\psi\rangle$ and the particular eigenvector.

Quantum Information Theory is a branch of quantum mechanics that deals with how information can be processed and communicated using quantum systems. Among various other things, the theory of entanglement is a major topic that it covers. In this thesis, especially in the contents of Chapter 4, we focus our interests on the analytic tools coming from entanglement. Section 2.4 introduces two of the most famous measures of entanglement, namely the entropy of entanglement and the entanglement of formation. Section 2.5 introduces another concept in quantum information known as distillation. Distillation roughly means the ability to extract entanglement from a quantum state. The main result of this chapter is Theorem 2.5.18.

2.2 Dirac Bra-ket Notations

Dirac bra-ket notation is a powerful, concise and flexible notation used in quantum mechanics to represent quantum states, operators etc. It elegantly combines vectors and dual vectors into a framework, simplifying many complex computations. Throughout this thesis, we shall use Dirac bra-ket notations wherever it seems appropriate and easy.

Let $\mathcal{H}$ be a Hilbert space. Then a vector in $\mathcal{H}$ is denoted by $|v\rangle$, and is called a *ket*. The inner product in $\mathcal{H}$ is denoted by $\langle\cdot|\cdot\rangle : \mathcal{H}\times\mathcal{H} \to \mathbb{C}$ which is linear in the second coordinate and anti-linear in the first coordinate (the opposite of the convention in the area of Pure mathematics). For $|v\rangle \in \mathcal{H}$, define the bounded linear functional $f : \mathcal{H} \to \mathbb{C}$ given by

$$f(|u\rangle) = \langle v|u\rangle .$$

Then the bounded linear functional f is denoted by $\langle v|$, and called a *bra*. This way $\langle v|$ is dual to $|v\rangle$.

For $|v\rangle , |u\rangle \in \mathcal{H}$, we have $T : \mathcal{H} \to \mathcal{H}$ given by

$$T(|w\rangle) = (\langle u|w\rangle) |v\rangle = |v\rangle \langle u|w\rangle .$$

Then the linear operator T is denoted by $|v\rangle \langle u|$. In particular, when $|v\rangle$ is a unit vector, the operator $|v\rangle \langle v|$ is nothing but the orthogonal projection onto the one-dimensional subspace spanned by $|v\rangle$. For $A \in \mathrm{End}(\mathcal{H})$, the action of A on a ket $|v\rangle$ is denoted by $A |v\rangle$. The notation $\langle u| A |v\rangle$ denotes the number in $\mathbb{C}$ that we get after applying the functional $\langle u|$ on the vector $A |v\rangle$.

When we have a tensor product $\mathcal{H}_1 \otimes ... \otimes \mathcal{H}_n$ of a finite number of Hilbert spaces, then $|v_1, ..., v_n\rangle$ or $|v_1...v_n\rangle$ or $|v_1\rangle ... |v_n\rangle$ are sometimes used to denote $|v_1\rangle \otimes ... \otimes |v_n\rangle$. Similarly $\langle v_1, ..., v_n|$ or $\langle v_1...v_n|$ or $\langle v_1| ... \langle v_n|$ are sometimes used to denote $\langle v_1| \otimes ... \otimes \langle v_n|$.

2.3 Quantum States

Suppose $\mathcal{H}$ denote a finite-dimensional complex Hilbert space that models a closed quantum system.

Definition 2.3.1 (Pure state)**.** A unit vector $|v\rangle \in \mathcal{H}$ is called a *pure state*.

However, for practical purposes due to various reasons, for instance, quantum decoherence with the environment, we don't always get a closed quantum system. When an external system $\mathcal{E}$ is also involved, to describe the state of a quantum particle we need vectors in the closed system $\mathcal{H} \otimes \mathcal{E}$. But when the information about an external system $\mathcal{E}$ is missing from the picture, we need a way to describe these states only using $\mathcal{H}$. The unit vectors in $\mathcal{H}$ are not enough to describe these states and we need operators on $\mathcal{H}$. These states are known as mixed states. By a quantum state (or simply a state), we always mean mixed states, not just pure states unless explicitly stated. Below, we formally define a quantum state.

Definition 2.3.2 (Quantum state or mixed state)**.** Let $\mathcal{H}$ be a complex Hilbert space of finite dimensions. A *quantum state or a mixed state* (or simply a *state*) ρ is a hermitian positive semidefinite operator in $\mathrm{End}(\mathcal{H})$ having trace 1.

Remark 2.3.3 (Pure state). The pure state $|v\rangle$ can be identified to the quantum state $|v\rangle\langle v|$ (the orthogonal projection onto the subspace spanned by $|v\rangle$). This way, we can view all pure states as mixed state as well.

By spectral theorem, we can eigen-decompose a state $\rho = \sum_j p_j \left|v_j\right\rangle\left\langle v_j\right|$ where $p_j \geq 0$ are eigenvalues of ρ and $\left|v_j\right\rangle$ are eigenvectors of ρ. The unit trace condition on ρ implies that $\sum_j p_j = 1$. From the eigen-decomposition, we see that every state can be written as a convex combination of pure states. Writing a state as a convex combination of pure states is called an *ensemble*. Therefore, a mixed state is an ensemble of pure states. Another interpretation of an ensemble is that a mixed state ρ is a statistical mixture of the pure states $\left|v_j\right\rangle\left\langle v_j\right|$ and the probability ρ being in the state $\left|v_j\right\rangle\left\langle v_j\right|$ is p_j. We need to be careful that, this ensemble decomposition of a mixed state into the constituent pure states is not unique.

Notation 2.3.4. *We denote the set of all pure states on the Hilbert space $\mathcal{H}$ by $\Omega_p(\mathcal{H})$ and the set of all mixed states is by $\Omega(\mathcal{H})$.*

Remark 2.3.5. Note that if $|v\rangle = e^{i\theta}|u\rangle$ for some $\theta \in \mathbb{R}$, then $|v\rangle\langle v| = |u\rangle\langle u|$ and therefore the pure states $|v\rangle$ and $|u\rangle$ are said to be *equivalent states*. In other words, quantum mechanics does not distinguish between the global phase. Therefore, the set of pure states is the set of equivalence classes of the action of $\mathbb{S}^1$ on the set of unit vectors in $\mathcal{H}$. This is topologically equivalent to the projective space $\mathbb{P}(\mathcal{H})$. When $\mathcal{H} = \mathbb{C}^2$, the set of pure states is the complex projective line $\mathbb{P}^1$, which is topologically equivalent to the 2-dimensional sphere. Using an appropriate identification, this sphere is called the Bloch sphere and has many applications in quantum information theory and quantum computing. As seen above, any mixed state of the quantum system modelled by $\mathcal{H}$ can be seen as a convex combination of pure states. Hence the set of quantum states $\Omega(\mathcal{H})$ can be seen as a convex set in the real vector space $\mathrm{Herm}(\mathcal{H})$ of all the hermitian operators on $\mathcal{H}$. Note that with the identification of a pure state $|v\rangle$ with the orthogonal projection $|v\rangle\langle v|$, we can view the set of pure states inside $\mathrm{Herm}(\mathcal{H})$. In this way, the pure states form the set of extreme points of $\Omega(\mathcal{H})$ [GKM05, Section 4].

2.4 Entanglement Measures

One of the most important features of quantum mechanics is entanglement. Entanglement is a very interesting phenomenon in quantum physics where two or more particles become correlated in such a way that the state of one particle is dependent on the state of the others. When two or more particles are entangled, they share a unified quantum state. It is impossible to describe the state of one of the particles without the help of the description of the other particles involved. In this thesis, we only concentrate on the theory of entanglement when two particles are involved. For that, we need two quantum systems A and B, corresponding to the two particles, represented by the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. When there is no entanglement between two particles and we know that the state of the particles can be described using pure states, then the pure state of the composite system is equal to the tensor product of the pure states for each individual subsystem. A non-entangled pure state can be represented as a product state, where the overall state of the system can be completely described by considering the states of its individual components independently. Throughout these sections $m = \dim(\mathcal{H}_A)$ and $n = \dim(\mathcal{H}_B)$ and without loss of generality we assume $1 \leq m \leq n$.

Definition 2.4.1 (Separable and entangled pure states)**.** A pure state in $\mathcal{H}_A \otimes \mathcal{H}_B$ is said to be *separable or non-entangled* if it can be written as $|u\rangle \otimes |v\rangle$ for some $|u\rangle \in \mathcal{H}_A$ and $|v\rangle \in \mathcal{H}_B$. Otherwise, it is said to be *entangled*.

Example 2.4.2. Let $\{|0\rangle, |1\rangle\}$ be the standard orthonormal basis of $\mathbb{C}^2$, i.e. $|0\rangle = (1,0)^t$ and $|1\rangle = (0,1)^t$. Then $|00\rangle = |0\rangle \otimes |0\rangle$ is a separable state. The following states, known as *Bell states*,

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$
$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle)$$
$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$$
$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$$

are examples of entangled states.

Notice that in the above definition of entangled states, we only covered the pure states. However, entanglement can be present in mixed states as well. As we described in Section 2.3, a mixed state can be described as a statistical mixture of pure states, we can extend the definition for pure states to mixed states as follows:

Definition 2.4.3 (Separable and entangled mixed states)**.** A mixed state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is said to be *separable or non-entangled* if there exists a convex decomposition $\rho = \sum_j p_j \left|v_j\right\rangle \left\langle v_j\right|$ (where $0 \leq p_j \leq 1$ with $\sum_j p_j = 1$) of ρ such that each of the pure states $\left|v_j\right\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ are separable. Otherwise, it is said to be *entangled*.

Example 2.4.4. Let ρ be a mixed state on $\mathbb{C}^2 \otimes \mathbb{C}^2$ defined by the following matrix in the standard orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$\rho = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Then $\rho = \frac{2}{3}\left(\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)\right)\left(\frac{1}{\sqrt{2}}(\langle 00| + \langle 01|)\right) + \frac{1}{3}|10\rangle\langle 10|$, i.e. it is a convex combination of the pure separable state $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ and $|10\rangle$. Therefore ρ is separable.

One of the central questions in Quantum information theory is to know the extent of entanglement of a state and the related question of the amount of quantum information stored in a state. There are various quantities that measure this. One of the most widely used measures for pure states is the entropy of entanglement and that for mixed states is the entanglement of formation.

2.4.1 Entropy of Entanglement

The von Neumann entropy of a quantum state σ on a quantum Hilbert space $\mathcal{H}$ is defined to be the quantity $-\sum_j \lambda_j \ln \lambda_j$, where λ_j's are the positive eigenvalues of σ. For a quantum state on $\mathcal{H}_A \otimes \mathcal{H}_B$, we look at the "part" of the state belonging to the individual sub-systems A and B known as the reduced states and compute von Neumann entropy of these reduced states to define the entropy of entanglement. These reduced states are defined using partial traces which are defined below.

Definition 2.4.5 (Partial traces)**.** *Partial trace* of an operator in $\mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$ over system B is defined to be a linear operator $\mathrm{Tr}_B : \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathrm{End}(\mathcal{H}_A)$ given by

$$\mathrm{Tr}_B(X \otimes Y) = \mathrm{Tr}(Y)X$$

and then extending by linearity where $X \in \mathrm{End}(\mathcal{H}_A)$ and $Y \in \mathrm{End}(\mathcal{H}_B)$. Similarly, we define partial trace over the system A, denoted by Tr_A.

Application of partial trace on a state again gives a hermitian positive semi-definite operator on the respective sub-system with trace 1, therefore they are quantum states on the respective sub-systems. The reduced state corresponding to a given sub-system is obtained by tracing out the other system using the partial trace operator.

Definition 2.4.6 (Reduced states)**.** For a state ρ, we call $\rho_A = \mathrm{Tr}_B(\rho)$ the *reduced state* of ρ corresponding to system A. Similarly, $\rho_B = \mathrm{Tr}_A(\rho)$ is called the reduced state of ρ corresponding to the system B.

Definition 2.4.7 (Entropy of entanglement)**.** For a pure state $|v\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, the *entropy of entanglement*, denoted by $E(|v\rangle)$, is defined to be

$$E(|v\rangle) = -\sum_{j=1}^{m} \lambda_j \ln\left(\lambda_j\right) \tag{2.1}$$

where $\lambda_1, ..., \lambda_m$ are eigenvalues of the reduced state $\mathrm{Tr}_B(|v\rangle\langle v|)$ with the convention that $0 \log 0 = 0$. That is the entropy of entanglement of a pure state is the von Neumann entropy of the reduced state corresponding to A.

Example 2.4.8. Take $|v\rangle = |u\rangle \otimes |w\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Then $\mathrm{Tr}_B(|v\rangle\langle v|) = \mathrm{Tr}_B(|u\rangle\langle u| \otimes |w\rangle\langle w|) = |u\rangle\langle u|$, i.e. eigenvalues of $\mathrm{Tr}_B(|v\rangle\langle v|)$ are $1, 0, ..., 0$, i.e. $E(|v\rangle) = 0$.

Example 2.4.9. Take $\mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^2 \otimes \mathbb{C}^2$ and $|v\rangle = \alpha_1 |0\rangle \otimes |0\rangle + \alpha_2 |1\rangle \otimes |1\rangle$ where $\{|0\rangle, |1\rangle\}$ is the standard basis of $\mathbb{C}^2$ and $\alpha_1, \alpha_2 \in \mathbb{C}$ with $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Then we have

$$|v\rangle\langle v| = \sum_{j=0}^{1} |\alpha_j|^2 |j\rangle\langle j| \otimes |j\rangle\langle j| \implies \mathrm{Tr}_B(|v\rangle\langle v|) = \sum_{j=1}^{2} |\alpha_j|^2 |j\rangle\langle j|.$$

Therefore, $E(|v\rangle) = -|\alpha_1|^2 \ln\left(|\alpha_1|^2\right) - |\alpha_2|^2 \ln\left(|\alpha_2|^2\right)$.

Theorem 2.4.10 (Schmidt Decomposition Theorem)**.** *For any $|v\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, there exist an orthonormal basis $\{|u_1\rangle, ..., |u_m\rangle\}$ of $\mathcal{H}_A$ and an orthonormal set $\{|f_1\rangle, ..., |f_m\rangle\}$ of $\mathcal{H}_B$ and $0 \le \alpha_1 \le \alpha_2 \le ... \le \alpha_m$ such that $|v\rangle = \sum_{j=1}^{m} \alpha_j \left|u_j\right\rangle \otimes \left|f_j\right\rangle$.*

Proof. We have a canonical isomorphism $T : \mathcal{H}_A \otimes \mathcal{H}_B \to M_{m\times n}(\mathbb{C})$ given by $|x\rangle \otimes |y\rangle \mapsto |x\rangle\langle y|$ and extending linearly. We apply Singular Value Decomposition on the matrix $T(|v\rangle)$ to get that there exists unitary matrices U of size $m \times m$, F of size $n \times n$ and a diagonal matrix $\Sigma = \mathrm{diag}\{\alpha_1, ..., \alpha_m\}$ of size $m \times m$ such that

$$T(|v\rangle) = U\begin{pmatrix}\Sigma & 0_{m,n-n}\end{pmatrix}F^*.$$

We write $F = [F_1 F_2]$ where F_1 is the matrix having first m columns of F and F_2 is the matrix having last $n - m$ columns to get that $T(|v\rangle) = U\Sigma F_1^*$. For $j, k \in \{1, ..., m\}$, we take $\left|u_j\right\rangle \in \mathcal{H}_A$ to be the j-th column of E and $|f_k\rangle \in \mathcal{H}_B$ to be the k-th column of $\overline{F_1}$ to get that

$$T(|v\rangle) = \sum_{j=1}^{m} \alpha_j \left|u_j\right\rangle \langle f_k| \implies v = \sum_{j=1}^{m} \alpha_j \left|u_j\right\rangle \otimes \left|f_j\right\rangle$$

where we note that α_j's being singular values are real non-negative and $\{|f_1\rangle, ..., |f_m\rangle\}$ being first m columns of the unitary matrix F is an orthonormal set. Finally, we order the α's in increasing order and rename the indices of $\left|u_j\right\rangle$'s and $\left|f_j\right\rangle$'s to get the required result. □

From the proof, it is evident that the Schmidt Decomposition Theorem is just a restatement of Singular Value Decomposition. The numbers α_j's are sometimes called the *Schmidt coefficients* of the vector $|v\rangle$.

Proposition 2.4.11. *Let $\rho = |v\rangle\langle v|$ be a pure state. Then the set of non-zero eigenvalues of $\rho_A = \mathrm{Tr}_B(\rho)$ and $\rho_B = \mathrm{Tr}_A(\rho)$ are equal (with the same multiplicity).*

Proof. Using Schmidt decomposition (Theorem 2.4.10), there exist an orthonormal basis $\{|u_1\rangle, ..., |u_m\rangle\}$ of $\mathcal{H}_A$ and an orthonormal set $\{|f_1\rangle, ..., |f_m\rangle\}$ of $\mathcal{H}_B$ and $0 \le \alpha_1 \le \alpha_2 \le ... \le \alpha_m$ such that

$$|v\rangle = \sum_{j=1}^{m} \alpha_j \left|u_j\right\rangle \otimes \left|f_j\right\rangle \implies \rho = \sum_{j=1}^{m} \alpha_j^2 \left|u_j\right\rangle \left\langle u_j\right| \otimes \left|f_j\right\rangle \left\langle f_j\right|.$$

Therefore,

$$\rho_A = \sum_{j=1}^{m} \alpha_j^2 \left|u_j\right\rangle \left\langle u_j\right|$$

$$\rho_B = \sum_{j=1}^{m} \alpha_j^2 \left|f_j\right\rangle \left\langle f_j\right|.$$

We see that the non-zero eigenvalues of both ρ_A and ρ_B are the non-zero elements of the set $\{\alpha_1^2, \alpha_2^2, ..., \alpha_m^2\}$. □

This shows that in the definition of entropy of entanglement, the appearance of Tr_B is not special and in fact we could have taken Tr_A to get the same value. In other words, the entropy of entanglement of a pure state is the von Neumann entropy corresponding to any one of the reduced states. Now, we shall see how we can use the Schmidt decomposition theorem to compute the entropy of entanglement easily.

Proposition 2.4.12. *Suppose $|v\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a pure state. Then*

$$E(|v\rangle) = -\sum_{j=1}^{m} \alpha_j^2 \ln\left(\alpha_j^2\right) \tag{2.2}$$

where $\{\alpha_1, ..., \alpha_m\}$ *are the Schmidt coefficients of* $|v\rangle$*.*

Proof. A direct consequence of the proof of Proposition 2.4.11. □

Proposition 2.4.13. *Suppose* $|v\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ *be a pure state and* $\theta \in \mathbb{R}$*. Then* $E(|v\rangle) = E(e^{i\theta}|v\rangle)$*.*

Proof. Suppose $|v\rangle = \sum_{j=1}^{m} \alpha_j \left|u_j\right\rangle \otimes \left|f_j\right\rangle$ be a Schmidt decomposition of $|v\rangle$. Therefore, $\{\left|u_j\right\rangle\}_{j=1}^{m}$ is an orthonormal basis for $\mathcal{H}_A$. Then $\{e^{i\theta}\left|u_j\right\rangle\}_{j=1}^{m}$ is also an orthonormal basis for $\mathcal{H}_A$, i.e. $\sum_{j=1}^{m} \alpha_j (e^{i\theta}\left|u_j\right\rangle) \otimes \left|f_j\right\rangle$ is a Schmidt decomposition of $e^{i\theta}|v\rangle$, i.e. Schmidt coefficients of $|v\rangle$ and $e^{i\theta}|v\rangle$ are the same. Hence $E(|v\rangle) = E(e^{i\theta}|v\rangle)$. □

Remark 2.4.14. By Remark 2.3.5, we have seen that two states are equivalent if they are multiple of each other by a complex number of absolute value 1. Now, from the above Proposition 2.4.13, we get that the entropy of entanglement is truly well-defined on pure states, that is, the entropy of entanglement is the same for two equivalent states.

Proposition 2.4.15. *The entanglement entropy is a continuous function on the set* $\Omega_p(\mathcal{H}_A \otimes \mathcal{H}_B)$*.*

Proof. We write the entanglement entropy function E as the composition $\Omega_p(\mathcal{H}_A \otimes \mathcal{H}_B) \xrightarrow{S} \mathbb{R}^m_{\geq 0} \xrightarrow{f} \mathbb{R}$, where S denotes the map of extracting Schmidt coefficients (in ascending order) and f denotes the multivariate function $\sigma = (\sigma_j) \mapsto -\sum_j \sigma_j^2 \ln \sigma_j^2$.

To obtain the Schmidt coefficients, we fix orthonormal bases $\{\left|e_j\right\rangle\}$ and $\{|f_k\rangle\}$ of $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. We write $|v\rangle = \sum_{j,k} \alpha^{(v)}_{jk} \left|e_j\right\rangle \otimes |f_k\rangle$ and define $T(|v\rangle) = (\alpha^{(v)}_{kj})$. When $|v\rangle$ and $|u\rangle$ are close in $\Omega_p(\mathcal{H}_A \otimes \mathcal{H}_B)$, then the coefficients $\alpha^{(v)}_{jk}$ and $\alpha^{(u)}_{jk}$ are close and so $T(|v\rangle)$ and $T(|u\rangle)$ are close, i.e. $T : \Omega_p(\mathcal{H}_A \otimes \mathcal{H}_B) \to M_{n,m}(\mathbb{C})$ is continuous. The Schmidt coefficients of $|v\rangle$ are nothing but eigenvalues of $\sqrt{T(|v\rangle)^* T(|v\rangle)}$. The map $M_{n,m}(\mathbb{C}) \to \mathrm{HP}(\mathbb{C}^m)$, where $\mathrm{HP}(\mathbb{C}^m)$ is the set of hermitian positive semi-definite operators on $\mathbb{C}^m$, given by $X \mapsto \sqrt{X^*X}$ is continuous and extracting eigenvalues from an element of $\mathrm{HP}(\mathbb{C}^m)$ (in ascending order) is also continuous (because of the continuity of the zeroes of a polynomial and the continuity of characteristic polynomial), hence $S : \Omega_p(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathbb{R}^m$ is continuous.

For continuity of f, it is enough to show that for each $j \in \{1, 2, ..., m\}$ the map $f_j(\sigma) = -\sigma_j^2 \ln \sigma_j^2$ (with $0 \ln 0 = 0$) is continuous. As the map f_j is independent of σ_k if $k \neq j$, it is enough to show that the map $g : \mathbb{R}_{\geq 0} \to \mathbb{R}$ given by $x \mapsto x^2 \ln x^2$ when $x \neq 0$ and $0 \mapsto 0$ is continuous. Clearly, g is continuous when $x \neq 0$. Now,

$$\lim_{x \to 0^+} g(x) = \lim_{x \to 0^+} x^2 \ln x^2 = 2 \lim_{x \to 0^+} \frac{\ln x}{\frac{1}{x^2}} = 2 \lim_{x \to 0^+} \frac{\frac{1}{x}}{\frac{-2}{x^3}} = -\lim_{x \to 0^+} x^2 = 0 = g(0).$$

Therefore g is continuous. Hence the entanglement entropy is a continuous function. □

Proposition 2.4.16. *Let $|v\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a pure state. Then $|v\rangle$ is separable if and only if $E(|v\rangle) = 0$.*

Proof. We see that $|v\rangle$ is separable if and only if the Schmidt coefficients of $|v\rangle$ are $1, 0, ..., 0$ if and only if $E(|v\rangle) = 0$. □

The value of $E(|v\rangle)$ lies in the interval $[0, \ln m]$ with $E(|v\rangle) = 0$ if and only if $|v\rangle$ is separable if and only if $|v\rangle\langle v| \in \mathrm{End}(\mathcal{H}_A) \otimes \mathrm{End}(\mathcal{H}_B)$ is decomposable, in this case we call the pure state v is *non-entangled*. The maximum value $\ln m$ is attained when the eigenvalues of $\mathrm{Tr}_B(|v\rangle\langle v|)$ are equal, i.e. $\lambda_1 = ... = \lambda_m = \frac{1}{m}$. In a way, entanglement entropy $E(|v\rangle)$ characterizes "how much non-decomposable" the vector $|v\rangle$ by measuring how close the eigenvalues of $\mathrm{Tr}_B(|v\rangle\langle v|)$ are to being equidistributed with the entropy being maximal if and only if the eigenvalues are equidistributed.

2.4.2 Entanglement of Formation

In Section 2.4.1, we have seen a measure of entanglement for pure states. We need a similar measure for the entanglement of mixed states. As mixed states are sums of pure states, so we want to extend the entropy of entanglement to mixed states. But we can write a mixed state ρ as an ensemble of pure states in a lot of different ways, so simply summing the entropy of entanglement for the constitute pure states is not enough. For illustration, consider the state

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

which is also equal to the convex combination

$$\rho = \frac{1}{2}\left[\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right)\right] + \frac{1}{2}\left[\left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| - \langle 11|}{\sqrt{2}}\right)\right].$$

As $|00\rangle$ and $|11\rangle$ are separable, summing over the entropy of entanglement in the first ensemble will produce 0. However, $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$ being the Bell states (see Example 2.4.2) have entropy of entanglement $\ln(2)$, so the second ensemble will produce $\ln(2)$. This is why we take infimum over all such possible ensembles.

Definition 2.4.17 (Entanglement of formation)**.** [Ben+96b] For a mixed state ρ, *entanglement of formation* $\tilde{E}(\rho)$ is given by

$$\tilde{E}(\rho) = \inf \sum_j p_j E(|v_j\rangle)$$

where $\rho = \sum_j p_j |v_j\rangle\langle v_j|$ with the summation done over a finite index set and $p_j > 0$ with $\sum_j p_j = 1$. The infimum is taken over all such possible finite sums.

A minimum can replace the infimum in the definition. The rest of this section is proof of this fact inspired by [Uhl10]. For this purpose, let us first define a few concepts related to convex roof construction.

Let Ω be a compact convex set in $\mathbb{R}^n$ and Ω_p be the set of extremal points of the convex set Ω (points in Ω_p are also called "pure" points).

Definition 2.4.18 (Roof points)**.** For a real valued function G on a compact convex set Ω, a point $w \in \Omega$ is called a *roof point* of G if there exist an extremal convex decomposition $w = \sum_j p_j v_j$ (i.e. $p_j \in \mathbb{R}$, $p_j \geq 0$, $\sum_j p_j = 1$ and $v_j \in \Omega_p$) such that $G(w) = \sum p_j G(v_j)$. Such a decomposition is called optimal with respect to G or equivalently G-optimal.

Definition 2.4.19 (Roofs and Roof extensions)**.** A real function G on Ω is called a *roof* if every point on Ω is a roof point of G. If g is a real-valued function on Ω_p, a roof G is called a *roof extension of* g if $G(w) = g(w)$ for all $w \in \Omega_p$.

Some examples of roofs and roof extensions can be found in [Uhl10].

Definition 2.4.20 (Convex roof extension)**.** A real valued function G on Ω is called a *convex extension* of $g : \Omega_p \to \mathbb{R}$, if $G(w) = g(w)$ for all $w \in \Omega_p$ and G is a convex function, i.e. $G(tw_1 + (1-t)w_2) \leq tG(w_1) + (1-t)G(w_2)$ for all $t \in [0,1]$ and $w_1, w_2 \in \Omega$. A convex extension that is also a roof is called a *convex roof extension*.

Proposition 2.4.21. *For a real-valued function g on Ω_p, the extension $g^\cup : \Omega \to \mathbb{R}$ defined by*

$$g^\cup(w) = \inf \sum_j p_j g(v_j)$$

where infimum is taken over all convex combinations of $w = \sum_j p_j v_j$ with $v_j \in \Omega_p$, is the largest convex extension of g. Further, if a convex roof extension of g exists, then it is unique and is equal to $g^\cup$.

Proof. Let $w_1, w_2 \in \Omega$. Let $w_1 = \sum_j p_j v_j$ and $w_2 = \sum_k q_k u_k$ be arbitrary convex combination of w_1 and w_2 in terms of elements from Ω_p, i.e. $v_j, u_k \in \Omega_p$ and $\sum_j p_j = 1 = \sum_k q_k$. Now,

$$\begin{aligned}
&g^\cup(tw_1 + (1-t)w_2) \\
=&g^\cup(t\sum_j p_j v_j + (1-t)\sum_k q_k u_k) \\
\leq&\sum_j tp_j g(v_j) + \sum_k (1-t) q_k g(u_k) \text{ (by definition of } g^\cup \text{ as } \textstyle\sum_j tp_j + \sum_k (1-t)q_k = 1)
\end{aligned}$$

As the convex combination we took were arbitrary, so taking infimum, we get

$$g^\cup(tw_1 + (1-t)w_2) \leq t \inf\left\{\sum_j p_j g(v_j)\right\} + (1-t)\inf\left\{\sum_k q_k g(u_k)\right\} = tg^\cup(w_1) + (1-t)g^\cup(w_2).$$

We see that $g^\cup$ is a convex extension of g. It is the largest convex extension possible because if G is any other convex extension of g, then $G(w) \leq \sum_j p_j g(v_j)$ for every convex combination, yielding $G(w) \leq \inf \sum_j p_j g(v_j) = g^\cup(w)$.

Now, suppose there exists a convex roof extension G of g. Then any point $w \in \Omega$ is a roof point for the convex extension G of g. So, there exists an optimal convex combination $w = \sum_k q_k u_k$ such that $G(w) = \sum_k q_k g(u_k) \geq \inf_{\{\sum_j p_j v_j | w = \sum_j p_j v_j\}} \sum_j p_j g(v_j) = g^\cup(w)$. Also by convexity of G, we have $G \leq g^\cup$ (from the previous paragraph). Therefore, $G = g^\cup$, i.e. if a convex roof extension of g exists then it is unique and is equal to $g^\cup$. □

Corollary 2.4.22. *The entanglement of formation is a convex function on $\Omega(\mathcal{H}_A \otimes \mathcal{H}_B) \subset$ Herm(QH).*

Proof. Observe that the entanglement of formation $\tilde{E}$ is equal to $E^\cup$. Therefore, the statement follows from the first part of Proposition 2.4.21 □

There is a sufficient condition that guarantees that $g^\cup$ is a roof. The proof of the following proposition can be found in [Uhl10].

Proposition 2.4.23. *Let Ω be a convex set and both Ω and Ω_p be compact. Let g be a continuous map on Ω_p. Then the extension $g^\cup$ is a roof.*

Proposition 2.4.24. *The function entanglement of formation is the convex roof extension of the entropy of entanglement. In other words, for a mixed state ρ, entanglement of formation $\tilde{E}(\rho)$ is given by*

$$\tilde{E}(\rho) = \min \sum_j p_j E(\left|v_j\right\rangle)$$

where $\rho = \sum_j p_j \left|v_j\right\rangle \left\langle v_j\right|$ with the summation done over a finite index set and $p_j > 0$ with $\sum_j p_j = 1$. The minimum is taken over all such possible finite sums.

Proof. We have $\Omega(\mathcal{H}_A \otimes \mathcal{H}_B) = \mathrm{Tr}^{-1}(\{1\})$, where tr : Herm$(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathbb{C}$ is the trace map which is continuous, so $\Omega(\mathcal{H}_A \otimes \mathcal{H}_B)$ is closed. The 2-norm of a linear operator ρ is equal to the maximum singular value of ρ (in other words, the maximum eigenvalue of $\rho^*\rho$). For a quantum state ρ, the eigenvalues are non-negative and sum to 1, so each one of the eigenvalues is less than or equal to 1. Therefore eigenvalues of ρ^2 are less than or equal to 1. But we have $\rho^*\rho = \rho^2$ (as $\rho^* = \rho$), so the eigenvalues of $\rho^*\rho$ are bounded above by 1, i.e. the 2-norm of ρ is bounded above by 1. Therefore $\Omega(\mathcal{H}_A \otimes \mathcal{H}_B)$ is bounded in the Euclidean space Herm$(\mathcal{H}_A \otimes \mathcal{H}_B)$. Hence $\Omega(\mathcal{H}_A \otimes \mathcal{H}_B)$ is compact. The set of pure states $\Omega_p(\mathcal{H}_A \otimes \mathcal{H}_B)$ as a subset of Herm$(\mathcal{H})$, being the homeomorphic image of the projective space $\mathbb{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$, is also compact. By Proposition 2.4.15 is continuous on the set of pure states, so the entanglement of formation is a roof extension of the entanglement entropy (by Proposition 2.4.23). Hence, the infimum is in fact a minimum. □

As we have seen in Section 2.4.1 entanglement entropy can distinguish between separable pure states and entangled pure states. The analogous statement is true for the entanglement of formation with mixed states.

Proposition 2.4.25. *Let ρ be a mixed state in $\mathcal{H}_A \otimes \mathcal{H}_B$. The state ρ is separable if and only if $\tilde{E}(\rho) = 0$.*

Proof. Let ρ be separable. Then there exists a decomposition $\rho = \sum_j p_j \left|v_j\right\rangle \left\langle v_j\right|$ of ρ such that each of $\left|v_j\right\rangle$ are separable pure states, therefore we see that $\sum_j p_j E(\left|v_j\right\rangle) = 0$ and so we have $\tilde{E}(\rho) = 0$. Conversely, let $\tilde{E}(\rho) = 0$. The minimum is attained at some decomposition by Proposition 2.4.24. As the minimum is 0, the decomposition where the minimum is attained must consist of all separable, i.e. ρ is separable. □

2.5 Distillation of Quantum States

In this section, we shall discuss a few concepts related to the distillability of quantum states, a summary of the advances made towards partial solutions to the NPT distillabilty problem and a result relating operator Schmidt rank and distillabilty. The principal result in this section is Theorem 2.5.18.

In a broad sense, the distillability of a quantum state implies the capacity to extract a maximally entangled state from a substantial number of copies of that state using local operations and classical communications (LOCC). LOCC are a class of maps characterized by [NC10, Theorem 12.5]. An alternative definition of distillability can be made using a well-known fact that all 2×2 entangled states can be distilled using the so-called recurrence and hashing protocols [Ben+96a]. Due to this, we can get a simplified definition to capture the distillability of a quantum state ρ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim(\mathcal{H}_A)$, $\dim(\mathcal{H}_B) \geq 2$ by equivalently asking the question of the ability to convert $\rho^{\otimes n}$ to a 2×2 entangled state using projectors as local operations.

2.5.1 Peres-Horodecki Criterion

In Section 2.4, we mentioned that given a quantum state, it is difficult to decide whether the state is entangled. Using partial transpose of the quantum state, there is a one-sided criterion, known as the Peres-Horodecki criterion, to decide if a state is entangled.

Definition 2.5.1 (Partial transpose)**.** The *Partial transpose* (with respect to the system B) is a linear map $\mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$ defined by setting

$$(X \otimes Y)^{T_B} = X \otimes Y^T$$

and then extending by linearity, where $X \in \mathrm{End}(\mathcal{H}_A)$ and $Y \in \mathrm{End}(\mathcal{H}_B)$. We denote ρ^{T_B} to mean partial transpose of ρ with respect to the system B. Similarly, we can define the partial transpose of ρ with respect to the system A by using the transpose on X instead of Y in the above equation, denoted by ρ^{T_A}. For $\rho \in \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$, $\{u_i\}$ an orthonormal basis of $\mathcal{H}_A$ and $\{f_j\}$ an orthonormal basis of $\mathcal{H}_B$, we can write

$$\rho = \sum_{i,j=1}^{M} \sum_{k,l=1}^{N} \rho_{i,j,k,l} |u_i\rangle\langle u_j| \otimes |f_k\rangle\langle f_l| \text{ for some constants } \rho_{i,j,k,l}.$$

Then

$$\rho^{T_A} = \sum_{i,j=1}^{M} \sum_{k,l=1}^{N} \rho_{i,j,k,l} |u_j\rangle\langle u_i| \otimes |f_k\rangle\langle f_l|$$

and

$$\rho^{T_B} = \sum_{i,j=1}^{M} \sum_{k,l=1}^{N} \rho_{i,j,k,l} |u_i\rangle\langle u_j| \otimes |f_l\rangle\langle f_k|.$$

Proposition 2.5.2. *For a state $\rho \in End(\mathcal{H}_A \otimes \mathcal{H}_B)$, we have equality $\rho^{T_A} = (\rho^{T_B})^T$ so that ρ^{T_A} and $(\rho^{T_B})^T$ are simultaneously positive semi-definite or non-positive semi-definite.*

Proof. It is enough to show for operators of the form $\rho = X \otimes Y$. Then $\rho^{T_A} = X^T \otimes Y = (X \otimes Y^T)^T = (\rho^{T_B})^T$. Also for $|v\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $\sigma \in \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$, we have $\langle v|\sigma|v\rangle = \langle v^*|\sigma^T|v^*\rangle$, so the result follows. □

Definition 2.5.3 (PPT and NPT state)**.** A quantum state ρ is called *Positive Partial Transposition* or in short, *PPT* if ρ^{T_B} (or ρ^{T_A}) is a positive semi-definite. It is called *Non-positive Partial Transposition* or in short, *NPT* if it is not PPT.

Theorem 2.5.4 (Peres-Horodecki criterion [Per96; HHH96])**.** *Let ρ be a mixed state in $\mathcal{H}_A \otimes \mathcal{H}_B$. If ρ is NPT, then ρ is entangled. Further when $mn \leq 6$ (where $m = dim(\mathcal{H}_A)$ and $n = dim(\mathcal{H}_B)$), then the converse is also true.*

Example 2.5.5. Let $\rho_1, \rho_2 \in$ be two mixed states on $\mathbb{C}^2 \otimes \mathbb{C}^2$ defined by the following matrices in the standard orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$\rho_1 = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \rho_2 = \begin{pmatrix} 1/4 & 0 & 0 & 1/4 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/4 & 0 & 0 & 1/4 \end{pmatrix}$$

Then,

$$\rho_1^{T_B} = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \rho_2^{T_B} = \begin{pmatrix} 1/4 & 0 & 0 & 0 \\ 0 & 1/2 & 1/4 & 0 \\ 0 & 1/4 & 0 & 0 \\ 0 & 0 & 0 & 1/4 \end{pmatrix}$$

We see that $\rho_1^{T_B}$ is positive semi-definite and $\rho_2^{T_B}$ is not (one of the eigenvalues is negative), i.e. ρ_1 is PPT and ρ_2 is NPT. Since the size of ρ_1 is 4 which is less than 6, so converse of the Peres-Horodecki criterion is applicable. We see that ρ_1 is separable. The state ρ_2 being NPT is entangled.

2.5.2 The NPT distillability problem

Definition 2.5.6 (1-distillable state)**.** [Dür+00] A quantum state ρ is said to be *1-distillable* if there exists a pure state $|\psi\rangle$ of Schmidt rank at most 2 in $\mathcal{H}_A \otimes \mathcal{H}_B$ (where Schmidt rank at most 2 means that at most two Schmidt coefficients can be non-zero, i.e. $|\psi\rangle = a\,|e_1, f_1\rangle + b\,|e_2, f_2\rangle$ for some $a, b \geq 0$, $\{|e_1\rangle, |e_2\rangle\}$ are orthonormal vectors in $\mathcal{H}_A$ and $\{|f_1\rangle, |f_2\rangle\}$ are orthonormal vectors in $\mathcal{H}_B$) such that $\langle\psi|\rho^{T_B}|\psi\rangle < 0$.

Definition 2.5.7 (Distillable state)**.** A quantum state ρ is said to be *n-distillable* if the state $\rho^{\otimes n}$ on the quantum Hilbert space $(\mathcal{H}_A^{\otimes n}) \otimes (\mathcal{H}_B^{\otimes n})$ is a 1-distillable state. A quantum state is called *distillable* if it is n-distillable for some $n \in \mathbb{N}$.

Proposition 2.5.8. *A state is distillable if and only if for some $n \in \mathbb{N}$ there exists 2-dimensional projectors P and Q acting on $\mathcal{H}_A^{\otimes n}$ and $\mathcal{H}_B^{\otimes n}$ such that the state $(P \otimes Q)\rho^{\otimes n}(P \otimes Q)^\dagger$ is an NPT state.*

Proposition 2.5.9. *A PPT state is not distillable.*

Proof. A proof can be found here [HHH98]. □

The proposition above indicates that all distillable states must be NPT. However, an open question remains regarding whether the converse is true [HRŽ20].

Definition 2.5.10. States that are entangled but not distillable are called *bound entangled (BE)* states.

As in higher dimensions, there exist some PPT states that are entangled, so we know the existence of PPT BE states, but it's unclear whether NPT BE states exist. Over the years, several advances were made and we have an abundance of partial results based on different criteria such as rank, operator Schmidt rank, matrix rank of the states etc. We list a few known results and works towards this problem below.

1. All NPT states in $\mathcal{H}_A \otimes \mathcal{H}_B$ where $\dim(\mathcal{H}_A)= 2$ and $\dim(\mathcal{H}_B) = n$ for some $n \geq 2$ are distillable, in fact they are 1-distillable [Dür+00]. The proof that uses LOCC operators is a difficult one. However, using Definition 2.5.7, it is easy to see this. If ρ is NPT, then there exists $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that $\langle\psi|\rho|\psi\rangle < 0$. Since $\dim(\mathcal{H}_A) = 2$, the Schmidt decomposition of $|\psi\rangle$ has at max 2 terms and we are done.

2. If $\mathrm{rank}(\rho) < \max(\mathrm{rank}(\rho_A), \mathrm{rank}(\rho_B))$, then ρ is distillable [Hor+03]. A useful corollary of this is that a rank n undistillable state has support in at most $n \times n$ subspace. Using this, it is shown that rank 2 NPT states are distillable [Hor+03].

3. Any rank 3 NPT states are distillable [CC08].

4. Any rank 4 NPT states are distillable [CD16]. In [CD16], the authors also constructed a one-parameter family of 3×3 NPT state that is not 1-distillable (which could potentially be n-undistillable).

5. In [CD23], the authors proved various results related to distillability in terms of Schmidt rank and matrix rank.

6. It is shown that any state can be converted to Werner state (a useful one-parameter family of states) [Dür+00; Wer89], so search for undistillable NPT state can be equivalently made in these states only. In [Dok16], the authors showed 2-undistillablity of certain Werner states and mentioned known results based on the parameter.

There is also an equivalent formulation of this problem in the language of C^*-algebras [DiV+00; Cla05]. The search for an NPT-bound entangled state will be over if one finds a map with the property described in Proposition 2.5.14 below:

Definition 2.5.11. A linear map $\Lambda : M_d(\mathbb{C}) \to M_d(\mathbb{C})$, where $M_d(\mathbb{C})$ denotes the set of all matrices of size $d \times d$, is called a *positive map* if $\Lambda(A)$ is positive semi-definite for all $A \in M_d(\mathbb{C})$ that are positive semi-definite.

Definition 2.5.12 (k-positive maps)**.** For $k \in \mathbb{N}$, a linear map $\Lambda : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ is called *k-positive* if and only if $I_k \otimes \Lambda : M_k(\mathbb{C}) \otimes M_d(\mathbb{C}) \to M_k(\mathbb{C}) \otimes M_d(\mathbb{C})$ is a positive map, where $I_k : M_k(\mathbb{C}) \to M_k(\mathbb{C})$ is the identity map. We call Λ *completely positive* if it is k-positive for each $k \in \mathbb{N}$.

Definition 2.5.13 (k-co-positive)**.** A map $\Lambda : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ is called *k-co-positive* if and only if the composition $T \circ \Lambda$ is k-positive, where T is the transposition map. We call Λ *completely co-positive* if it is k-co-positive for all $k \in \mathbb{N}$.

Proposition 2.5.14. *If there exists a positive map Λ that is completely co-positive but not completely positive such that $\Lambda^{\otimes n}$ is 2-positive for each $n \in \mathbb{N}$, then there exist NPT bound entangled states that can be constructed explicitly with the help of the map.*

2.5.3 Some non-distillable states

In this section, we shall construct a family of non-distillable states. In addition to that, we shall see that any quantum state ρ in $\mathcal{H}_A \otimes \mathcal{H}_B$ can be identified with a state $\tilde{\rho}$ inside a suitable Hilbert space $\mathcal{H}'_A \otimes \mathcal{H}'_B \subset \mathcal{H}_A \otimes \mathcal{H}_B$ such that the reduced states $\tilde{\rho}_A$ and $\tilde{\rho}_B$ are invertible.

Lemma 2.5.15. *Let* $\rho = \left[\begin{array}{c|c} A & C^\dagger \\ \hline C & 0 \end{array}\right]$ *(where A is a square matrix) be positive semi-definite, then* $C = 0$.

Proof. There exists $B = \left[\begin{array}{c|c} B_1 & B_2 \\ \hline B_3 & B_4 \end{array}\right]$ such that $\rho = \left[\begin{array}{c|c} B_1^\dagger B_1 + B_3^\dagger B_3 & B_1^\dagger B_2 + B_3^\dagger B_4 \\ \hline B_2^\dagger B_1 + B_4^\dagger B_3 & B_2^\dagger B_2 + B_4^\dagger B_4 \end{array}\right]$, so $B_2^\dagger B_2 + B_4^\dagger B_4 = 0$, i.e. $\mathrm{tr}\left(B_2^\dagger B_2 + B_4^\dagger B_4\right) = 0$. But $\mathrm{tr}\left(B_2^\dagger B_2\right), \mathrm{tr}\left(B_4^\dagger B_4\right) \geq 0$, so $\mathrm{tr}\left(B_2^\dagger B_2\right) = 0 = \mathrm{tr}\left(B_4^\dagger B_4\right)$. As $B_2^\dagger B_2$ and $B_4^\dagger B_4$ are positive semi-definite with trace 0, so $B_2 = 0$ and $B_4 = 0$. Therefore, $C = 0$. □

Proposition 2.5.16. *Let* $\rho \in End(\mathcal{H}_A \otimes \mathcal{H}_B)$ *(where* $dim\mathcal{H}_A = M$ *and* $dim\mathcal{H}_B = N$*) be a quantum state such that* $rank(\rho_A) = m$ *and* $rank(\rho_B) = n$*. Then there exist subspaces* $\mathcal{H}'_A$ *and* $\mathcal{H}'_B$ *of* $\mathcal{H}_A$ *and* $\mathcal{H}_B$ *respectively of respective dimensions m and n such that if* $\tilde{\rho} : \mathcal{H}'_A \otimes \mathcal{H}'_B \to \mathcal{H}'_A \otimes \mathcal{H}'_B$ *given by*

$$\tilde{\rho} = \rho|_{\mathcal{H}'_A \otimes \mathcal{H}'_B},$$

then $\rho = \tilde{\rho} \oplus 0$ *(i.e.* ρ *can be thought of as a quantum state in* $End(\mathcal{H}'_A \otimes \mathcal{H}'_B) \cong End(\mathbb{C}^m \otimes \mathbb{C}^n)$*. In other words, every bipartite state* ρ *can be realized inside suitable Hilbert space such that* ρ_A *and* ρ_B *are invertible).*

Proof. We can write $\rho = \rho_A \otimes \rho_B + \sum_{j=1}^k A_j \otimes B_j$ for a linearly independent set of hermitian operators $\{A_j : j = 1, ..., k\} \subset \mathrm{End}(\mathcal{H}_A)$ and a linearly independent set of hermitian operators $\{B_j : j = 1, ..., k\} \subset \mathrm{End}(\mathcal{H}_B)$. Using the definition of partial traces we get that $\sum_{j=1}^k \mathrm{tr}\left(B_j\right) A_j = 0 = \sum_{j=1}^k \mathrm{tr}\left(A_j\right) B_j$ which implies that for each $j \in \{1, ..., k\}$ we have $\mathrm{tr}\left(A_j\right) = 0 = \mathrm{tr}\left(B_j\right)$. Let $\mathcal{H}'_A = \ker(\rho_A)^\perp$ and $\mathcal{H}'_B = \ker(\rho_B)^\perp$ and let $\beta' = \{|u_1\rangle, ..., |u_m\rangle\}$ and $\gamma' = \{|v_1\rangle, ..., |v_n\rangle\}$ be (ordered) orthonormal bases of $\mathcal{H}'_A$ and $\mathcal{H}'_B$ respectively and let $\alpha' = \beta' \otimes \gamma'$. We extend the orthonormal sets β' and γ' to (ordered) orthonormal bases $\beta = \{|u_1\rangle, ..., |u_M\rangle\}$ and $\gamma = \{|v_1\rangle, ..., |v_N\rangle\}$ of $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. For each $j \in \{1, ..., k\}$, we write the matrix of A_j and B_j with respect to the bases β and γ respectively to get the block matrices $A_j = \left[\begin{array}{c|c} A_j^{(1)} & (A_j^{(2)})^\dagger \\ \hline A_j^{(2)} & A_j^{(3)} \end{array}\right]$ and $B_j = \left[\begin{array}{c|c} B_j^{(1)} & (B_j^{(2)})^\dagger \\ \hline B_j^{(2)} & B_j^{(3)} \end{array}\right]$ where $A_j^{(1)}$ is an $m \times m$ matrix and $B_j^{(1)}$ is an $n \times n$ matrix .

We write the matrices of $\rho_A \otimes \rho_B$ and $\sum_{j=1}^k A_j \otimes B_j$ in the basis $\alpha = \beta \otimes \gamma$ (with the ordering that makes it compatible with the tensor product of the block matrices $A_j \otimes B_j$) to get that

$$[\rho]_\alpha = \left[\begin{array}{cc|c} [\rho_A \otimes \rho_B]_{\alpha'} + \sum_{j=1}^k A_j^{(1)} \otimes B_j^{(1)} & \sum_{j=1}^k A_j^{(1)} \otimes (B_j^{(2)})^\dagger & \\ \sum_{j=1}^k A_j^{(1)} \otimes B_j^{(2)} & \sum_{j=1}^k A_j^{(1)} \otimes B_j^{(3)} & C^\dagger \\ \hline \multicolumn{2}{c|}{C} & D \end{array}\right]$$

where $C = \sum_{j=1}^k A_j^{(2)} \otimes B_j$ and $D = \sum_{j=1}^k A_j^{(3)} \otimes B_j$. Note that $\mathrm{tr}(D) = \sum_{j=1}^k \mathrm{tr}\left(A_j^{(3)}\right)\mathrm{tr}\left(B_j\right) = 0$. Also, D being a principal sub-matrix of a positive semi-definite matrix ρ is itself positive semi-definite. Therefore, $D = 0$. As ρ is positive semi-definite and $D = 0$, using Lemma 2.5.15 we must have $C = 0$. Therefore,

$$[\rho]_\alpha = \left[\begin{array}{c|c} [\rho_A \otimes \rho_B]_{\alpha'} + \sum_{j=1}^k A_j^{(1)} \otimes B_j^{(1)} & (\sum_{j=1}^k A_j^{(1)} \otimes (B_j^{(2)})^\dagger) \oplus 0 \\ \hline (\sum_{j=1}^k A_j^{(1)} \otimes B_j^{(2)}) \oplus 0 & (\sum_{j=1}^k A_j^{(1)} \otimes B_j^{(3)}) \oplus 0 \end{array}\right]$$

Further $D = 0$ implies that $\sum_{j=1}^k A_j^{(3)} \otimes B_j^{(1)} = 0$, so $\mathrm{tr}\left(\sum_{j=1}^k A_j^{(1)} \otimes B_j^{(3)}\right) = -\mathrm{tr}\left(\sum_{j=1}^k A_j^{(3)} \otimes B_j^{(3)}\right) = \mathrm{tr}\left(\sum_{j=1}^k A_j^{(3)} \otimes B_j^{(1)}\right) = 0$. Again $\sum_{j=1}^k A_j^{(1)} \otimes B_j^{(3)} \oplus 0$ being a principal sub-matrix of a positive semi-definite matrix is positive semi-definite having trace 0, so it must be zero. Finally, as ρ is positive semi-definite, so using Lemma 2.5.15 we must have $\sum_{j=1}^k A_j^{(1)} \otimes B_j^{(2)} = 0$. Therefore, we see that $\rho = \rho|_{\mathcal{H}'_A \otimes \mathcal{H}'_B} \oplus 0$. □

Definition 2.5.17. For an operator $\rho \in \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$, the *Operator Schmidt rank* of ρ is defined to be the minimum integer k such that we can decompose $\rho = \sum_{j=1}^k A_j \otimes B_j$ for some $A_j \in \mathrm{End}(\mathcal{H}_A)$ and $B_j \in \mathrm{End}(\mathcal{H}_B)$, denoted by $osr(\rho)$. A decomposition $\rho = \sum_{j=1}^k A_j \otimes B_j$ is called a *operator Schmidt decomposition* if $k = osr(\rho)$. For any two operator Schmidt decompositions $\sum_{j=1}^{osr(\rho)} A_j \otimes B_j = \rho = \sum_{j=1}^{osr(\rho)} A'_j \otimes B'_j$, we have $\mathrm{span}\{A_j : j = 1, ..., osr(\rho)\} = \mathrm{span}\{A'_j : j = 1, ..., osr(\rho)\}$ (similar statement for the Bs) and we call this linear space as the *space* $\mathcal{A}$ of ρ (similarly *space* $\mathcal{B}$).

Theorem 2.5.18. *Let ρ be a state with rank$(\rho_A) = M$ and rank$(\rho_B) = N$ and operator Schmidt rank k such that the space $\mathcal{A}$ (or alternately space $\mathcal{B}$) of ρ has exactly $k-1$ rank one hermitian operators that are mutually orthogonal with respect to the Frobenius inner product, then $k \leq M$ (alternately $k \leq N$) and ρ is PPT and so is not distillable.*

Proof. The case $k = 1$ is trivially true as in that case $\rho = \rho_A \otimes \rho_B$. We shall now prove for $k \geq 2$. By Proposition 2.5.16, without loss of generality, we can assume that $\rho \in \mathrm{End}(\mathcal{H}_A \otimes \mathcal{H}_B)$ with $\dim(\mathcal{H}_A) = M$ and $\dim(\mathcal{H}_B) = N$, i.e. we can assume that the reduced state ρ_A and ρ_B are invertible. Further, without loss of generality, let us assume that the space $\mathcal{A}$ of ρ contains $k-1$ rank one hermitian operators that are mutually orthogonal with respect to the Frobenius operator norm. We use induction on k to prove that ρ is locally equivalent by an unitary operator to the state $I \otimes B_1 + \sum_{j=2}^k E_{j-1}^M \otimes B_j$ for some $B_j \in \mathrm{End}(\mathcal{H}_B)$ where E_j^M denotes matrix with size $M \times M$ and entry 1 at jj-th position and zeroes everywhere. For $k = 2$, we write $\rho = \rho_A \otimes B_1 + A_2 \otimes B_2$ with A_2 rank 1 hermitian. As ρ_A is invertible, we can unitarily diagonalize ρ_A by U_1 to get $U_1 \rho_A U_1^\dagger = I$. We note that $U_1 A_2 U_1^\dagger$ is again a hermitian operator of rank 1, so we can unitarily diagonalize $U_1 A_2 U_1^\dagger$ by unitary U_2 such that $U_2(U_1 A_2 U_1^\dagger)U_2^\dagger = \mu E_{11}^M$ where μ is the only non-zero eigenvalue of A_2. Let $U = U_2 U_1$, then $(U \otimes I)\rho(U^\dagger \otimes I) = I \otimes B_1 + E_{11}^M \otimes \mu B_2$, i.e. ρ is locally equivalent by an unitary operator to $I \otimes B_1 + E_{11}^M \otimes \mu B_2$.

Let $\rho = \rho_A \otimes B_1 + \sum_{j=2}^k A_j \otimes B_j$ with $\{A_j : j = 2, ..., k\}$ a set of mutually orthogonal rank 1 hermitian operators. Let $\sigma = \rho_A \otimes B_1 + \sum_{j=2}^{k-1} A_j \otimes B_j$, so σ is an $M \times N$ state with operator Schmidt rank $k-1$ such that the space $\mathcal{A}$ of σ has $k-2$ rank one hermitian operators that are mutually orthogonal with respect to the Frobenius inner product. By the induction hypothesis, there exists unitary U_3 such that $(U_3 \otimes I)\sigma(U_3^\dagger \otimes I) = I \otimes B_1' + \sum_{j=2}^{k-1} E_{j-1}^M \otimes B_j'$, i.e.

$$(U_3 \otimes I)\rho(U_3^\dagger \otimes I) = I \otimes B_1' + \sum_{j=2}^{k-1} E_{j-1}^M \otimes B_j' + U_3 A_k U_3^\dagger \otimes B_k.$$

We write $U_3 A_k U_3^\dagger$ as a block matrix $\left[\begin{array}{c|c} F & C^\dagger \\ \hline C & A_k' \end{array}\right]$, where F is a hermitian $(k-2) \times (k-2)$ matrix. Then A_k' is a hermitian matrix (with rank 0 or 1), so we can unitarily diagonalize A_k' by U_4' to get that if $U_4 = \left[\begin{array}{c|c} I_{k-2} & 0 \\ \hline 0 & U_4' \end{array}\right]$, then $U_4(U_3 A_k U_3^\dagger)U_4^\dagger = \left[\begin{array}{c|c} F & C^\dagger U_4'^\dagger \\ \hline U_4' C & D_k \end{array}\right]$ where D_k is a diagonal matrix with the possible non-zero eigenvalue at the 11-th position and zeroes everywhere. Note that $U_4 E_{j-1}^M U_4^\dagger = E_{j-1}$ for each $j \in \{2, ..., k-1\}$. Let $U = U_4 U_3$, then

$$(U \otimes I)\rho(U^\dagger \otimes I) = I \otimes B_1' + \sum_{j=2}^{k-1} E_{j-1}^M \otimes B_j' + U A_k U^\dagger \otimes B_k.$$

As for unitary U, we have $\mathrm{Tr}\Big(U A_i U^\dagger U A_j U^\dagger\Big) = \mathrm{Tr}\Big(A_i A_j\Big)$, so the set $\{U A_j U^\dagger : j = 2, ..., k\}$ is also orthogonal. But $\{E_{j-1}^M : j = 2, ..., k-1\}$ is in the span of $\{U A_j U^\dagger : j = 2, ..., k-1\}$, so $U A_k U^\dagger$ is orthogonal to E_{j-1}^M for each $j = 2, ..., k-1$, i.e. for each $j \in \{1, ..., k-2\}$ the jj-th entry of $U A_k U^\dagger$ is 0, i.e. the diagonal entries of F are zero. Also $U A_k U^\dagger$ has rank 1 (so all the rows are multiple of a non-zero single row), so $F = 0$. As only the 11-th entry of D_k is non-zero and rank of A_k is 1, so $U_2' C = 0$, i.e. $U A_k U^\dagger = \mu E_{k-1}^M$ where μ is the only non-zero eigenvalue of A_k. Therefore,

$$(U \otimes I)\rho(U^\dagger \otimes I) = I \otimes B_1' + \sum_{j=2}^{k-1} E_{j-1}^M \otimes B_j' + E_{k-1}^M \otimes \mu B_k = I \otimes B_1' + \sum_{j=2}^{k} E_{j-1}^M \otimes B_j'.$$

This finishes our proof by induction. This also shows that $k \leq M$. Finally $[(U \otimes I)\rho(U^\dagger \otimes I)]^{T_A} =$

$I^T \otimes B'_1 + \sum_{j=2}^{k}(E^M_{j-1})^T \otimes B'_j = I \otimes B'_1 + \sum_{j=2}^{k} E^M_{j-1} \otimes B'_j = (U \otimes I)\rho(U^\dagger \otimes I)$, so ρ is PPT and therefore not distillable. □

Chapter 3

Complex Differential Geometry

In this chapter, we shall briefly recall a few basic concepts from the theory of complex differential geometry and algebraic geometry that frequently appear in this thesis. A partial list of references where more comprehensive treatments of the concepts can be found in the books [Zhe00; GH78; Mir95].

3.1 Kähler Manifolds

Definition 3.1.1 (Complex manifold)**.** Let M be a topological space which is connected, Hausdorff and second countable. We call M a *complex manifold* of (complex) dimension $n \in \mathbb{N}$, if there exits an open covering $\{U_a : a \in \mathcal{I}\}$ and for each $a \in \mathcal{I}$ there exists a homeomorphism f_a from U_a onto an open set $V_a \subset \mathbb{C}^n$, such that for any pair $a, b \in \mathcal{I}$ with $U_{ab} := U_a \cap U_b \neq \emptyset$, the mapping $f_a \circ f_b^{-1} : f_b(U_{ab}) \to f_a(U_{ab})$ (called the *transition function*) is a biholomorphism. Let $z = (z_1, z_2, ..., z_n)$ be the standard coordinate of $\mathbb{C}^n$, then we call U_a or (U_a, f_a) a *coordinate neighbourhood* and call $z_a = z \circ f_a$ a *local holomorphic coordinate*.

Example 3.1.2*.* Let $\mathbb{P}^n$ denote the complex projective space of dimension n. Let $U_j = \{[z_0, z_1, ..., z_n] \in \mathbb{C}^{n+1} : z_j \neq 0\}$ and $f_j : U_j \to \mathbb{C}^n$ be defined by

$$f_j([z_0, z_1, ..., z_n]) = \Big(z_0/z_j, ..., z_{j-1}/z_j, z_{j+1}/z_j, ..., z_n/z_j\Big).$$

Then $\{U_j\}_{j\in\{0,1,...,n\}}$ is an open cover of $\mathbb{P}^n$ and f_j is a homeomorphism for each j. Further, the transition function $f_j \circ f_k^{-1} : f_k(U_{jk}) \to f_j(U_{jk})$ given by

$$(z_0/z_k, ..., z_{k-1}/z_k, z_{k+1}/z_k, ..., z_n/z_k) \mapsto \frac{z_k}{z_j}(z_0/z_k, ..., z_{k-1}/z_k, z_{k+1}/z_k, ..., z_n/z_k)$$

is a biholomorphism between open subsets of $\mathbb{C}^n$. Therefore $\mathbb{P}^n$ is a complex manifold of dimension n.

Definition 3.1.3 (Holomorphic maps)**.** A map $\phi : M_1 \to M_2$ between two complex manifolds M_1 and M_2 of dimension n and m respectively is called *holomorphic* at $p \in M_1$ if there exists a coordinate neighbourhood (U_a, f_a) of p and (V_b, g_b) of $\phi(p) \in M_2$, such that the map $g_b \circ \phi \circ f_a^{-1}$ from an open set in $\mathbb{C}^n$ to an open set in $\mathbb{C}^m$ is holomorphic at $f_a(p)$. We say ϕ is holomorphic if it is holomorphic at all points of M_1.

Definition 3.1.4 (Almost Complex Structure)**.** An endomorphism J of the tangent bundle TM of a differentiable manifold M satisfying $J^2 = -I$ is called an *almost complex structure* on M.

Example 3.1.5. Let M be a complex manifold of dimension n and $M_{\mathbb{R}}$ be the underlying differentiable manifold of M. In a local holomorphic coordinate $(z_1 = x_1 + iy_1, ..., z_n = x_n + iy_n)$, we define the map $J : TM_{\mathbb{R}} \to TM_{\mathbb{R}}$ given by

$$J\left(\frac{\partial}{\partial x_j}\right) = \frac{\partial}{\partial y_j},\ J\left(\frac{\partial}{\partial y_j}\right) = -\frac{\partial}{\partial x_j} \quad \text{for } 1 \leq j \leq n$$

and extend linearly over $\mathbb{R}$. Then J is an almost complex structure on $M_{\mathbb{R}}$. Here the almost complex structure on $M_{\mathbb{R}}$ comes from the complex (manifold) structure of M, such almost complex structures are called *integrable* and in that case we sometimes call J a *complex structure* on $M_{\mathbb{R}}$. We take the complexified tangent bundle of $M_{\mathbb{R}}$, denoted by $TM_{\mathbb{R}}^{\mathbb{C}} (= TM_{\mathbb{R}} \otimes \mathbb{C})$. We extend the map J to the complexified tangent bundle using linearity over $\mathbb{C}$ and still denote the map by J. Then we get the decomposition $TM_{\mathbb{R}}^{\mathbb{C}} = TM^{(1,0)} \oplus TM^{(0,1)}$ of eigen-spaces of J corresponding to the eigenvalues i and $-i$ into sum of complex sub-bundles of equal rank, with one equal to the complex conjugation of the other. Then the set $\{\frac{\partial}{\partial z_1}, ..., \frac{\partial}{\partial z_n}\}$ gives a local frame for $TM^{(1,0)}$ and $\{\frac{\partial}{\partial \bar{z}_1}, ..., \frac{\partial}{\partial \bar{z}_n}\}$ gives a local frame for $TM^{(0,1)}$. The map $TM \to TM^{(1,0)}$ given by $V \mapsto V - iJV$ gives the canonical isomorphism between the tangent bundle and the holomorphic tangent bundle.

Definition 3.1.6 (Holomorphic Vector Bundle)**.** Suppose M and E are complex manifolds. We call E an *holomorphic vector bundle* over M, if there exists a continuous mapping $\pi : E \to M$ called the projection such that

1. for all $x \in M$, $E_x = \pi^{-1}(x)$ is complex vector space of rank r, i.e. $E_x \cong \mathbb{C}^r$.

2. There exists an open covering $\{U_\alpha\}_{\alpha \in \mathcal{I}}$ of M and holomorphic maps $\phi_\alpha : \pi^{-1}(U_\alpha) \to U_\alpha \times \mathbb{C}^r$ such that

$$\phi_\alpha : E_x \to \{x\} \times \mathbb{C}^r \cong \mathbb{C}^r \quad \text{for all } x \in U_\alpha$$

is a $\mathbb{C}$ linear isomorphism of complex vector spaces E_x and $\mathbb{C}^r$.

We call (U_α, ϕ_α) a *local trivialization* of E and we call $\{(U_\alpha, \phi_\alpha)\}_{\alpha \in \mathcal{I}}$ a *trivializing open cover* of E. For any pair of $\alpha, \beta \in \mathcal{I}$ with $U_\alpha \cap U_\beta \neq \emptyset$, let $\phi_{\alpha\beta} : U_\alpha \cap U_\beta \to GL_r(\mathbb{C})$ be defined by

$$\phi_{\alpha\beta}(x) = (\phi_\alpha \circ \phi_\beta^{-1})\Big|_{\{x\}\times\mathbb{C}^r} \qquad \text{for all} x \in U_\alpha \cap U_\beta.$$

Then $\phi_{\alpha\beta}$ is called a *transition function* and is holomorphic.

3. The transition functions satisfy the following compatibility conditions:

$$\phi_{\alpha\beta} = \phi_{\beta\alpha}^{-1} \quad \text{on } U_\alpha \cap U_\beta$$
$$\phi_{\alpha\beta} \circ \phi_{\beta\gamma} = \phi_{\alpha\gamma} \quad \text{on } U_\alpha \cap U_\beta \cap U_\gamma.$$

Alternatively, a holomorphic vector bundle over a complex manifold M is a complex vector bundle over M such that the total space E is a complex manifold and the projection map $\pi : E \to M$ is holomorphic.

Definition 3.1.7 (Holomorphic section)**.** Let $E \to M$ be a holomorphic vector bundle and U be an open set of M. A map $s : U \to E$ is said to be *local section* E over U if $\pi \circ s(x) = x$ for all $x \in U$. It is said to be a *local holomorphic section* if the map $s : U \to E$ is holomorphic. A map $s : M \to E$ is said to be a *global holomorphic section* if $\pi \circ s(x) = x$ for all $x \in M$ and $s : M \to E$ is holomorphic. The space of all global holomorphic sections of E is denoted by $H^0(M, E)$.

Example 3.1.8. A common set of examples of holomorphic vector bundles are the holomorphic line bundles $\mathcal{O}(m) \to \mathbb{P}^n$ for $m, n \in \mathbb{N}$. Let us first describe $\pi : \mathcal{O}(1) \to \mathbb{P}^n$, also known as the hyperplane line bundle over the projective space $\mathbb{P}^n$. This line bundle is the dual of the tautological line bundle over $\mathbb{P}^n$. The line bundle $\mathcal{O}(m) \to \mathbb{P}^n$ is m-times tensor power of the line bundle $\mathcal{O}(1) \to \mathbb{P}^n$.

Let $\mathbf{x} = [z_0 : z_1 : ... : z_n] \in \mathbb{P}^n$, then $(z_0, z_1, ..., z_n) \in \mathbb{C}^{n+1}$. Let $V_\mathbf{x}$ be the subspace of $\mathbb{C}^{n+1}$ spanned by $\mathbf{x}$. Then fiber of $\mathcal{O}(1)$ at $\mathbf{x}$ is $V_\mathbf{x}^*$. Let $U_j = \{[z_0, z_1, ..., z_n] \in \mathbb{C}^{n+1} : z_j \neq 0\}$. If $\mathbf{x} \in U_j$, then $\mathbf{x} = [z_0/z_j : ... : 1 : ... : z_n/z_j]$. Define the linear functional $f : V_\mathbf{x} \to \mathbb{C}$ given by $f(v) = \langle v, (z_0/z_j, ..., 1, ..., z_n/z_j)\rangle$, then $\{f\}$ is a basis for $V_\mathbf{x}^*$. Then we have holomorphic map $\phi_j : \pi^{-1}(U_j) \to U_j \times \mathbb{C}$ such that restriction of ϕ_j to the fiber $\phi_j : \mathcal{O}(1)_\mathbf{x} \to \{\mathbf{x}\} \times \mathbb{C}$ is given by $\phi_j(\lambda f) = \lambda$. With these maps (U_j, ϕ_j) becomes a trivializing open cover of the line bundle $\mathcal{O}(1) \to \mathbb{P}^n$ with the transition maps $\phi_{jk} : U_j \cap U_k \to GL_1(\mathbb{C})$ given by $\phi_{jk}(\mathbf{x}) : \mathbb{C} \to \mathbb{C}$ that maps $\phi_{jk}(\mathbf{x})(z) \to z\frac{z_j}{z_k}$.

The line bundle $\mathcal{O}(1) \to \mathbb{P}^n$ has non-zero global holomorphic sections. The space $H^0(\mathbb{P}^n, \mathcal{O}(1))$ is a $(n+1)$-dimensional Hilbert space with a basis $\{w_0, w_1, ..., w_n\}$ where the section w_j is given by the following:

$$\phi_k \circ w_j([w_0 : w_1 : ... : w_n]) = ([w_0 : w_1 : ... : w_n], \frac{w_j}{w_k}).$$

Definition 3.1.9 (Holomorphic Tangent and Cotangent Bundle)**.** On a complex manifold M of dimension n, the bundle $TM^{(1,0)}$ (see Example 3.1.5) is a holomorphic vector bundle as it has the local frame $\{\frac{\partial}{\partial z_1}, ..., \frac{\partial}{\partial z_n}\}$ that vary holomorphically. This bundle is called the *holomorphic tangent bundle* and denoted by $TM^{(1,0)}$. The complex dual bundle to this bundle is called the *holomorphic cotangent bundle* and denoted by $\Omega_M^{1,0}$ or simply Ω_M.

A section of $\Omega_M^{p,q} = \bigwedge^p \Omega_M \otimes \bigwedge^q \overline{\Omega_M}$ is called a (p,q)-form on M and the space of all (p,q)-forms is denoted by $\mathcal{A}^{p,q}(M)$. An r-form is an element of $\mathcal{A}^r(M) := \oplus_{p+q=r}\mathcal{A}^{p,q}(M)$. Let us extend the exterior differentiation operator of the underlying differentiable manifolds structure linearly over $\mathbb{C}$ and still denote it by d. Then d maps $\Omega_M^{p,q}$ into $\Omega_M^{p+1,q} \oplus \Omega_M^{p,q+1}$, so we write $d = \partial + \overline{\partial}$ in this decomposition. It is easy to see that we have $\partial^2 = 0$, $\overline{\partial}^2 = 0$, and $\partial\overline{\partial} + \overline{\partial}\partial = 0$. These two operators are known as *Dolbeault operators* on M. For a holomorphic vector bundle E over a complex manifold M, the space of all the sections of $\Omega_M^{p,q} \otimes E$ is denoted by $\mathcal{A}^{p,q}(E)$. An E-valued r-form is an element of $\mathcal{A}^r(E) := \oplus_{p+q=r}\mathcal{A}^{p,q}(E)$. We can define these operators ∂ and $\overline{\partial}$ on $\mathcal{A}^{p,q}(E)$ by applying the operators only on the $\mathcal{A}^{p,q}(M)$ part of pure tensors and extending linearly.

Definition 3.1.10 (Holomorphic p-form)**.** A $(p,0)$-form ϕ is called a *holomorphic p-form* if $\overline{\partial}\phi = 0$. The space of all holomorphic p-forms is denoted by $H^{p,0}(M)$.

Definition 3.1.11 (Symplectic manifold)**.** A *symplectic form* on a smooth manifold M is a closed non-degenerate differential 2-form ω. A *symplectic manifold* is a pair (M,ω) where ω is a symplectic form on M.

Definition 3.1.12 (Hermitian metric)**.** A *hermitian metric* h on a complex vector bundle E assigns a hermitian inner product h_p to the fibers E_p for each $p \in M$, such that h_p varies smoothly with respect to p.

Definition 3.1.13 (Hermitian vector bundle)**.** A holomorphic vector bundle endowed with a hermitian metric is called a *hermitian vector bundle*.

Definition 3.1.14 (Hermitian manifold)**.** [Bal06] Let M be a complex manifold with a complex structure J. A Riemannian metric g is said to be *compatible with the complex structure J* if

$$g(JX, JX) = g(X, Y)$$

for any vector fields X, Y on M. A complex manifold together with a compatible Riemannian metric is called a *hermitian manifold*. Then we have an associated $(1,1)$-form given by

$$\omega(X, Y) := g(JX, Y)$$

for vector fields X, Y on M. This associated form ω is also non-degenerate and preserves the almost complex structure J (i.e. $\omega(JX, JY) = \omega(X, Y)$). Then we get a hermitian metric h on the holomorphic tangent bundle given by $h = g - i\omega$.

Definition 3.1.15 (Kähler manifold)**.** Let M be a hermitian manifold with a complex structure J and a compatible Riemannian metric g. We call M a *Kähler manifold* if ω is closed (hence ω is a symplectic form). In this case, ω is also called a *Kähler form* and the hermitian metric h on the holomorphic tangent bundle is called a *Kähler metric*.

Example 3.1.16. The complex projective space $\mathbb{P}^n$ can be realized as a quotient $\mathbb{S}^{2n+1}/\mathbb{S}^1$ (this is the *Hopf fibration* $\mathbb{S}^{2n+1} \to \mathbb{P}^n$). The Euclidean metric on $\mathbb{R}^{2n+2}$ can be restricted to $\mathbb{S}^{2n+1}$ to give the so called "round metric" g on $\mathbb{S}^{2n+1}$. This metric is invariant under the action of $\mathbb{S}^1$, so the Riemannian metric g descends to the Riemannian metric g_{FS} on the quotient $\mathbb{P}^n$. The complex projective space $\mathbb{P}^n$ already has the complex structure J. Then the 2-form $\omega_{FS} = g_{FS}(J(\cdot), \cdot)$ give us the Kähler form on $\mathbb{P}^n$ known as the Fubini-Study form. Then the hermitian metric $h_{FS} = g_{FS} - i\omega_{FS}$ is known as the Fubini-Study metric on $\mathbb{P}^n$. This way the projective space $\mathbb{P}^n$ is a Kähler manifold.

Definition 3.1.17 (Complex Connection)**.** Let E be a complex vector bundle over a smooth manifold N. A *complex connection* on E is a complex linear map $\nabla : \mathcal{A}^0(E) \to \mathcal{A}^1(E)$ that satisfies the *Leibniz* rule :

$$\nabla(f\phi) = df \otimes \phi + f\nabla\phi, \ \forall\ f \in C^\infty(N, \mathbb{C}), \forall\ \phi \in \mathcal{A}^0(E).$$

Definition 3.1.18 (Chern Connection)**.** Let E be a holomorphic vector bundle over a complex manifold M equipped with a hermitian metric h. A complex connection ∇ can be decomposed into $\nabla = \nabla^{1,0} + \nabla^{0,1}$ corresponding to the direct sum decomposition $\mathcal{A}^1(E) = \mathcal{A}^{1,0}(E) \oplus \mathcal{A}^{0,1}(E)$. Then there exists a unique connection on E such that the connection is compatible with h (i.e. $Xh(s_1, s_2) = h(\nabla_X s_1, s_2) + h(s_1, \nabla_X s_2)$ for any vector field X on M and section s_1, s_2 of E) and $\nabla^{0,1} = \bar{\partial}$, the Dolbeault operator. This connection is called the *Chern connection* on E.

Definition 3.1.19 (Curvature of a connection)**.** The connection $\nabla : \mathcal{A}^0(E) \to \mathcal{A}^1(E)$ can be extended to a complex linear map $\nabla_p : \mathcal{A}^p(E) \to \mathcal{A}^{p+1}(E)$ for any $p \geq 1$ by the property

$$\nabla_p(\phi \otimes f) = d\phi \otimes f + (-1)^p \phi \wedge \nabla f \forall \phi \in \mathcal{A}^p(M), \forall f \in \mathcal{A}^0(E).$$

The composition $\nabla^2 = \nabla_1 \circ \nabla : \mathcal{A}^0(E) \to \mathcal{A}^2(E)$ is called the *curvature* of the connection ∇.

Definition 3.1.20 (Embedded Submanifold)**.** An *immersed submanifold* is the image $\iota(N)$ of a map $\iota : N \to M$ between differentiable manifolds such that the differential map $d\iota : TN \to TM$

is injective. An *embedded submanifold* is an immersed submanifold such that ι is a homeomorphism onto its image where the image is endowed with subspace topology. In this thesis, we shall write submanifold to mean embedded submanifold and write $N \subset M$ to mean $\iota(N) \subset M$.

Definition 3.1.21 (Symplectic Submanifold)**.** A submanifold X of a symplectic manifold (M, ω) is called *symplectic submanifold* if the restriction $\omega|_X$ $(= \iota^*\omega)$ is a symplectic form.

3.2 Ample Line bundles

Definition 3.2.1 (Very Ample and Ample Line Bundle)**.** A holomorphic line bundle L over a complex compact manifold M *base-point free* if the intersection of the zero sets of all the global holomorphic sections is empty. Then the associated map $\Phi_L : M \to \mathbb{P}^n$ given by

$$\Phi_L(p) = [s_0(p) : s_1(p) : ... : s_n(p)]$$

where $\{s_0, s_1, ..., s_n\}$ is a basis for $H^0(M, L)$ is a well-defined morphism. A holomorphic line bundle L is said to be *very ample* if it is base-point free and the map Φ_L gives a holomorphic projective embedding of M. We say L is *ample* if $L^{\otimes k}$ is very ample for some $k \in \mathbb{N}$.

Example 3.2.2. As described in Example 3.1.8, the space $H^0(\mathbb{P}^n, \mathcal{O}(1))$ has a basis $\{z_0, z_1, ..., z_n\}$ and we see that the zero set of z_j is $\mathbb{P}^n \setminus U_j$. Therefore, the intersection of the zero set of all the global holomorphic sections is empty. Further, the map $\Phi_{\mathcal{O}(1)} : \mathbb{P}^n \to \mathbb{P}^n$, being the identity map is a holomorphic embedding of $\mathbb{P}^n$. Hence, the hyperplane line bundle $\mathcal{O}(1)$ over $\mathbb{P}^n$ is very ample.

A form ω on a complex manifold M is said to be a *positive form* if for any non-zero $V \in TM$, we have $\omega(V, JV) > 0$. For a Kähler form ω, we have $\omega(V, JV) = g(V, V) > 0$ as g is a Riemannian metric, i.e. a Kähler form is a positive form.

Definition 3.2.3. For $j \in \{1, 2\}$, let M_j be a smooth manifold and $L_j \to M_j$ be a line bundle. Let $\pi_1 : M_1 \times M_2 \to M_1$ and $\pi_2 : M_1 \times M_2 \to M_2$ are projection onto the first and second coordinates respectively. Then the line bundle $\pi_1^*(L_1) \otimes \pi_2^*(L_2) \to M_1 \times M_2$ is denoted by $L_1 \boxtimes L_2 \to M_1 \times M_2$. This line bundle is sometimes also called the *box product* or *external tensor product* of the line bundles L_1 and L_2.

Chapter 4

Manifolds and Corresponding Quantum Hilbert Spaces

In the theory of geometric quantization, corresponding to a symplectic manifold having a line bundle with certain structures, we get a subspace of the space of global sections of the line bundle as the quantum Hilbert space. In this chapter, we consider compact complex manifold M having a positive holomorphic hermitian line bundle L. Then the corresponding quantum Hilbert space is defined to be the finite-dimensional Hilbert space $H^0(M, L)$ of the global holomorphic sections of L. We study different quantum information theoretic properties associated with this Hilbert space. The main results in this chapter are Theorems 4.2.1, 4.2.4, 4.2.6, 4.3.1,4.4.7, 4.4.10,4.4.11 and Corollary 4.4.9.

4.1 Introduction

Quantization is an approach to defining a system in quantum mechanics corresponding to a system in classical mechanics. In this section, without going into detail, we shall briefly summarize what is meant by quantization. A partial list of references to learn more about quantization is [Car18; Kir07; CLL21]. The theory of classical mechanics is modelled using the cotangent bundle $M = T^*Q$ for some configuration space Q consisting of local position coordinates. The classical observables are functions on this manifold. The cotangent bundle T^*Q is called the classical phase space. The theory of quantum mechanics, on the other hand, is modelled using a quantum Hilbert space and the observables are operators on this Hilbert space. Quantization is a process, for which there is no general recipe, that attempts to produce a correct quantum theory corresponding to a classical theory, in some limiting cases. The cotangent bundle $M = T^*Q$ naturally has a symplectic manifold structure. Geometric quantization does not only attempt to quantize symplectic manifolds that are cotangent bundles but also attempts to produce a theory of quantization for a general symplectic manifold (M, ω).

The aim is to produce a map from the algebra of functions of M to a suitable Hilbert space having some specific properties (sometimes also called the Dirac conditions). It turns out that to satisfy these conditions is equivalent to having a hermitian line bundle L over M with a connection ∇ such that the curvature form is proportional to the symplectic form ω (such a line bundle is called a *pre-quantum line bundle*). A symplectic manifold (M, ω) is said to be *pre-quantizable* if there exists a pre-quantum line bundle over M. The map that carries functions on M to operators on the Hilbert space $\mathcal{H}_p$ (known as a *pre-quantum Hilbert space*) of square-integrable sections of the line bundle, is known as the pre-quantization map. However, this Hilbert space does not provide the right quantum observables corresponding to classical observables and we need to cut down the pre-quantum Hilbert space. This process is known as choosing a polarization and we finally get a subspace of the pre-quantum Hilbert space known as the quantum Hilbert space. The process of choosing a polarization is not unique in general. For Kähler manifolds (M, ω) with a pre-quantum line bundle, there is a standard method of choosing the polarization to get the standard quantum Hilbert space $H^0(M, L)$ [Kir07]. This is also known as Kähler Quantization. For pre-quantizable non-Kähler manifolds, there are multiple methods of choosing the polarizations, notably almost Kähler quantization [BU96] and Spin^c quantization [Mei98].

This chapter's central object of study is compact complex manifolds with a positive holomorphic hermitian line bundle. We study how properties of the manifold or subsets of this manifold manifest in the quantum information-theoretic properties of the Hilbert space $H^0(M, L)$.

The setup for the works involved in the contents of this chapter is the following: for $j \in \{1, 2\}$ let (L_j, h_j) be a positive holomorphic hermitian line bundle on a compact complex manifold M_j. (Equivalently, consider L_j to be a holomorphic hermitian line bundle on a compact Kähler manifold (M_j, ω_j) of complex dimension $d_j \geq 1$ such that the curvature of the Chern connection on L_j is $-i\omega_j$.) The line bundle defined above is an ample line bundle. Let μ_j be the measure on M_j associated to the volume form $\frac{\omega_j^{d_j}}{d_j!}$ and μ be the measure on $M_1 \times M_2$ associated to the volume form $\frac{\omega_1^{d_1} \omega_2^{d_2}}{d_1! d_2!}$. Let $\pi_1 : M_1 \times M_2 \to M_1$ and $\pi_2 : M_1 \times M_2 \to M_2$ be the projections onto the first and the second manifold respectively. Recall that the holomorphic hermitian line bundle $L_1^N \boxtimes L_2^N \to M_1 \times M_2$ (the external tensor product of line bundles $L_1^N \to M_1$ and $L_2^N \to M_2$) is defined by $L_1^N \boxtimes L_2^N = \pi_1^*(L_1^N) \otimes \pi_2^*(L_2^N)$ and we have

$$H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N) \cong H^0(M_1, L_1^N) \otimes H^0(M_2, L_2^N). \tag{4.1}$$

Further, since the Kähler manifolds involved are compact, these spaces are finite-dimensional. The space of global holomorphic sections $H^0(M_j, L_j^N)$ forms a Hilbert space with the following inner product:

$$\langle s_1, s_2\rangle_j = \int_{M_j} h_j(s_1(z), s_2(z))d\mu_j(z) \text{ for } s_1, s_2 \in H^0(M_j, L_j^N).$$

Similarly, the space $H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N)$ is a Hilbert space with the inner product $\langle ., .\rangle$ given using $\langle ., .\rangle_1$ and $\langle ., .\rangle_2$ and the relation 4.1.

4.2 Average entropy and asymptotics

In this section, we determine the $N \to \infty$ asymptotics of the expected value of entanglement entropy for pure states in $H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N)$. The work presented in this section is the contents of the paper [BSaikia24], modified slightly to fit the context.

4.2.1 Motivation

Calculations of entropy on the Hilbert spaces of geometric quantization or Toeplitz quantization lead to interesting insights [BP17; CE19]. In [FZ22], the main result is the $k \to \infty$ asymptotics of the Shannon entropies of μ_z^k, where $k \in \mathbb{N}$, $z \in M$, M is a toric Kähler manifold with an ample toric hermitian line bundle, and μ_z^k are the Bergman measures that were introduced by Zelditch in [Zel09] to define generalized Bernstein polynomials and were subsequently used in [SZ12; ZZ21]. In a series of papers on random sections of line bundles, starting with [SZ99], Shiffmann and Zelditch worked with the probability space

$$\prod_{k=1}^{\infty} SH^0(M, L^k)$$

where $L \to M$ is an ample holomorphic hermitian line bundle on a compact complex manifold M and $SH^0(M, L^k)$ is the unit sphere in the finite-dimensional Hilbert space $H^0(M, L^k)$. In this section, we consider instead the probability space

$$\Omega = \prod_{k=1}^{\infty} S(H^0(M, L^k) \otimes H^0(M, L^k)). \tag{4.2}$$

and a sequence of random variables ($\mathbb{R}$-valued functions on Ω) $E_k \circ p_k$, where p_k is the projection to the k-th component in the product $\prod_{k=1}^{\infty}$ above in (4.2), and E_k is the entanglement entropy. We find the $k \to \infty$ asymptotics of the sequence of expected values of these random variables. In fact, we prove a more general result.

Theorem 4.2.1 ([BSaikia24]). *Let $L_1 \to M_1$ and $L_2 \to M_2$ be positive holomorphic hermitian line bundles on compact complex manifolds M_1 and M_2 of complex dimensions d_1 and d_2 respectively. Assume w.l.o.g. $d_1 \leq d_2$. Let $d\mu_N$, for each $N \in \mathbb{N}$, be the measure on the unit sphere $S_N = S(H^0(M_1, L_1^N) \otimes H^0(M_2, L_2^N))$ induced by the hermitian metrics. There are the following $N \to \infty$ asymptotics for the average entanglement entropy*

$$\langle E_N \rangle = \frac{\int_{S_N} E_N(v) d\mu_N(v)}{\int_{S_N} d\mu_N(v)}.$$

Let

$$\beta_j = \int_{M_j} \frac{c_1(L_j)^{d_j}}{d_j!} \quad \text{and} \quad \gamma_j = \frac{1}{2} \int_{M_j} \frac{c_1(TM_j) c_1(L_j)^{d_j - 1}}{(d_j - 1)!}$$

for $j \in \{1, 2\}$. As $N \to \infty$,

$$\langle E_N \rangle \sim \begin{cases} \ln \beta_1 + d_1 \ln N - \frac{\beta_1}{2\beta_2} + \left(\frac{\gamma_1}{\beta_1} - \frac{\beta_1}{2\beta_2} (\frac{\gamma_1}{\beta_1} - \frac{\gamma_2}{\beta_2}) \right) \frac{1}{N} + O(\frac{1}{N^2}), \text{ if } d_1 = d_2; \\ \ln \beta_1 + d_1 \ln N + \left(\frac{\gamma_1}{\beta_1} - \frac{\beta_1}{2\beta_2} \right) \frac{1}{N} + O(\frac{1}{N^2}), \text{ if } d_1 = d_2 - 1; \\ \ln \beta_1 + d_1 \ln N + \frac{\gamma_1}{\beta_1} \frac{1}{N} + O(\frac{1}{N^2}), \text{ if } d_1 - d_2 \leq -2. \end{cases}$$

Remark 4.2.2. We observe that a statement analogous to Theorem 4.2.1 holds for semi-positive line bundles L_j on Moishezon manifolds M_j, $j \in \{1, 2\}$. A compact connected complex manifold M of complex dimension d is called a Moishezon manifold if it possesses d algebraically independent meromorphic functions [MM00]. Equivalently, M is Moishezon if and only if it is bi-meromorphic to a d-dimensional projective algebraic variety. The following is true. Let $L_1 \to M_1$ and $L_2 \to M_2$ be holomorphic hermitian line bundles on compact connected complex manifolds M_1 and M_2 of complex dimensions d_1 and d_2 respectively. Assume w.l.o.g. $d_1 \leq d_2$. Assume M_1 and M_2 are Moishezon and L_1, L_2 are semi-positive. Let $d\mu_N$, for each $N \in \mathbb{N}$, be the measure on the unit sphere $S_N = S(H^0(M_1, L_1^N) \otimes H^0(M_2, L_2^N))$ induced by the hermitian metrics. There are the following $N \to \infty$ asymptotics for the average entanglement entropy on the Hilbert spaces $H^0(M_1, L_1^N) \otimes H^0(M_2, L_2^N)$: as $N \to \infty$

$$\langle E_N \rangle \sim \begin{cases} \ln \beta_1 + d_1 \ln N - \frac{\beta_1}{2\beta_2} + o(1), \text{ if } d_1 = d_2; \\ \ln \beta_1 + d_1 \ln N + o(1), \text{ if } d_1 < d_2. \end{cases}$$

where, as before, $\beta_j = \int_{M_j} \frac{c_1(L_j)^{d_j}}{d_j!}$ for $j = 1, 2$. The proof is similar to the proof of Theorem 4.2.1 in section 4.2.3 below, with (4.22, 4.23) replaced by (from Theorem 1.7.1 [MM00])

$$m = m(N) = \dim H^0(M_1, L_1^N) = N^{d_1} \int_{M_1} \frac{c_1(L_1)^{d_1}}{d_1!} + o(N^{d_1})$$

$$n = n(N) = \dim H^0(M_2, L_2^N) = N^{d_2} \int_{M_2} \frac{c_1(L_2)^{d_2}}{d_2!} + o(N^{d_2}).$$

4.2.2 Preliminaries and setup

In this section, we establish the background and write the proofs needed for Theorem 4.2.1. An expression for the average entanglement entropy for the tensor product of two finite-dimensional Hilbert spaces is the statement of Page conjecture [Pag93]. There were several derivations of this formula in the physics literature, including [Sen96]. They seem to assume the equality (4.4) (see below) as a starting point. Our Theorem 4.2.4 below is a proof of (4.4). Then, our proof of Theorem 4.2.6 follows the idea of Sen [Sen96]. Finally, we rely on the semiclassical methods, together with the statement of Theorem 4.2.6, to prove our main result, Theorem 4.2.1 above.

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two complex Hilbert spaces of complex-dimension m and n respectively with $m \leq n$. We note that $\mathcal{H}_A \otimes \mathcal{H}_B \cong \mathbb{C}^m \otimes \mathbb{C}^n \cong \mathbb{R}^{2mn}$. The average value of entanglement over all the pure states would mathematically mean that we integrate the function entropy of entanglement over the set of all pure states (which is geometrically the complex projective space $\mathbb{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$) with respect to the normalized volume measure. In this section, we also provide a clarification of why considering the integral over $\mathbb{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ instead of $\mathbb{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is sufficient. It is due to the property that the entropy of entanglement is invariant under the action of the circle $\mathbb{S}^1$, we can instead use the Hopf fibration to compute the integral over $\mathbb{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ with the spherical measure on $\mathbb{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ (see Proposition 4.2.5).

The spherical measure, in turn, can be written in terms of the ambient Euclidean measure on the unit ball in $\mathcal{H}_A \otimes \mathcal{H}_B \cong \mathbb{R}^{2mn}$ with some adjustment in the integrand function. Motivated by the fact that the Singular Value Decomposition (SVD) of a matrix and the Schmidt decomposition of a vector are essentially the same (see Theorem 2.4.10), we use a change of variable using the SVD to reduce the number of variables in the integral from $2mn$ to only $\min\{m, n\}$ real variable.

Let $\mathbb{S}^{2mn-1} = \{v \in \mathcal{H}_A \otimes \mathcal{H}_B : \|v\| = 1\} \subset \mathcal{H}_A \otimes \mathcal{H}_B$ be the unit sphere in $\mathcal{H}_A \otimes \mathcal{H}_B$ and $d\mu$ be the standard spherical measure on $\mathbb{S}^{2mn-1}$, normalized so that $\int_{\mathbb{S}^{2mn-1}} d\mu = 1$. We fix an orthonormal basis $\{e_1, e_2, ..., e_m\}$ for $\mathcal{H}_A$ and $\{f_1, f_2, ..., f_n\}$ for $\mathcal{H}_B$. Then we have a canonical isomorphism $A : \mathcal{H}_A \otimes \mathcal{H}_B \to M_{n\times m}(\mathbb{C})$ given by

$$v = \sum_{j=1}^{n} \sum_{k=1}^{m} a_{jk}(v) e_k \otimes f_j \mapsto A(v) = (a_{jk}(v))_{n\times m}. \tag{4.3}$$

This map is also a diffeomorphism. Using $M_{n\times m}(\mathbb{C}) \cong \mathbb{R}^{2mn}$, we identify an $n \times m$ matrix with a point in $\mathbb{R}^{2mn}$. For $v \in \mathcal{H}_A \otimes \mathcal{H}_B$, we have the SVD of $A(v) = U(v)\begin{pmatrix} \Sigma(v) \\ 0 \end{pmatrix} V(v)^*$, where

$U(v) \in \mathcal{U}(n)$ and $V(v) \in \mathcal{U}(m)$ and $\Sigma(v) = \text{diag}\{\sigma_1(v), \sigma_2(v), ..., \sigma_m(v)\}$ is a diagonal matrix with $0 \le \sigma_1 \le \sigma_2 \le ... \le \sigma_m$, called the singular values of the matrix $A(v)$. Note that in the SVD of a matrix, the diagonal matrix $\Sigma(v)$ is unique (up to permutation), however, the choice of $U(v)$ and $V(v)$ is not unique.

The Schmidt coefficients of v are the same as the singular values of $A(v)$. If $\sigma_1(v), \sigma_2(v), ...,$ $\sigma_m(v)$ are Schmidt coefficients of $v \in \mathbb{B}^{2mn}$ (where $\mathbb{B}^{2mn}$ is the closed unit ball in $\mathbb{R}^{2mn}$), then $\sum_{j=1}^{m} \sigma_j(v)^2 = \|v\|^2 \le 1$, i.e. for every $v \in \mathbb{B}^{2mn}$, there exists a triple $(U(v), \Sigma(v), V(v))$ such that $A(v) = U(v)\begin{pmatrix}\Sigma(v)\\ 0\end{pmatrix}V(v)^*$, where $U(v) \in \mathcal{U}(n)$ and $V(v) \in \mathcal{U}(m)$ are unitary matrices and $\Sigma(v) = \text{diag}\{\sigma_1(v), \sigma_2(v), ..., \sigma_m(v)\}$ a diagonal matrix with $0 \le \sigma_1(v) \le \sigma_2(v) \le ... \le \sigma_m(v)$ and $\sum_{j=1}^{m} \sigma_j(v)^2 \le 1$. Conversely, if $A(v) \in M_{n\times m}$ has a SVD $A(v) = U(v)\begin{pmatrix}\Sigma(v)\\ 0\end{pmatrix}V(v)^*$ such that $\sum_{j=1}^{m} \sigma_j^2 \le 1$, then $v \in \mathbb{B}^{2mn}$.

Lemma 4.2.3. *The singular value decomposition $A = U\begin{pmatrix}\Sigma\\ 0\end{pmatrix}V^*$ of a matrix $A \in M_{n\times m}(\mathbb{C})$ is not unique. However, for a matrix A with distinct non-zero singular values, we can find a unique triple $([\tilde{U}], \Sigma, [\tilde{V}])$, where $[\tilde{U}] \in V_m^n(\mathbb{C})$ (= $\mathcal{U}(n)/\mathcal{U}(n-m)$, the complex Stiefel manifold), $\Sigma \in \{diag\{x_1, x_2, ..., x_m\} : 0 < x_1 < x_2 < ... < x_m\}$, and $[\tilde{V}] \in \mathcal{U}(m)/\mathcal{U}(1)^m$ such that the first non-vanishing entry in each column of V is positive and $A = \tilde{U}\begin{pmatrix}\Sigma\\ 0\end{pmatrix}\tilde{V}$. Let us call this decomposition the "modified SVD" for the matrix A.*

Proof. Let A be a $n \times m$ matrix with distinct singular values and $A = U\begin{pmatrix}\Sigma\\ 0\end{pmatrix}V^*$ be an SVD of A, so the entries of Σ are distinct. Let $U = \begin{pmatrix}U_1 & U_2\end{pmatrix}$ where U_1 is the matrix whose columns are the first m columns of U and U_2 is the matrix whose columns are the last $n-m$ columns of U. Then we see that $A = U_1\Sigma V^*$. To see that SVD is not unique, let $\tau = \text{diag}\{e^{i\theta_1}, e^{i\theta_2}, ..., e^{i\theta_m}\}$ for $-\pi < \theta_1, \theta_2, ..., \theta_m \le \pi$. Let $V' = V\tau$ and $U' = U\begin{pmatrix}\tau & 0\\ 0 & I\end{pmatrix}$ are unitary matrices respective size. Then $U'\Sigma V'^* = \begin{pmatrix}U_1 & U_2\end{pmatrix}\begin{pmatrix}\tau & 0\\ 0 & I\end{pmatrix}\begin{pmatrix}\Sigma\\ 0\end{pmatrix}(V\tau)^* = U_1\Sigma V^* = A$ is also an SVD of A.

Let $V = [v_{jk}] \in \mathcal{U}(m)$. For each $j \in \{1, 2, ..., m\}$, suppose $v_{k_j j}$ be the first entry in the j-th column such that $v_{k_j j} \neq 0$. Let $v_{k_j j} = |v_{k_j j}|e^{i\theta_j}, \theta_j \in (-\pi, \pi]$, we define

$$\tilde{V}_j = (v_{1j}e^{-i\theta_j}, ..., |v_{k_j j}|, ..., v_{nj}e^{-i\theta_j})^T$$
$$(\tau_V)_j = (0, ..., e^{i\theta_j}, ..., 0)^T$$

Let $\tilde{V}$ and τ_V be the unitaries with j-th column equal to $\tilde{V}_j$ and $(\tau_V)_j$ respectively. Then we see that $V = \tilde{V}\tau_V$. The map $\mathcal{U}(m) \to (\mathcal{U}(m)/(\mathcal{U}(1))^m) \times (\mathcal{U}(1))^m$ given by $V \mapsto ([\tilde{V}], \tau_V)$ is a bijection, where $[\tilde{V}]$ represents the equivalent class of $(\mathcal{U}(m)/(\mathcal{U}(1))^m)$ containing $\tilde{V}$.

Now, suppose $A = U\begin{pmatrix}\Sigma\\0\end{pmatrix}V^*$ is an SVD of A where diagonal entries of Σ are in ascending order. Let $V = \tilde{V}\tau_V$ be the factorization of V as above and $\tilde{U} = \begin{pmatrix}U_1 & U_2\end{pmatrix}\begin{pmatrix}\tau_V^* & 0\\ 0 & I\end{pmatrix} = \begin{pmatrix}U_1\tau_V^* & U_2\end{pmatrix} = \begin{pmatrix}\tilde{U}_1 & \tilde{U}_2\end{pmatrix}$ (say). Thus, we have a triple $([\tilde{U}], \Sigma, [\tilde{V}])$ such that the first non-zero entry of each column of V is positive and $\tilde{U}\begin{pmatrix}\Sigma\\0\end{pmatrix}\tilde{V}^* = A$.

Suppose we have another triple $([\tilde{E}], \Sigma, [\tilde{F}])$ such that the first non-zero entry of each column F is positive and $A = \tilde{E}\begin{pmatrix}\Sigma\\0\end{pmatrix}\tilde{F}^*$. Since Σ is the same as before and all entries of Σ are non-zero and distinct, the j-th column of $\tilde{F}$ must be $e^{i\phi_j}\tilde{V}_j$ for some $\phi_j \in (-\pi, \pi]$. Further, since k_j-th entries of both these columns must be positive, therefore we must have $\phi_j = 0$, i.e. $\tilde{F} = \tilde{V}$. Since $\tilde{V} = \tilde{F}$ and all entries of the diagonal matrix Σ are non-zero and distinct, using the following

$$\tilde{E}\begin{pmatrix}\Sigma\\0\end{pmatrix}\tilde{F}^* = A = \tilde{U}\begin{pmatrix}\Sigma\\0\end{pmatrix}\tilde{V}^*,$$

we get that the j-th column of $\tilde{E}$ is equal to the j-th column of $\tilde{U}$ for all $j \in \{1, 2, ..., m\}$, i.e. $\tilde{E}_1 = \tilde{U}_1$, i.e. $[\tilde{E}] = [\tilde{U}]$ as an element of $\mathcal{U}(n)/\mathcal{U}(n-m)$. This completes the uniqueness part of the proof. □

Note that for matrix A with singular values that are not distinct, even the "modified SVD" is not unique. This is because we can permute the equal singular values in Σ to get a different SVD decomposition of A where the columns of $\tilde{U}$ and $\tilde{V}$ are also permuted accordingly.

Theorem 4.2.4 ([BSaikia24]). *Let f be a continuous function on $\mathbb{S}^{2mn-1}$ that depends only on the squares of the Schmidt coefficients. For $v \in \mathbb{B}^{2mn}$, let $\sigma_1(v), ..., \sigma_m(v)$ be the Schmidt coefficients of v and $p_1(v), ..., p_m(v)$ be the eigenvalues of* $\mathrm{Tr}_B(vv^*)$ *(i.e. by the proof of Proposition 2.4.11, we have $p_j(v) = \sigma^2_{\tau(j)}(v)$ for some $\tau \in S_m$), then*

$$\int_{\mathbb{S}^{2mn-1}} f(u)d\mu(u) = \frac{\int_{T_m} f\left(\frac{p_1(v)}{\sum_{k=1}^m p_k(v)}, ..., \frac{p_m(v)}{\sum_{k=1}^m p_k(v)}\right) \prod\limits_{1\le j<k\le m}^{m} (p_k(v) - p_j(v))^2 \prod_{j=1}^m p_j(v)^{n-m} dp_j(v)}{\int_{T_m} \prod_{1\le j<k\le m}^m (p_k(v) - p_j(v))^2 \prod_{j=1}^m p_j(v)^{n-m} dp_j(v)} \tag{4.4}$$

where $T_m = \{(x_1, ..., x_m) \in \mathbb{R}^m : 0 < x_1 < ... < x_m$ and $x_1 + ... + x_m \le 1\}$ and μ is the standard spherical measure on $\mathbb{S}^{2mn-1}$ normalized so that $\int_{\mathbb{S}^{2mn-1}} d\mu = 1$.

Proof. We will use the Lebesgue measure ν of the ambient Euclidean space $\mathbb{R}^{2mn}$ and then for $X \subset \mathbb{S}^{2mn-1}$, $\mu(X) = \frac{1}{\mathrm{Vol}(\mathbb{B}^{2mn})}\nu(\{tx | x \in X \text{ and } t \in [0,1]\})$. Then for an integrable function defined on $\mathbb{S}^{2mn-1}$, we have

$$\int_{\mathbb{S}^{2mn-1}} f(u)d\mu(u) = \frac{1}{\mathrm{Vol}(\mathbb{B}^{2mn})} \int_{\mathbb{B}^{2mn}} f\left(\frac{v}{||v||}\right) d\nu(v).$$

Suppose $\mathcal{S} = \{v \in \mathbb{B}^{2mn} :$ the singular values of $A(v)$ are non-zero and distinct$\}$ where $A(v)$ is the matrix given by the map A defined in Equation (4.3). Let $\mathcal{B}$ be the set $\{(x_1, ..., x_m) \in \mathbb{R}^m : 0 < x_1 < x_2 < ... < x_m \text{ and } x_1^2 + ... + x^2 \leq 1\}$. Then the "modified SVD" composed with the map A gives an one-to-one correspondence between $\mathcal{S}$ and $V_m^n(\mathbb{C}) \times \mathcal{B} \times (U(m)/(U(1))^m)$. Note that $\mathbb{B}^{2mn} \setminus \mathcal{S}$ is a set of measure zero, therefore

$$\int_{\mathbb{B}^{2mn}} f\left(\frac{v}{||v||}\right) d\nu(v) = \int_{\mathcal{S}} f\left(\frac{v}{||v||}\right) d\nu(v).$$

For $v \in \mathcal{S}$, we will make a change of variables using singular value decomposition of $A(v) = \tilde{U}(v)\begin{pmatrix}\Sigma(v)\\0\end{pmatrix}\tilde{V}(v)^*$, where $\tilde{U} = \begin{pmatrix}\tilde{U}_1 & \tilde{U}_2\end{pmatrix}$ with $\tilde{U}_1$ and $\tilde{U}_2$ the matrices with columns the first m columns of $\tilde{U}$ and last $n-m$ columns of $\tilde{U}$ respectively. Let $\tilde{u}_j(v)$ be the j-th column of $\tilde{U}(v)$ and $\tilde{v}_k(v)$ be the k-th column of $\tilde{V}(v)$. Now,

$$A(v) = \tilde{U}(v)\begin{pmatrix}\Sigma(v)\\0\end{pmatrix}\tilde{V}^*(v)$$

hence

$$dA(v) = d\tilde{U}(v)\begin{pmatrix}\Sigma(v)\\0\end{pmatrix}\tilde{V}^*(v) + \tilde{U}(v)\begin{pmatrix}d\Sigma(v)\\0\end{pmatrix}\tilde{V}^*(v) + \tilde{U}(v)\begin{pmatrix}\Sigma(v)\\0\end{pmatrix}d\tilde{V}^*(v).$$

The volume measure at $v_0 \in \mathcal{S}$ can be written as $\tilde{U}^*(v_0)dA(v)\tilde{V}(v_0)|_{v=v_0}$ (as $\tilde{U}^*(v_0)$ and $\tilde{V}(v_0)$ being unitary matrices do not affect the volume). Let

$$dB(v_0) = \tilde{U}^*(v_0)dA(v)\tilde{V}(v_0)|_{v=v_0}.$$

Then,

$$\begin{aligned} dB(v_0) &= \tilde{U}^*(v_0)d\tilde{U}(v_0)\begin{pmatrix}\Sigma(v_0)\\0\end{pmatrix} + \begin{pmatrix}d\Sigma(v_0)\\0\end{pmatrix} + \begin{pmatrix}\Sigma(v_0)\\0\end{pmatrix}d\tilde{V}^*(v_0)\tilde{V}(v_0) \\ &= \begin{pmatrix}\tilde{U}_1^*(v_0)d\tilde{U}_1(v_0)\Sigma(v_0) + d\Sigma(v_0) + \Sigma(v_0)d\tilde{V}^*(v_0)\tilde{V}(v_0)\\ \tilde{U}_2^*(v_0)d\tilde{U}_1(v_0)\Sigma(v_0)\end{pmatrix}\end{aligned}$$

As v_0 was an arbitrary point in $\mathcal{S}$, so we have

$$dB(v) = \begin{pmatrix} \tilde{U}_1^*(v)d\tilde{U}_1(v)\Sigma(v) + d\Sigma(v) + \Sigma(v)d\tilde{V}^*(v)\tilde{V}(v) \\ \tilde{U}_2^*(v)d\tilde{U}_1(v)\Sigma(v) \end{pmatrix}$$

For notational convenience, we drop the "(v)" to write

$$dB = \begin{pmatrix} \tilde{U}_1^*d\tilde{U}_1\Sigma + d\Sigma + \Sigma d\tilde{V}^*\tilde{V} \\ \tilde{U}_2^*d\tilde{U}_1\Sigma \end{pmatrix}.$$

Since $\tilde{U}_1^*\tilde{U}_1 = I$, it follows that $d\tilde{U}_1^*\tilde{U}_1 + \tilde{U}_1^*d\tilde{U}_1 = 0$, then

$$\tilde{U}_1^*d\tilde{U}_1 = -d\tilde{U}_1^*\tilde{U}_1 = -(\tilde{U}_1^*d\tilde{U}_1)^*,$$

so $\tilde{U}_1^*d\tilde{U}_1$ is an anti-hermitian matrix. Similarly, $\tilde{V}^*d\tilde{V}$ is also anti-hermitian. Denote $E = \tilde{U}_1^*d\tilde{U}_1$ and $F = \tilde{V}^*d\tilde{V}$, then for $j,k \in \{1,2,...,m\}$ we have $E_{jk} = \tilde{u}_j^*d\tilde{u}_k$ and $F_{jk} = \tilde{v}_j^*d\tilde{v}_k$. Now,

$$dB = \begin{pmatrix} E\Sigma + d\Sigma - \Sigma F \\ \tilde{U}_2^*d\tilde{U}_1\Sigma \end{pmatrix}.$$

As E and F are anti-hermitian, the diagonal elements of E and F are imaginary. It follows that the real parts of diagonal elements of dB are exactly the diagonal elements of $d\Sigma$ and imaginary parts of the diagonal elements of dB come from the matrix $E\Sigma - \Sigma F$, i.e,

$$\mathrm{Re}(dB_{jj}) = d\Sigma_{jj} = d\sigma_j$$

$$\mathrm{Im}(dB_{jj}) = \sigma_j(\mathrm{Im}(\tilde{u}_j^*d\tilde{u}_j) - \mathrm{Im}(\tilde{v}_j^*d\tilde{v}_j))$$

for $j \in \{1,2,...,m\}$. Let $j \in \{1,2,...,m\}$ with $j > k$, then

$$\begin{aligned} dB_{jk} &= \sigma_k E_{jk} - \sigma_j F_{jk} \\ dB_{kj} &= \sigma_j E_{kj} - \sigma_k F_{kj} = -\sigma_j \overline{E_{jk}} + \sigma_k \overline{F_{jk}}. \end{aligned}$$

We get,

$$\begin{aligned} \mathrm{Re}(dB_{jk}) &= \sigma_k \,\mathrm{Re}(E_{jk}) - \sigma_j \,\mathrm{Re}(F_{jk}) \\ \mathrm{Im}(dB_{jk}) &= \sigma_k \,\mathrm{Im}(E_{jk}) - \sigma_j \,\mathrm{Im}(F_{jk}) \\ \mathrm{Re}(dB_{kj}) &= -\sigma_j \,\mathrm{Re}(E_{jk)} + \sigma_k \,\mathrm{Re}(F_{jk}) \\ \mathrm{Im}(dB_{kj}) &= \sigma_j \,\mathrm{Im}(E_{jk}) - \sigma_k \,\mathrm{Im}(F_{jk}) \end{aligned}$$

Computing the wedge of real parts and the imaginary parts,

$$\mathrm{Re}(dB_{jk})\,\mathrm{Re}(dB_{kj}) = (\sigma_k^2 - \sigma_j^2)\,\mathrm{Re}(E_{jk})\,\mathrm{Re}(F_{jk})$$
$$\mathrm{Im}(dB_{jk})\,\mathrm{Im}(dB_{kj}) = (\sigma_k^2 - \sigma_j^2)\,\mathrm{Im}(F_{jk})\,\mathrm{Im}(E_{jk})$$

we get that

$$\mathrm{Re}(dB_{jk})\,\mathrm{Im}(dB_{jk})\,\mathrm{Re}(dB_{kj})\,\mathrm{Im}(dB_{kj}) = -(\sigma_k^2 - \sigma_j^2)^2\,\mathrm{Re}(\tilde{u}_j^* d\tilde{u}_k)\,\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_k)\,\mathrm{Re}(\tilde{v}_j^* d\tilde{v}_k)\,\mathrm{Im}(\tilde{v}_j^* d\tilde{v}_k).$$

Combining all these and ignoring the sign, we get the form

$$\begin{aligned}&\bigwedge_{j=1}^{m} \mathrm{Re}(dB_{jj}) \bigwedge_{j,k=1,\, j\neq k}^{m} \mathrm{Re}(dB_{jk})\,\mathrm{Im}(dB_{jk})\\ =&\bigwedge_{j=1}^{m} d\sigma_j \prod_{1\le j<k\le m}^{m} (\sigma_k^2 - \sigma_j^2)^2 \eta \bigwedge_{1\le j<k\le m} \mathrm{Re}(\tilde{u}_j^* d\tilde{u}_k)\,\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_k)\end{aligned}$$

where

$$\eta = \bigwedge_{1\le j<k\le m} \mathrm{Re}(\tilde{v}_j^* d\tilde{v}_k)\,\mathrm{Im}(\tilde{v}_j^* d\tilde{v}_k).$$

We note that η is a volume form of $\mathcal{U}(m)/(\mathcal{U}(1)^m)$. For the imaginary part of the diagonal entries, for $j,k \in \{1,...,m\}$ with $j \neq k$, let's look at the following

$$\begin{aligned}&\mathrm{Im}(dB_{jj}) \wedge \mathrm{Im}(dB_{kk})\\ =&\sigma_j(\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_j) - \mathrm{Im}(\tilde{v}_j^* d\tilde{v}_j)) \wedge \sigma_k(\mathrm{Im}(\tilde{u}_k^* d\tilde{u}_k) - \mathrm{Im}(\tilde{v}_k^* d\tilde{v}_k))\\ =&\sigma_j\sigma_k\,\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_j)\,\mathrm{Im}(\tilde{u}_k^* d\tilde{u}_k) + \kappa\end{aligned}$$

where $\kappa = \sigma_j\sigma_k[\mathrm{Im}(\tilde{v}_j^* d\tilde{v}_j)\,\mathrm{Im}(\tilde{v}_k^* d\tilde{v}_k) - \mathrm{Im}(\tilde{u}_j^* d\tilde{u}_j)\,\mathrm{Im}(\tilde{v}_k^* d\tilde{v}_k) - \mathrm{Im}(\tilde{u}_k^* d\tilde{u}_k)\,\mathrm{Im}(\tilde{v}_j^* d\tilde{v}_j)]$. We note that η is the volume form of the compact group $\mathcal{U}(m)/\mathcal{U}(1)^m$, so $\kappa \wedge \eta = 0$ (as η already contains all the independent variables coming from V). So,

$$\bigwedge_{j=1}^{m} \mathrm{Im}(dB_{jj}) = \prod_{j=1}^{m} \sigma_j \bigwedge_{j=1}^{m} \mathrm{Im}(\tilde{u}_j^* d\tilde{u}_j).$$

Therefore,

$$\begin{aligned}&\bigwedge_{j,k=1}^{m} (\mathrm{Re}(dB_{jk})\,\mathrm{Im}(dB_{jk})\\ =&\prod_{j=1}^{m} \sigma_j \prod_{1\le j<k\le m} (\sigma_k^2 - \sigma_j^2)^2 \eta \bigwedge_{1\le j<k\le m} \mathrm{Re}(\tilde{u}_j^* d\tilde{u}_k)\,\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_k) \bigwedge_{j=1}^{m} \mathrm{Im}(\tilde{u}_j^* d\tilde{u}_j) \bigwedge_{j=1}^{m} d\sigma_j\end{aligned}$$

Now, for $k \in \{1, 2, ..., m\}$ and $j \in \{m+1, m+2, ..., n\}$, we have $dB_{jk} = (\tilde{U}_2 d\tilde{U}_1 \Sigma)_{j-m,k} = \sigma_k \tilde{u}_j^* d\tilde{u}_k$. Therefore,

$$\bigwedge_{j=m+1}^{n} \bigwedge_{k=1}^{m} \mathrm{Re}(dB_{jk}) \,\mathrm{Im}(dB_{jk}) = \bigwedge_{j=m+1}^{n} \bigwedge_{k=1}^{m} \sigma_k^2 \,\mathrm{Re}(\tilde{u}_j^* d\tilde{u}_k) \,\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_k)$$
$$= \prod_{j=1}^{m} \sigma_k^{2(n-m)} \bigwedge_{j=m+1}^{n} \bigwedge_{k=1}^{m} \mathrm{Re}(\tilde{u}_j^* d\tilde{u}_k) \,\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_k)$$

Gathering all these and ignoring sign, we get that

$$\rho = \bigwedge_{j=1}^{n} \bigwedge_{k=1}^{m} \mathrm{Re}(dB_{jk}) \,\mathrm{Im}(dB_{jk})$$
$$= \prod_{j=1}^{m} \sigma_j \prod_{1 \le j < k \le m} (\sigma_k^2 - \sigma_j^2)^2 \prod_{j=1}^{m} \sigma_k^{2(n-m)} \eta \omega \bigwedge_{j=1}^{m} d\sigma_j$$

where

$$\omega = \bigwedge_{1 \le j < k \le m} \mathrm{Re}(\tilde{u}_j^* d\tilde{u}_k) \,\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_k) \bigwedge_{j=1}^{m} \mathrm{Im}(\tilde{u}_j^* d\tilde{u}_j) \bigwedge_{j=m+1}^{n} \bigwedge_{k=1}^{m} \mathrm{Re}(\tilde{u}_j^* d\tilde{u}_k) \,\mathrm{Im}(\tilde{u}_j^* d\tilde{u}_k)$$

is a form independent of σ_j's. We have

$$\int_{\mathbb{S}^{2mn-1}} d\mu = \frac{1}{\mathrm{Vol}(\mathbb{B}^{2mn})} \int_{\mathcal{S}} d\nu$$
$$= \frac{c(m,n)}{\mathrm{Vol}(\mathbb{B}^{2mn})} \int_{(\mathcal{U}(m)/(\mathcal{U}(1))^m) \times \mathcal{B} \times V_m^n(\mathbb{C})} \rho$$
$$= \frac{c(m,n)}{\mathrm{Vol}(\mathbb{B}^{2mn})} \int_{\mathcal{U}(m)/(\mathcal{U}(1))^m} \eta \int_{V_m^n(\mathbb{C})} \omega \int_{\mathcal{B}} \prod_{j=1}^{m} \sigma_j \prod_{1 \le j < k \le m} (\sigma_k^2 - \sigma_j^2)^2 \prod_{j=1}^{m} \sigma_j^{2(n-m)} d\sigma_j$$

where $c(m,n)$ is a constant due to the requirement that $\int_{\mathbb{S}^{2mn-1}} d\mu = 1$. For the integral $\int_{\mathcal{B}} \prod_{j=1}^{m} \sigma_j \prod_{1 \le j < k \le m}^{m} (\sigma_k^2 - \sigma_j^2)^2 \prod_{j=1}^{m} \sigma_j^{2(n-m)} d\sigma_j$, we change variables to $p_j = \sigma_j^2$ to get

$$\int_{\mathcal{B}} \prod_{j=1}^{m} \sigma_j \prod_{1 \le j < k \le m}^{m} (\sigma_k^2 - \sigma_j^2)^2 \prod_{j=1}^{m} \sigma_j^{2(n-m)} d\sigma_j = \frac{1}{2^m} \int_{T_m} \prod_{1 \le j < k \le m}^{m} (p_k - p_j)^2 \prod_{j=1}^{m} p_j^{n-m} dp_j.$$

We note that for $v \in \mathbb{B}^{2mn}$, if $p_1, ..., p_m$ are the eigenvalues of $\mathrm{Tr}_B(vv^*)$, then $\frac{p_1}{\sum_{j=1}^m p_j}, ..., \frac{p_m}{\sum_{j=1}^m p_j}$ are the eigenvalues of $\mathrm{Tr}_B(\frac{vv^*}{\|v\|^2})$. Therefore, for a function f on $\mathbb{S}^{2mn-1}$ that depends only on the squares of the Schmidt coefficients $\sigma_j(u)$ of $u \in \mathbb{S}^{2mn-1}$ (in other words, depends only on

$p_j(u)$'s), we get

$$
\begin{aligned}
&\int_{\mathbb{S}^{2mn-1}} f(u)d\mu(u)\\
=&\frac{1}{\mathrm{Vol}(\mathbb{B}^{2mn})}\int_S f\left(\frac{v}{\|v\|}\right)d\nu(v)\\
=&\frac{c(m,n)}{\mathrm{Vol}(\mathbb{B}^{2mn})}\int_{(\mathcal{U}(m)/(\mathcal{U}(1))^m)\times\mathcal{B}\times V_m^n(\mathbb{C})} f\left(\frac{v}{\|v\|}\right)\rho\\
=&\frac{\frac{c(m,n)}{\mathrm{Vol}(\mathbb{B}^{2mn})}\int_{(\mathcal{U}(m)/(\mathcal{U}(1))^m)\times\mathcal{B}\times V_m^n(\mathbb{C})} f\left(\frac{v}{\|v\|}\right)\rho}{\frac{c(m,n)}{\mathrm{Vol}(\mathbb{B}^{2mn})}\int_{(\mathcal{U}(m)/(\mathcal{U}(1))^m)\times\mathcal{B}\times V_m^n(\mathbb{C})}\rho} \quad \text{(as the denominator is } \int_S d\mu = 1)\\
=&\frac{\int_{T_m} f\left(\frac{p_1(v)}{\sum_{k=1}^m p_k(v)},\dots,\frac{p_m(v)}{\sum_{k=1}^m p_k(v)}\right)\prod_{1\le j<k\le m}^m (p_k(v)-p_j(v))^2\prod_{j=1}^m p_j(v)^{n-m}dp_j(v)}{\int_{T_m}\prod_{1\le j<k\le m}^m (p_k(v)-p_j(v))^2\prod_{j=1}^m p_j(v)^{n-m}dp_j(v)}.
\end{aligned}
$$

□

Proposition 4.2.5. *Let $\mathbb{S}^{2n+1}\to\mathbb{P}^n$ be the Hopf fibration and $f:\mathbb{S}^{2n+1}\to\mathbb{R}$ be a continuous function such that f is constant on the fibers, i.e. $f:\mathbb{P}^n\to\mathbb{R}$ is also a well-defined continuous function. Then*

$$
\frac{\int_{\mathbb{S}^{2n+1}} f(x)d\mu(x)}{\int_{\mathbb{S}^{2n+1}} d\mu(x)} = \frac{\int_{\mathbb{P}^n} f(x)d\nu(x)}{\int_{\mathbb{P}^n} d\nu(x)} \tag{4.5}
$$

where μ is the standard spherical measure on $\mathbb{S}^{2n+1}$ and ν is the measure coming from Fubini-Study metric on $\mathbb{P}^n$.

Proof. Let η_k be the standard Riemannian volume form on $\mathbb{S}^k$ and ω_{FS} be the Fubini-Study form on $\mathbb{P}^n$. The standard spherical measure on $\mathbb{S}^{2n+1}$ comes from the standard Riemannian metric g on the sphere. This metric is invariant under the action of $\mathbb{S}^1$ and descends the quotient $\mathbb{S}^{2n+1}/\mathbb{S}^1$ to produce the Fubini-Study metric g_{FS} on $\mathbb{P}^n$.

Let $\{U_j\}$ be a trivializing open cover for the Hopf fibration $\mathbb{S}^{2n+1}\to\mathbb{P}^n$. Let $g^{(j)}$ be the metric restricted to $U_j\times\mathbb{S}^1$ and $g_{FS}^{(j)}$ be the metric restricted to U_j. Then $g^{(j)}$ is simply the product metric of $g_{FS}^{(j)}$ and the standard Riemannian metric on $\mathbb{S}^1$. Therefore the restricted Riemannian volume form on $U_j\times\mathbb{S}^1$ is given by $\eta_{2n+1}|_{U_j\times\mathbb{S}^1} = c_j\omega_{FS}^n|_{U_j}\wedge\eta_1$ for some non-zero constant c. Let us denote $\omega_j = \omega_{FS}^n|_{U_j}$.

Let $\{\rho_j\}$ be a partition of unity subordinate to the open cover $\{U_j\}$ of $\mathbb{P}^n$, then $\{\rho'_j\}$ is a partition of unity subordinate to the open cover $\{U_j\times\mathbb{S}^1\}$ where $\rho'_j(x,y)=\rho_j(x)$ for all $(x,y)\in U_j\times\mathbb{S}^1$ and $\rho'_j(x,y)=0$ for all $(x,y)\notin U_j\times\mathbb{S}^1$. Then we have

$$
\omega_{FS}^n = \sum_j \rho_j\omega_j^n
$$

and

$$\eta_{2n+1} = \sum_j c_j \rho'_j \omega_j^n \wedge \eta_1.$$

Now for any continuous function $h : S^{2n+1} \to \mathbb{R}$ that is constant on the fibers, we have

$$\begin{aligned}
\int_{\mathbb{S}^{2n+1}} h\eta_{2n+1} &= \sum_j c_j \int_{U_j \times \mathbb{S}^1} h\rho'_j \omega_j^n \wedge \eta_1 \\
&= \sum_j c_j \int_{U_j} h\rho_j \omega_j^n \int_{\mathbb{S}^1} \eta_1 \quad \text{(using Fubini's Theorem)} \\
&= 2\pi \sum_j c_j \int_{U_j} h\rho_j \omega_j^n \\
&= 2\pi \int_{\mathbb{P}^n} h\omega_{FS}^n
\end{aligned}$$

Hence, we have

$$\frac{\int_{\mathbb{S}^{2n+1}} f(x) d\mu(x)}{\int_{\mathbb{S}^{2n+1}} d\mu(x)} = \frac{2\pi \int_{\mathbb{P}^n} f(x) d\nu(x)}{2\pi \int_{\mathbb{P}^n} d\nu(x)} = \frac{\int_{\mathbb{P}^n} f(x) d\nu(x)}{\int_{\mathbb{P}^n} d\nu(x)}.$$

□

From the Propositions 2.4.13 and 2.4.15, we have seen that the entropy of entanglement is a continuous function on $\mathbb{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ that is also well defined on $\mathbb{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$, therefore the expected value of the entropy of entanglement over all the pure states is

$$\frac{\int_{\mathbb{P}(\mathcal{H}_A \otimes \mathcal{H}_B)} E_{(m,n)}(u) d\nu(u)}{\int_{\mathbb{P}(\mathcal{H}_A \otimes \mathcal{H}_B)} d\nu(x)},$$

which by the above Proposition 4.2.5 is equivalent to the Equation 4.6 below.

Theorem 4.2.6. *[BSaikia24] The expected value of the entropy of entanglement of all the pure states in $\mathcal{H}_A \otimes \mathcal{H}_B$ is*

$$\langle E_{(m,n)} \rangle = \sum_{k=n+1}^{mn} \frac{1}{k} + \frac{m-1}{2n}.$$

Proof. We base our proof on the general idea of the proof in [Sen96]. Let μ be the spherical measure on $\mathbb{S}^{2mn-1}$ normalized such that $\int_{\mathbb{S}^{2mn-1}} d\mu = 1$. The expected value of the entropy of entanglement over all the pure states is given by

$$\int_{\mathbb{S}^{2mn-1}} E_{(m,n)}(u) d\mu(u). \tag{4.6}$$

Now, using Theorem 4.2.4, we get

$$\int_{\mathbb{S}^{2mn-1}} E_{(m,n)}(u)d\mu(u)$$
$$=\frac{\int_{T_m}\left(-\sum_{j=1}^m \frac{p_j}{\sum_{k=1}^m p_k}\ln\frac{p_j}{\sum_{k=1}^m p_k}\right)\prod_{1\le j<k\le m}^m (p_k-p_j)^2\prod_{j=1}^m p_j^{n-m}dp_j}{\int_{T_m}\prod_{1\le j<k\le m}^m (p_k-p_j)^2\prod_{j=1}^m p_j^{n-m}dp_j}. \tag{4.7}$$

Note that both the functions $P(p_1, ..., p_m) = \prod_{1\le j<k\le m}^m (p_k-p_j)^2\prod_{j=1}^m p_j^{n-m}$ and $E_{(m,n)} = \left(-\sum_{j=1}^m \frac{p_j}{\sum_{k=1}^m p_k}\ln\frac{p_j}{\sum_{k=1}^m p_k}\right)P(p_1, ..., p_m)$ are symmetric in the arguments $p_1, ..., p_m$, therefore the condition in the region of integration $0 < x_1 < .... < x_m$ of T_m can be removed to rewrite

$$\langle E_{(m,n)}\rangle = \frac{2^m\int_{T_m}\left(-\sum_{j=1}^m \frac{p_j}{\sum_{k=1}^m p_k}\ln\frac{p_j}{\sum_{k=1}^m p_k}\right)\prod_{1\le j<k\le m}^m (p_k-p_j)^2\prod_{j=1}^m p_j^{n-m}dp_j}{2^m\int_{T_m}\prod_{1\le j<k\le m}^m (p_k-p_j)^2\prod_{j=1}^m p_j^{n-m}dp_j}$$
$$=\frac{\int_{R_m}\left(-\sum_{j=1}^m \frac{p_j}{\sum_{k=1}^m p_k}\ln\frac{p_j}{\sum_{k=1}^m p_k}\right)\prod_{1\le j<k\le m}^m (p_k-p_j)^2\prod_{j=1}^m p_j^{n-m}dp_j}{\int_{R_m}\prod_{1\le j<k\le m}^m (p_k-p_j)^2\prod_{j=1}^m p_j^{n-m}dp_j}, \tag{4.8}$$

where $R_m = \{(x_1, ..., x_m) \in \mathbb{R}^m : 0 \le x_1, ..., x_m \text{ and } x_1 + ... + x_m \le 1\}$.

We change variables to $(q_1, ..., q_{m-1}, r)$ such that $q_1 + ... + q_{m-1} + q_m = 1$, and $q_k = rp_k$ for $k = 1, 2, ..., m$ (i.e. $r = \frac{1}{\sum_{j=1}^m p_j}$), so $r \in [1,\infty)$. Then for $j \in \{1, ..., m\}$ we have,

$$\frac{\partial q_k}{\partial p_j} = \delta_{jk} r \text{ for } k \in \{1, ..., m-1\}$$
$$\frac{\partial r}{\partial p_j} = \frac{\partial}{\partial p_j}\left(\frac{1}{\sum_k p_k}\right) = \frac{-1}{(\sum_k p_k)^2} = -r^2$$

We denote $F_m = \{(x_1, x_2, ..., x_m) \in \mathbb{R}^m : x_1, x_2, ..., x_m \ge 0 \text{ and } x_1 + x_2 + ... + x_m = 1\}$. So, the integral becomes

$$\frac{\int_1^\infty\int_{F_m}\left(-\sum_{j=1}^m q_j\ln q_j\right)\prod_{1\le j<k\le m}^m(\frac{q_k}{r}-\frac{q_j}{r})^2\prod_{j=1}^m\left(\frac{q_j}{r}\right)^{n-m}\frac{1}{r^{m+1}}dr\prod_{j=1}^{m-1}dq_j}{\int_1^\infty\int_{F_m}\prod_{1\le j<k\le m}^m(\frac{q_k}{r}-\frac{q_j}{r})^2\prod_{j=1}^m\left(\frac{q_j}{r}\right)^{n-m}\frac{1}{r^{m+1}}dr\prod_{j=1}^{m-1}dq_j}$$
$$=\frac{\int_1^\infty\frac{dr}{r^{mn+1}}\int_{F_m}\left(-\sum_{j=1}^m q_j\ln q_j\right)\prod_{1\le j<k\le m}^m(q_k-q_j)^2\prod_{j=1}^m q_j^{n-m}\prod_{j=1}^{m-1}dq_j}{\int_1^\infty\frac{dr}{r^{mn+1}}\int_{F_m}\prod_{1\le j<k\le m}^m(q_k-q_j)^2\prod_{j=1}^m q_j^{n-m}\prod_{j=1}^{m-1}dq_j}$$
$$=\frac{\int_{F_m}\left(-\sum_{j=1}^m q_j\ln q_j\right)\prod_{1\le j<k\le m}^m(q_k-q_j)^2\prod_{j=1}^m q_j^{n-m}\prod_{j=1}^{m-1}dq_j}{\int_{F_m}\prod_{1\le j<k\le m}^m(q_k-q_j)^2\prod_{j=1}^m q_j^{n-m}\prod_{j=1}^{m-1}dq_j} \tag{4.9}$$

Let $x_k = tq_k$ for $k = 1, 2, ..., m$ with $t \in [0,\infty)$, so that $x_1 + x_2 + ... + x_m = t$ and $x_k \in [0,\infty)$.

Then, for $j \in \{1, 2, ..., m\}$, we have

$$\frac{\partial q_k}{\partial x_j} = \delta_{jk} t \text{ for } k \in \{1, 2, ..., m-1\} \text{ and } \frac{\partial t}{\partial x_j} = 1$$

Using the determinant of the Jacobian, we get

$$\begin{aligned} dq_1 \wedge ... \wedge dq_{m-1} \wedge dt &= \frac{1}{t^{m-1}} dx_1 \wedge ... \wedge dx_{m-1} \wedge dx_m \\ &= \frac{1}{t^{m-1}} dx_1 \wedge ... \wedge dx_{m-1} \wedge d(x_1 + ... + x_{m-1} + x_m) \\ &= \frac{1}{t^{m-1}} dx_1 \wedge ... \wedge dx_{m-1} \wedge dt \end{aligned} \tag{4.10}$$

Now, we use the gamma function $\Gamma(z) = \int_0^\infty y^{z-1} e^{-y} dy$ and the derivative of the gamma function $\Gamma'(z) = \int_0^\infty y^{z-1} e^{-y} \ln y dy$. In particular,

$$\begin{aligned} \int_0^\infty t^{mn} e^{-t} dt &= \Gamma(mn+1) = (mn)!, \\ \int_0^\infty t^{mn} e^{-t} \ln t dt &= \Gamma'(mn+1) = (mn)! \psi(mn+1), \end{aligned}$$

where $\psi(N+1) = -\gamma + \sum_{k=1}^N \frac{1}{k}$ and γ is the Euler constant. We have,

$$\begin{aligned} &\frac{\int_{F_m} \left(-\sum_{j=1}^m q_j \ln q_j\right) \prod_{1\le j<k\le m}^m (q_k - q_j)^2 \prod_{j=1}^m q_j^{n-m} \prod_{j=1}^{m-1} dq_j}{\int_{F_m} \prod_{1\le j<k\le m}^m (q_k - q_j)^2 \prod_{j=1}^m q_j^{n-m} \prod_{j=1}^{m-1} dq_j} \\ =&\frac{(mn-1)!}{(mn)!} \frac{\int_0^\infty t^{mn} e^{-t} dt \int_{F_m} \left(-\sum_{j=1}^m q_j \ln q_j\right) \prod_{1\le j<k\le m}^m (q_k - q_j)^2 \prod_{j=1}^m q_j^{n-m} \prod_{j=1}^{m-1} dq_j}{\int_0^\infty t^{mn-1} e^{-t} dt \int_{F_m} \prod_{1\le j<k\le m}^m (q_k - q_j)^2 \prod_{j=1}^m q_j^{n-m} \prod_{j=1}^{m-1} dq_j} \\ =&\frac{1}{mn} \frac{\int_{[0,\infty)^m} \left(-\sum_{j=1}^m \left(\frac{x_j}{t}\right) \ln\left(\frac{x_j}{t}\right)\right) \prod_{1\le j<k\le m}^m \left(\frac{x_k}{t} - \frac{x_j}{t}\right)^2 \prod_{j=1}^m \left(\frac{x_j}{t}\right)^{n-m} e^{-t} t^{mn} \frac{dt}{t^{m-1}} \prod_{j=1}^{m-1} dx_j}{\int_{[0,\infty)^m} \prod_{1\le j<k\le m}^m \left(\frac{x_k}{t} - \frac{x_j}{t}\right)^2 \prod_{j=1}^m \left(\frac{x_j}{t}\right)^{n-m} e^{-t} t^{mn-1} \frac{dt}{t^{m-1}} \prod_{j=1}^{m-1} dx_j} \\ =&\frac{1}{mn} \frac{\int_{[0,\infty)^m} \left(-\sum_{j=1}^m x_j \ln\left(\frac{x_j}{t}\right)\right) \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j}{\int_{[0,\infty)^m} \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j} \\ =&\frac{\int_{[0,\infty)^m} t \ln t \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j}{mn \int_{[0,\infty)^m} \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j} \\ &- \frac{\int_{[0,\infty)^m} \left(\sum_{j=1}^m x_j \ln x_j\right) \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j}{mn \int_{[0,\infty)^m} \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j} \end{aligned} \tag{4.11}$$

Let the first and the second integral in Equation (4.11) be denoted by I_1 and I_2 respectively. We have

$$
\begin{aligned}
I_1 =&\frac{\int_{[0,\infty)^m} t\ln t \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j}{mn\int_{[0,\infty)^m} \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j} \\
=&\frac{\int_0^\infty \int_{F_m} t\ln t \prod_{1\le j<k\le m}^m (tq_k - tq_j)^2 \prod_{j=1}^m (tq_j)^{n-m} e^{-t} t^{m-1} dt \prod_{j=1}^{m-1} dq_j}{mn\int_0^\infty \int_{F_m} \prod_{1\le j<k\le m}^m (tq_k - tq_j)^2 \prod_{j=1}^m (tq_j)^{n-m} e^{-t} t^{m-1} dt \prod_{j=1}^{m-1} dq_j} \\
=&\frac{\int_0^\infty t^{mn} \ln t e^{-t} dt \int_{F_m} \prod_{1\le j<k\le m}^m (q_k - q_j)^2 \prod_{j=1}^m q_j^{n-m} \prod_{j=1}^{m-1} dq_j}{mn\int_0^\infty t^{mn-1} e^{-t} dt \int_{F_m} \prod_{1\le j<k\le m}^m (q_k - q_j)^2 \prod_{j=1}^m q_j^{n-m} \prod_{j=1}^{m-1} dq_j} \\
=&\frac{\Gamma'(mn+1)}{mn\Gamma(mn)} = \psi(mn+1)
\end{aligned} \tag{4.12}
$$

Using Equation (4.10), the second integral in Equation (4.11) becomes

$$
\begin{aligned}
I_2 =&\frac{\int_{[0,\infty)^m} \left(\sum_{j=1}^m x_j \ln x_j\right) \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j}{mn\int_{[0,\infty)^m} \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-t} dt \prod_{j=1}^{m-1} dx_j} \\
=&\frac{\sum_{l=1}^m \int_{[0,\infty)^m} x_l \ln x_l \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-(x_1+\ldots+x_m)} \prod_{j=1}^m dx_j}{mn\int_{[0,\infty)^m} \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-(x_1+\ldots+x_m)} \prod_{j=1}^m dx_j}
\end{aligned} \tag{4.13}
$$

We observe that the Vandermonde determinant

$$
\Delta(x_1, ..., x_m) = \prod_{1\le j<k\le m}^m (x_k - x_j) = \det \begin{pmatrix} 1 & \ldots & 1 \\ x_1 & \ldots & x_m \\ \vdots & \ddots & \vdots \\ x_1^{m-1} & \ldots & x_m^{m-1} \end{pmatrix}.
$$

As the determinant remains unchanged after applying elementary row operations, we see that

$$
\prod_{1\le j<k\le m}^m (x_k - x_j) = \det \begin{pmatrix} f_0(x_1) & \ldots & f_0(x_m) \\ f_1(x_1) & \ldots & f_1(x_m) \\ \vdots & \ddots & \vdots \\ f_{m-1}(x_1) & \ldots & f_{m-1}(x_m) \end{pmatrix} = \det_{m\times m}(f_{j-1}(x_k)),
$$

for any set of polynomials $\{f_0, f_1, ..., f_{m-1}\}$ with $f_0 = 1$ and f_k's are monic with $\deg(f_k) = k$ for $k = 1, ..., m-1$. We choose these polynomials cleverly for the $\Delta(x_1, ..., x_m)^2$ appearing in the numerator and the denominator in Equation (4.13). We use a class of orthogonal polynomials, generalized Laguerre polynomials, given by

$$
L_k^{(\alpha)}(x) = \frac{x^{-\alpha} e^x}{k!} \frac{d^k}{dx^k}(e^{-x} x^{k+\alpha}),
$$

where $\alpha \in \mathbb{R}$ and $k \in \mathbb{N} \cup \{0\}$. These polynomials satisfy the orthogonality relation,

$$\int_0^\infty x^\alpha e^{-x} L_k^{(\alpha)}(x) L_j^{(\alpha)}(x) dx = \frac{\Gamma(k+\alpha+1)}{k!}\delta_{jk}. \tag{4.14}$$

Using these polynomials, we have $\Delta(x_1,...,x_m) = \det_{m\times m}\left(L_{j-1}^{(\alpha)}(x_k)\right) = \sum_{\sigma\in S_m} \mathrm{sgn}(\sigma)\prod_{k=1}^m L_{\sigma(k-1)}^{(n-m)}(x_k)$. The integral in Equation (4.13) becomes

$$\begin{aligned}
I_2 =& \frac{\sum_{l=1}^m \left(\int_{[0,\infty)^m} x_l \ln x_l \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-(x_1+...+x_m)} \prod_{j=1}^m dx_j\right)}{mn \int_{[0,\infty)^m} \prod_{1\le j<k\le m}^m (x_k - x_j)^2 \prod_{j=1}^m x_j^{n-m} e^{-(x_1+...+x_m)} \prod_{j=1}^m dx_j} \\
=& \frac{\sum_{l=1}^m \left(\int_{[0,\infty)^m} x_l \ln x_l \Delta(x_1,...,x_m)\Delta(x_1,...,x_m) \prod_{j=1}^m x_j^{n-m} e^{-x_j} dx_j\right)}{mn \int_{[0,\infty)^m} \Delta(x_1,...,x_m)\Delta(x_1,...,x_m) \prod_{j=1}^m x_j^{n-m} e^{-x_j} dx_j} \\
=& \frac{\sum_{l=1}^m \left(\int_{[0,\infty)^m} x_l \ln x_l \sum_{\sigma,\tau\in S_m}\left(\mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\prod_{k=1}^m L_{\sigma(k-1)}^{(n-m)}(x_k) L_{\tau(k-1)}^{(n-m)}(x_k)\prod_{j=1}^m x_j^{n-m} e^{-x_j} dx_j\right)\right)}{mn \int_{[0,\infty)^m} \sum_{\sigma,\tau\in S_m} \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\prod_{k=1}^m L_{\sigma(k-1)}^{(n-m)}(x_k) L_{\tau(k-1)}^{(n-m)}(x_k)\prod_{j=1}^m x_j^{n-m} e^{-x_j} dx_j} \\
=& \frac{\sum_{l=1}^m \sum_{\sigma,\tau\in S_m}\left(\mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\int_{[0,\infty)^m} x_l \ln x_l \prod_{k=1}^m L_{\sigma(k-1)}^{(n-m)}(x_k) L_{\tau(k-1)}^{(n-m)}(x_k) x_k^{n-m} e^{-x_k} dx_k\right)}{mn \sum_{\sigma,\tau\in S_m}\left(\mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\int_{[0,\infty)^m} \prod_{k=1}^m L_{\sigma(k-1)}^{(n-m)}(x_k) L_{\tau(k-1)}^{(n-m)}(x_k) x_k^{n-m} e^{-x_k} dx_k\right)} \\
=& \frac{\sum_{l=1}^m \sum_{\sigma,\tau\in S_m}\left(\mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\prod_{k=1}^m \int_0^\infty (x_k \ln x_k)^{\delta_{lk}} L_{\sigma(k-1)}^{(n-m)}(x_k) L_{\tau(k-1)}^{(n-m)}(x_k) x_k^{n-m} e^{-x_k} dx_k\right)}{mn \sum_{\sigma,\tau\in S_m}\left(\mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\prod_{k=1}^m \int_0^\infty L_{\sigma(k-1)}^{(n-m)}(x_k) L_{\tau(k-1)}^{(n-m)}(x_k) x_k^{n-m} e^{-x_k} dx_k\right)} \\
=& \frac{\sum_{l=1}^m \sum_{\sigma\in S_m}\left(\prod_{k=1}^m \int_0^\infty (x_k \ln x_k)^{\delta_{lk}} [L_{\sigma(k-1)}^{(n-m)}(x_k)]^2 x_k^{n-m} e^{-x_k} dx_k\right)}{mn \sum_{\sigma\in S_m}\left(\prod_{k=1}^m \int_0^\infty [L_{\sigma(k-1)}^{(n-m)}(x_k)]^2 x_k^{n-m} e^{-x_k} dx_k\right)} \text{(using the orthogonal property)} \\
=& \frac{\sum_{l=1}^m \sum_{\sigma\in S_m}\left(\int_0^\infty x_l^{n-m+1} \ln x_l [L_{\sigma(l-1)}^{(n-m)}(x_l)]^2 e^{-x_l} dx_l \prod_{k=1,k\neq l}^m \left(\int_0^\infty [L_{\sigma(k-1)}^{(n-m)}(x_k)]^2 x_k^{n-m} e^{-x_k} dx_k\right)\right)}{mn \sum_{\sigma\in S_m}\left(\prod_{k=1}^m \int_0^\infty [L_{\sigma(k-1)}^{(n-m)}(x_k)]^2 x_k^{n-m} e^{-x_k} dx_k\right)} \\
=& \frac{\sum_{l=1}^m \sum_{\sigma\in S_m}\left(\int_0^\infty x^{n-m+1} \ln x [L_{\sigma(l-1)}^{(n-m)}(x)]^2 e^{-x} dx \prod_{k=1,k\neq l}^m \left(\int_0^\infty [L_{\sigma(k-1)}^{(n-m)}(x)]^2 x^{n-m} e^{-x} dx\right)\right)}{mn \sum_{\sigma\in S_m}\left(\prod_{k=1}^m \int_0^\infty [L_{\sigma(k-1)}^{(n-m)}(x)]^2 x^{n-m} e^{-x} dx\right)} \\
=& \frac{\sum_{l=1}^m \left((m-1)!\sum_{s=1}^m\left(\int_0^\infty x^{n-m+1} \ln x [L_{s-1}^{(n-m)}(x)]^2 e^{-x} dx \prod_{k=1,k\neq s}^m \left(\int_0^\infty [L_{k-1}^{(n-m)}(x)]^2 x^{n-m} e^{-x} dx\right)\right)\right)}{mn(m)! \prod_{j=1}^m \int_0^\infty [L_{j-1}^{(n-m)}(x)]^2 x^{n-m} e^{-x} dx} \\
=& \sum_{l=1}^m \sum_{s=1}^m \frac{\int_0^\infty x^{n-m+1} \ln x [L_{s-1}^{(n-m)}(x)]^2 e^{-x} dx}{m^2 n \int_0^\infty [L_{s-1}^{(n-m)}(x)]^2 x^{n-m} e^{-x} dx} \\
=& m \sum_{s=1}^m \frac{\int_0^\infty x^{n-m+1} \ln x [L_{s-1}^{(n-m)}(x)]^2 e^{-x} dx}{m^2 n \int_0^\infty [L_{s-1}^{(n-m)}(x)]^2 x^{n-m} e^{-x} dx} \\
=& \frac{1}{mn} \sum_{k=0}^{m-1} \frac{\int_0^\infty x^{n-m+1} \ln x [L_k^{(n-m)}(x)]^2 e^{-x} dx}{\int_0^\infty [L_k^{(n-m)}(x)]^2 x^{n-m} e^{-x} dx}
\end{aligned} \tag{4.15}$$

Let $I_k^{(\alpha)} = \int_0^\infty x^{\alpha+1}\ln x[L_k^{(\alpha)}(x)]^2 e^{-x}dx$ and $J_k(\alpha) = \int_0^\infty x^{\alpha+1}[L_k^{(\alpha)}(x)]^2 e^{-x}dx$. By properties of Laguerre polynomials, we have

$$J_k(\alpha) = \frac{(2k+\alpha+1)\Gamma(k+\alpha+1)}{k!}. \tag{4.16}$$

Now,

$$\frac{d}{d\alpha}J_k(\alpha) = \int_0^\infty x^{\alpha+1}\ln x[L_k^{(\alpha)}(x)]^2 e^{-x}dx + 2\int_0^\infty x^{\alpha+1}L_k^{(\alpha)}(x)\frac{dL_k^{(\alpha)}(x)}{d\alpha}e^{-x}dx$$

$$\implies I_k^{(n-m)} = \left[\frac{d}{d\alpha}J_k(\alpha) - 2\int_0^\infty x^{\alpha+1}L_k^{(\alpha)}(x)\frac{dL_k^{(\alpha)}(x)}{d\alpha}e^{-x}dx\right]_{\alpha=n-m} \tag{4.17}$$

Using Equation (4.16), we get

$$\begin{aligned}\frac{d}{d\alpha}J_k(\alpha) &= \frac{d}{d\alpha}\left(\frac{(2k+\alpha+1)\Gamma(k+\alpha+1)}{k!}\right)\\ &= \frac{\Gamma(k+\alpha+1)}{k!} + \frac{2k+\alpha+1}{k!}\frac{d\Gamma(k+\alpha+1)}{d\alpha}\\ &= \frac{\Gamma(k+\alpha+1)}{k!} + \frac{2k+\alpha+1}{k!}\Gamma(k+\alpha+1)\psi(k+\alpha+1)\\ &= \frac{\Gamma(k+\alpha+1)}{k!}[1+(2k+\alpha+1)\psi(k+\alpha+1)]\end{aligned} \tag{4.18}$$

We use the property $L_k^{(\alpha)}(x) = L_k^{(\alpha+1)}(x) - L_{k-1}^{(\alpha+1)}(x)$ and $\frac{dL_k^{(\alpha)}(x)}{d\alpha} = \sum_{j=0}^{k-1}\frac{L_j^{\alpha}(x)}{k-j}$ to compute

$$\begin{aligned}&\int_0^\infty x^{\alpha+1}L_k^{(\alpha)}(x)\frac{dL_k^{(\alpha)}(x)}{d\alpha}e^{-x}dx\\ &= \int_0^\infty x^{\alpha+1}L_k^{(\alpha)}(x)\sum_{j=0}^{k-1}\frac{L_j^{\alpha}(x)}{k-j}e^{-x}dx\\ &= \sum_{j=0}^{k-1}\frac{1}{k-j}\int_0^\infty x^{\alpha+1}\left(L_k^{(\alpha+1)}(x) - L_{k-1}^{(\alpha+1)}(x)\right)\left(L_j^{(\alpha+1)}(x) - L_{j-1}^{(\alpha+1)}(x)\right)e^{-x}dx\\ &= -\int_0^\infty x^{\alpha+1}[L_{k-1}^{(\alpha+1)}(x)]^2 e^{-x}dx\\ &= -\frac{\Gamma(k+\alpha+1)}{(k-1)!}\end{aligned} \tag{4.19}$$

Using Equations (4.18) and (4.19) in Equation (4.17), we get

$$I_k^{(n-m)} = \left[\frac{\Gamma(k+\alpha+1)}{k!}[1+(2k+\alpha+1)\psi(k+\alpha+1)] + 2\frac{\Gamma(k+\alpha+1)}{(k-1)!}\right]_{\alpha=n-m}$$

$$
\begin{aligned}
&= \left[\frac{\Gamma(k+\alpha+1)}{k!}(1+2k+(2k+\alpha+1)\psi(k+\alpha+1))\right]_{\alpha=n-m} \\
&= \frac{\Gamma(k+n-m+1)}{k!}[1+2k+(2k+n-m+1)\psi(k+n-m+1)] \qquad (4.20)
\end{aligned}
$$

Using Equations (4.14) and (4.20) in Equation (4.15), we get

$$
\begin{aligned}
I_2 =& \frac{1}{mn}\sum_{k=0}^{m-1}[1+2k+(2k+n-m+1)\psi(k+n-m+1)] \\
=& \frac{1}{mn}\sum_{0}^{m-1}(1+2k) + \frac{1}{mn}\sum_{k=0}^{m-1}\left[(2k+n-m+1)\left(-\gamma+\sum_{r=1}^{n-m+k}\frac{1}{r}\right)\right] \\
=& \frac{m+m(m-1)}{mn} - \gamma\frac{1}{mn}\sum_{k=0}^{m-1}(2k+n-m+1) + \frac{1}{mn}\sum_{k=0}^{m-1}\sum_{r=1}^{n-m+k}\frac{2k+n-m+1}{r} \\
=& \frac{m}{n} - \gamma + \left[mn + \frac{mn}{2} + \ldots + \frac{mn}{n-m} + \frac{mn-(n-m+1)}{n-m+1} + \ldots \right. \\
& \left. + \frac{mn-(n-m+1)-(n-m+1+2)\ldots-((n-m-1)+2(m-1)))}{n-m+m-1}\right] \times \frac{1}{mn} \\
=& \frac{m}{n} - \gamma + \sum_{k=1}^{n-1}\frac{1}{k} - \frac{1}{mn}\left[\frac{n-m+1}{n-m+1} + \ldots. + \frac{(m-1)(n-m)+(m-1)^2}{n-m+m-1}\right] \\
=& \frac{m}{n} - \gamma + \sum_{k=1}^{n-1}\frac{1}{k} - \frac{1}{mn}[1+\ldots.+(m-1)] \\
=& -\gamma + \sum_{k=1}^{mn}\frac{1}{k} - \sum_{k=n+1}^{mn}\frac{1}{k} + \frac{m-1}{2n} \\
=& \psi(mn+1) - \sum_{k=n+1}^{mn}\frac{1}{k} + \frac{m-1}{2n} \qquad (4.21)
\end{aligned}
$$

Using Equations (4.12), (4.21), (4.11) and (4.9), we get the expected value of Entropy of Entanglement over the pure states is

$$
\sum_{k=n+1}^{mn}\frac{1}{k} - \frac{m-1}{2n}.
$$

□

4.2.3 Asymptotics of average entropy

Proof of Theorem 4.2.1. For $j \in \{1, 2\}$, let (L_j, h_j) be a holomorphic hermitian line bundle on a compact Kähler manifold (M_j, ω_j) of complex dimension $d_j \geq 1$ such that the curvature of the Chern connection on L_j is $-i\omega_j$, and $d_1 \leq d_2$. For $N \in \mathbb{N}$, the Hilbert spaces $\mathcal{H}_A$ (of dimension $m = m(N)$) and $\mathcal{H}_B$ (of dimension $n = n(N)$) will be $H^0(M_1, L_1^N)$ and $H^0(M_2, L_2^N)$. Let $N \to \infty$.

We have [MM00, sec. 4.1.1.]:

$$m = m(N) = \beta_1 N^{d_1} + \gamma_1 N^{d_1-1} + O(N^{d_1-2}) \tag{4.22}$$

$$n = n(N) = \beta_2 N^{d_2} + \gamma_2 N^{d_2-1} + O(N^{d_2-2}) \tag{4.23}$$

where

$$\beta_j = \int_{M_j} \frac{c_1(L_j)^{d_j}}{d_j!}$$

$$\gamma_j = \frac{1}{2}\int_{M_j} \frac{c_1(TM_j)c_1(L_j)^{d_j-1}}{(d_j-1)!}$$

for $j \in \{1, 2\}$.

We notice that $m \leq n$ for large N. By Theorem 4.2.6, the average entanglement entropy $\langle E_N \rangle$ over all the pure states in $H^0(M_1, L_1^N) \otimes H^0(M_2, L_2^N)$ equals

$$\Big(\sum_{k=n+1}^{mn} \frac{1}{k}\Big) - \frac{m-1}{2n}. \tag{4.24}$$

To figure out the asymptotics of Equation (4.24), we apply the Euler-Maclaurin formula to $f(x) = \frac{1}{x}$, to conclude that

$$\sum_{k=n+1}^{mn} \frac{1}{k} = \int_n^{mn} \frac{1}{x} dx + \frac{f(mn) - f(n)}{2} + \sum_{k=1}^{[\frac{p}{2}]} \frac{B_{2k}}{(2k)!}(f^{(2k-1)}(mn) - f^{(2k-1)}(n)) + R_p$$

where B_{2k} are the Bernoulli numbers, in particular $B_2 = \frac{1}{6}$, and for the remainder we have the estimate

$$|R_p| \leq \frac{2\zeta(p)}{(2\pi)^p} \int_n^{mn} |f^{(p)}(x)| dx.$$

Therefore, $\langle E_N \rangle$ becomes

$$\ln m + \frac{1}{2mn} - \frac{m}{2n} + \sum_{k=1}^{[\frac{p}{2}]} \frac{B_{2k}}{(2k)!}(f^{(2k-1)}(mn) - f^{(2k-1)}(n)) + R_p. \tag{4.25}$$

In Equation (4.25), let us set $p = 2$ in the part

$$\frac{1}{2mn} + \sum_{k=1}^{[\frac{p}{2}]} \frac{B_{2k}}{(2k)!}(f^{(2k-1)}(mn) - f^{(2k-1)}(n)) + R_p$$

and by (4.22 and 4.23) we can now conclude that this part is $O(N^{-2d_2})$, because

$$|R_2| \leq \frac{\zeta(2)}{2\pi^2} \int_n^{mn} |f''(x)| dx = \frac{1}{12}(\frac{1}{n^2} - \frac{1}{m^2n^2}),$$

$$f'(mn) - f'(n) = -\frac{1}{m^2n^2} + \frac{1}{n^2}.$$

It remains to consider the term $\ln m - \frac{m}{2n}$ in (4.25). By (4.22)

$$\ln m = \ln\left(\beta_1 N^{d_1}\left(1 + \frac{\gamma_1}{\beta_1 N} + O(\frac{1}{N^2})\right)\right) \sim \ln\beta_1 + d_1 \ln N + \frac{\gamma_1}{\beta_1 N} + O(\frac{1}{N^2}).$$

If $d_1 = d_2$, then by (4.22,4.23), we get

$$\frac{m}{2n} = \frac{\beta_1(1 + \frac{\gamma_1}{\beta_1}\frac{1}{N} + O(\frac{1}{N^2}))}{2\beta_2(1 + \frac{\gamma_2}{\beta_2}\frac{1}{N} + O(\frac{1}{N^2}))} \sim \frac{\beta_1}{2\beta_2}\left(1 + (\frac{\gamma_1}{\beta_1} - \frac{\gamma_2}{\beta_2})\frac{1}{N}\right) + O(\frac{1}{N^2}).$$

Similarly, if $d_1 = d_2 - 1$, then

$$\frac{m}{2n} = \frac{\beta_1(1 + \frac{\gamma_1}{\beta_1}\frac{1}{N} + O(\frac{1}{N^2}))}{2\beta_2 N(1 + \frac{\gamma_2}{\beta_2}\frac{1}{N} + O(\frac{1}{N^2}))} \sim \frac{\beta_1}{2\beta_2}\frac{1}{N} + O(\frac{1}{N^2}),$$

and if $d_1 - d_2 \leq -2$, then

$$\frac{m}{2n} \sim O(\frac{1}{N^2}).$$

The statement of the theorem follows. □

4.3 Semiclassical asymptotics and entropy

In this section, we study the entanglement of quantum states associated with submanifolds of Kähler manifolds. As a motivating example, we discuss the semiclassical asymptotics of entanglement entropy of pure states on the two-dimensional sphere with the standard metric. The work presented in this section is the contents of the paper [BSaikia23], modified slightly to fit the context.

Our general philosophy is tied to the geometry versus analysis perspective. It emerges in different ways in mathematics, and those often align with physics-driven ideas. For instance, Lagrangian states or Bohr-Sommerfeld states have been a part of the philosophy of geometric quantization for a long time (see e.g. [BPU95]). Gelfand-Naimark theorem as well as other reconstruction theorems had a substantial impact on the development of non-commutative geometry and interesting applications to physics (see e.g. [GMT14]). Shannon entropy (information-theoretic entropy) has been brought into Kähler geometry. Semiclassical asymptotics, with various geometric aspects, have been addressed in [BP17; CE19; FZ22]. In [SHK11] the emphasis is on automorphisms and orbits.

Informally speaking, while discussing the geometry vs. analysis paradigm, by "geometry" we will mean a smooth manifold M, possibly with an additional structure (such as a symplectic form, a complex structure, or a Riemannian metric), and by "analysis" we will broadly understand function spaces on M, sections of line bundles, operators, norms, estimates, and so on. We will be looking for invariants, or asking to what extent "analysis" determines "geometry" (or whether one can see how the geometric properties of M manifest in "analysis" on M). A completely naive example would be to assign to a subset S of M its characteristic function χ_S and to observe that if $\chi_{S_1} \neq \chi_{S_2}$, then $S_1 \neq S_2$.

4.3.1 Preliminaries

Let $L \to M$ be a positive holomorphic hermitian line bundle on a compact complex m-dimensional manifold $M (m \in \mathbb{N})$. It is ample. Assume L is very ample. Denote by ∇ the Chern connection on L. The 2-form $\omega = i\mathrm{Curv}(\nabla)$ is a Kähler form on M, where $\mathrm{Curv}(\nabla)$ denotes the curvature of the connection ∇. (Or, alternatively, we could have stated that for an integral Kähler manifold (M, ω) such line bundle exists.) Let k be a positive integer. For a unit vector v in the finite-dimensional Hilbert space

$$H^0(M, L^k) \otimes H^0(M, L^k) \tag{4.26}$$

we can calculate its entanglement entropy $E_k(v)$. The expression for it is the formula for $E(v)$, either Equation 2.1 or 2.2. Here $H^0(M, L^k)$ is the space of holomorphic sections of the k-th tensor power of L, regarded as a (complex) Hilbert space, with the inner product induced by the pointwise hermitian metric on L. Let us also denote by S_k the unit sphere in the Hilbert space (4.26):

$$S_k = \{v \in H^0(M, L^k) \otimes H^0(M, L^k) \mid \|v\| = 1\}.$$

We also note an isomorphism of Hilbert spaces:

$$H^0(M, L^k) \otimes H^0(M, L^k) \simeq H^0(M \times M, L^k \boxtimes L^k). \tag{4.27}$$

Here $L^k \boxtimes L^k \to M \times M$ is the holomorphic line bundle

$$\pi_1^*(L^{\otimes k}) \otimes \pi_2^*(L^{\otimes k}),$$

where $\pi_m : M \times M \to M$, $m \in \{1, 2\}$, are the projections onto the first and second factor respectively. The hermitian metric on L induces a hermitian metric on $L^k \boxtimes L^k$. For a subset $\Lambda \subset M$, we will denote by R_k the restriction operator defined by

$$s \mapsto s\Big|_{\Lambda}$$

for $s \in H^0(M \times M, L^k \boxtimes L^k)$. Due to (4.27), we will also write $R_k(v)$ for vectors v in (4.26), not to complicate notation.

We will aspire to assign to a subset of M (say, Λ), some analytic construct built from the Hilbert space (4.26) via the quantum information concepts, such as entanglement entropy, negativity or entanglement of formation. As a start, on this note, we will consider $M = \mathbb{CP}^1$ with the Fubini-Study metric, L the hyperplane bundle, $\Lambda = S^1$ embedded antidiagonally as specified below, and we will prove the theorem below, with the intent to generalize this statement later to other M and Λ and to use Theorem 4.3.1 and its proof as a guiding example for the general case.

Theorem 4.3.1 ([BSaikia23]). *Let $M = \mathbb{CP}^1$ equipped with the Fubini-Study metric and let $L \to M$ be the hyperplane bundle, with the standard hermitian metric. Let $\Lambda \subset (M - \{[1 : 0]\}) \times (M - \{[1 : 0]\})$ be defined by*

$$\Lambda = \{(z, w) \in \mathbb{C} \times \mathbb{C} \mid z = e^{it}; w = e^{-it}; 0 \leq t \leq 2\pi\},$$

where

$$M - \{[1 : 0]\} \simeq \mathbb{C}$$

is the affine chart

$$\{[z_0 : z_1] \in \mathbb{CP}^1 \mid z_1 \neq 0\}$$

with the affine coordinate $z = \frac{z_0}{z_1}$. Let $\{e_j\}$ be the standard orthonormal basis in $H^0(M, L^k)$:

$$e_j = \sqrt{\frac{(k+1)!}{j!(k-j)!}}\, z^j$$

$j \in \{0, 1, 2, ..., k\}$. Let for each $k \in \mathbb{N}$,

$$W_k = \ker(R_k) \cap \operatorname{span}\{e_j \otimes e_j \mid j = 0, 1, ..., k\}.$$

Then

(a) $\ker(R_1)$ *is the span of* $\frac{1}{\sqrt{2}}(e_0 \otimes e_0 - e_1 \otimes e_1)$

(b) The sequence of vectors

$$b_k = \frac{1}{\sqrt{1+k^2}}(e_1 \otimes e_1 - k e_0 \otimes e_0)$$

is in $\ker R_k$ *for each* $k = 1, 2, 3, \ldots$*, and their entanglement entropy is*

$$E_k(b_k) = -\frac{1}{1+k^2}\ln\frac{1}{1+k^2} - \frac{k^2}{1+k^2}\ln\frac{k^2}{1+k^2}. \tag{4.28}$$

(c) The sequence of vectors

$$c_k = \frac{1}{\sqrt{2}}(e_0 \otimes e_0 - e_k \otimes e_k)$$

is in $\ker R_k$ *for each* $k = 1, 2, 3, \ldots$*, and their entanglement entropy is* $E_k(c_k) = \ln 2$ *for every* k*.*
(d) The linear subspace W_k *is* k*-dimensional. For all odd* k*, there is a vector of maximum Schmidt rank in* W_k *such that its entanglement entropy is* $\ln(k+1)$*. For each even natural number* k*,* W_k *contains a vector whose entanglement entropy is* $\ln k$*.*
(e) The endomorphism of the Hilbert space $H^0(M \times M, L \boxtimes L)$ *defined by the orthogonal projection onto* $\ker(R_1)$ *is the Berezin-Toeplitz operator* $T_f^{(1)}$ *with the symbol* $f \in C^\infty(M \times M)$ *given by*

$$f(z_0, z_1; w_0, w_1) = \frac{9}{2}\frac{(z_0 w_0 - z_1 w_1)(\bar{z}_0 \bar{w}_0 - \bar{z}_1 \bar{w}_1)}{(|z_0|^2 + |z_1|^2)(|w_0|^2 + |w_1|^2)} - 2.$$

Remark 4.3.2. For $k \in \mathbb{N}$ and a smooth function $F : M \times M \to \mathbb{C}$, the Berezin-Toeplitz operator $T_F^{(k)}$ with the symbol F, is an endomorphism of the Hilbert space $H^0(M \times M, L^k \boxtimes L^k)$ defined by

$$T_F^{(k)} : s \mapsto \Pi_k(Fs)$$

where $\Pi_k : L^2(M \times M, L^k \boxtimes L^k) \to H^0(M \times M, L^k \boxtimes L^k)$ is the orthogonal projection from the space of L^2 sections of the line bundle $L^k \boxtimes L^k$ onto the closed subspace of holomorphic sections.

Comments.

In Theorem 4.3.1(b), the sequence of vectors b_k is asymptotic to $-e_0 \otimes e_0$. Accordingly, $E_k(b_k) \to 0$ as $k \to \infty$.

In Theorem 4.3.1(c), the vector c_k represents a Bell state for each k.

Theorem 4.3.1(d) shows that the value of E_k on W_k reaches the maximum possible value. Generally, it does not have to be the case (for example, the value of entanglement entropy on a 1-dimensional subspace spanned by a decomposable vector is zero, or, as another example, if we consider the 2-dimensional subspace spanned by $e_0 \otimes e_0$ and $e_0 \otimes e_1$, every vector in this subspace is decomposable and its entanglement entropy is zero).

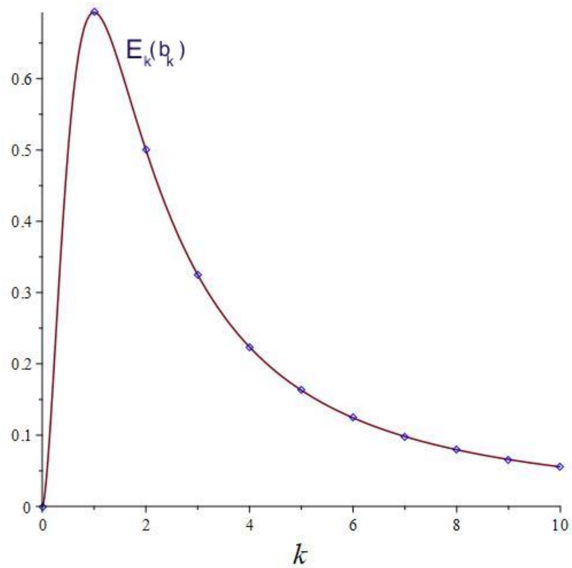


Figure 4.1: The values of (4.28) for $1 \leq k \leq 10$.

If we realize the linear operators that are relevant to the quantum information theory, as Toeplitz operators, then we would be able to use the asymptotic ($k \to \infty$) results about the spectrum of Toeplitz operators to make conclusions about the semiclassical asymptotics of entanglement. Part (e) is a demonstration of the first part of this statement in the setting of Theorem 4.3.1.

4.3.2 Proof of Theorem 4.3.1

Proof of (a). We observe:

$$ae_0 \otimes e_0 + be_0 \otimes e_1 + ce_1 \otimes e_0 + de_1 \otimes e_1$$

is in $\ker(R_1)$ if and only if $a = d$ and $b = c = 0$. The statement follows.

Proof of (b) and (c). We observe that, restricted to Λ,

$$e_j \otimes e_j = \binom{k}{j} e_0 \otimes e_0 \tag{4.29}$$

for all $0 \leq j \leq k$. Suppose a vector v in (4.26) is of the form

$$v = \sum_j a_j e_j \otimes e_j.$$

Then, the condition for v to be in $\ker(R_k)$ is

$$\sum_j \binom{k}{j} a_j = 0.$$

We see that the vectors b_k and c_k satisfy this condition and therefore are in $\ker(R_k)$ for all k. The values of their entanglement entropy are obtained from their Schmidt coefficients via 2.2.

Proof of (d). The first claim follows from (4.29) and the fact that $e_i \otimes e_j \notin W_k$ for $i \neq j$. Now, suppose $v = \sum_{j=0}^{k} a_j e_j \otimes e_j$ is of norm 1, i.e.

$$\sum_{j=0}^{k} |a_j|^2 = 1. \tag{4.30}$$

Suppose v is in W_k and it is of maximal Schmidt rank. It is equivalent to

$$\sum_{j=0}^{k} \binom{k}{j} a_j = 0 \tag{4.31}$$

(because it is in $\ker(R_k)$), and $a_j \neq 0$ for all j. By a direct calculation, we conclude that the entanglement entropy

$$E_k(v) = -\sum_{j=0}^{k} |a_j|^2 \ln\left(|a_j|^2\right). \tag{4.32}$$

Write $a_j = x_j + iy_j$ for $1 \leq j \leq k$. The right hand side of Equation (4.32) is a function of $2k$ real variables (using Equation (4.30)) :

$$f(x,y) = -\left(1 - \sum_{j=1}^{k}(x_j^2 + y_j^2)\right) \ln\left(1 - \sum_{j=1}^{k}(x_j^2 + y_j^2)\right) - \sum_{j=1}^{k}(x_j^2 + y_j^2) \ln\left(x_j^2 + y_j^2\right).$$

It is S^1-invariant with respect to the circle action on the Hilbert space in Equation 4.26 (see Proposition 2.4.13). To look for the critical points, we consider the equation

$$\nabla f = 0$$

that leads to

$$|a_1|^2 = ... = |a_k|^2 = 1 - \sum_{j=1}^{k} |a_j|^2.$$

When k is odd, there is a solution to these equations that also satisfies Equation (4.31), with

$|a_j|^2 = \frac{1}{k+1}$ for all $1 \leq j \leq k$ and such that

$$a_j = -a_{k-j}$$

for all $0 \leq j \leq k$. When k is even, we can set $a_{k/2} = 0$ and choose a_j for all $j \neq \frac{k}{2}$ so that $|a_j|^2 = \frac{1}{k}$ and $a_j = -a_{k-j}$. The value of E_k is now obtained from (4.32).
Proof of (e). The conclusion is obtained by a direct calculation: we apply the matrix of the orthogonal projection onto $\ker(R_1)$ and the linear operator $T_f^{(1)}$ to the four basis vectors.

4.4 Restrictions of holomorphic sections to products

In this section, we associate quantum states with subsets of a product of two compact connected Kähler manifolds M_1 and M_2, using the map that restricts holomorphic sections of the quantum line bundle over the product of the two Kähler manifolds to the subset. We present a description of the kernel of this restriction map when the subset is a finite union of products, which shows that the quantum state associated with such a subset is separable. Finally, for every pure state and certain mixed state, we construct subsets of $M_1 \times M_2$ such that the states associated with these subsets are the original states, to begin with. The work presented in this section is the contents of the paper [Saikia24], modified slightly to fit the context.

4.4.1 Motivation

The study of the interplay between geometric structures and analytic objects arising from these structures emerges in many different ways in mathematics. For instance, in [BPU95], the authors constructed, for each k, a holomorphic section of $H^0(M, L^k)$ associated to a Lagrangian submanifold Λ of a compact Kähler manifold M and studied various aspects of these states, for example, the authors computed large k asymptotics of $\langle Tu_k, u_k\rangle$ for a Toeplitz operator T and showed these states concentrate on Λ. Various similar studies have been made with the "geometry vs analysis" theme for Lagrangian submanifolds [BW00; DP06; Pao08] and isotropic submanifolds [GUW16] of a compact Kähler manifold.

Exploring the correspondence between submanifolds (or, more generally, subsets with nice properties) of Kähler manifolds and the corresponding states associated in different ways has appeared in many different contexts. In [BP17], the authors considered a compact connected complex manifold M and associated a sequence of quantum states with the Lagrangian submanifold M embedded anti-diagonally inside $M \times M$. The authors showed that this sequence of pure states is a sequence of maximally entangled states. In [BW23], the authors considered a submanifold Λ of the product of two integral compact Kähler manifolds M_1 and M_2 having pre-quantum line bundle L_1 and L_2. For every $N \in \mathbb{N}$, using the map that restricts global holomorphic sections of $L_1^N \boxtimes L_2^N \to M_1 \times M_2$, the authors associated a sequence of mixed states ρ_N with Λ and showed that when Λ is a product submanifold the states in this sequence are not entangled. Motivated by [BW23], in this section, we come up with a different recipe to associate quantum states with subsets of $M_1 \times M_2$ and study the entanglement properties of these newly associated states when we have a product subset. More generally, we showed that when Λ is the union of finitely many product subsets, the states are not entangled.

4.4.2 Associating quantum states

In this section, our quantum Hilbert space is $H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N)$. For notational convenience, from now onwards we denote $\mathcal{H}_A = H^0(M_1, L_1^N)$ and $\mathcal{H}_B = H^0(M_2, L_2^N)$ so that our quantum Hilbert space $H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N)$ is isomorphic to $\mathcal{H}_A \otimes \mathcal{H}_B$.

For $j \in \{1, 2\}$, let Λ_j be a non-empty subset of M_j. Let E_j be the total space of the line bundles L_j^N with the projection map $p_j : E_j \to M_j$ and W_j denote the vector space $\{s : \Lambda_j \to E_j \mid p_j \circ s(z) = z \text{ for all } z \in \Lambda_j\}$ (that means W_j is the space of sections restricted to Λ_j but these sections do not have any additional structure like smoothness etc, since we have not assumed any structure on Λ_j to keep our results in more general setup). Let $\mathcal{R}_{\Lambda_j} : H^0(M_j, L_j^N) \to W_j$ be the linear map

$$s \mapsto s\Big|_{\Lambda_j}$$

that restricts a holomorphic section of $L_j^N \to M_j$ to the subset $\Lambda_j \subset M_j$. Similarly, let E be the total space of line bundle $L_1^N \boxtimes L_2^N$ and $p : E \to M_1 \times M_2$ be the projection map. For a subset Λ of $M_1 \times M_2$, let us denote $\mathcal{R}_\Lambda : H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N) \to W$ be the map

$$\mathcal{R}_\Lambda(s) = s\Big|_{\Lambda_j} \tag{4.33}$$

that restricts a holomorphic section of $L_1^N \boxtimes L_2^N \to M_1 \times M_2$ to the subset $\Lambda \subset M_1 \times M_2$ where $W = \{s : \Lambda \to E \mid p \circ s(z) = z \text{ for all } z \in \Lambda\}$. We use the same notation $\mathcal{R}_\Lambda$ to mean all these three restriction maps, but we pick the appropriate one based on whether Λ is a subset of M_1, M_2 or $M_1 \times M_2$. We hope that it does not create any confusion.

Notation 4.4.1. *For a subset $\Lambda \subset M_1 \times M_2$, let $\Pi_\Lambda^{\ker}$ and $\Pi_\Lambda^{\ker^\perp}$ be the orthogonal projections onto* $\ker(\mathcal{R}_\Lambda)$ *and* $\ker(\mathcal{R}_\Lambda)^\perp$ *respectively. We denote $\rho_\Lambda^{\ker} = \frac{1}{\operatorname{tr}(\Pi_\Lambda^{\ker})}\Pi_\Lambda^{\ker}$ and $\rho_\Lambda^{\ker^\perp} = \frac{1}{\operatorname{tr}(\Pi_\Lambda^{\ker^\perp})}\Pi_\Lambda^{\ker^\perp}$ (whenever the trace is not zero). Whenever the trace is zero, we define the corresponding $\rho_\Lambda^{\ker}$ or $\rho_\Lambda^{\ker^\perp}$ as the zero operator.*

We associate the states $\rho_\Lambda^{\ker}$ and $\rho_\Lambda^{\ker^\perp}$ with the subset Λ of $M_1 \times M_2$. Note that $\ker(\mathcal{R}_\Lambda)$ or $\ker(\mathcal{R}_\Lambda)^\perp$ can be zero sometimes and in that case the corresponding operator $\rho_\Lambda^{\ker}$ or $\rho_\Lambda^{\ker^\perp}$ is technically not a state, because of it being the zero operator, the trace condition on states is not satisfied. However, at least one of $\rho_\Lambda^{\ker}$ or $\rho_\Lambda^{\ker^\perp}$ is a state. In this section, we ignore this technicality and say that both of them are states, even when one of the operators is zero.

Observation 4.4.2. *Note that the state $\rho_\Lambda^{\ker}$ is separable if and only if* $\ker(\mathcal{R}_\Lambda)$ *has an orthonormal basis of decomposable vectors. The subspace* $\ker(\mathcal{R}_\Lambda)^\perp$ *has an orthonormal basis of decomposable vectors if and only if* $\ker(\mathcal{R}_\Lambda)$ *has an orthonormal basis of decomposable vectors. Finally, the state $\rho_\Lambda^{\ker^\perp}$ is separable if and only if* $\ker(\mathcal{R}_\Lambda)^\perp$ *has an orthonormal basis of decomposable vectors. Therefore, the state $\rho_\Lambda^{\ker}$ is separable if and only if the state $\rho_\Lambda^{\ker^\perp}$ is separable.*

In [BW23], the authors considered a submanifold Λ of $M_1 \times M_2$ and considered the restriction map $\mathcal{R}_\Lambda : H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N) \to L^2(\Lambda, L_1^N \boxtimes L_2^N|_\Lambda)$. In their setup, due to the additional smooth structure on Λ, the integrals over Λ with respect to the measure μ are defined and in fact, the codomain becomes the space of L^2 sections. Using $\mathcal{R}_\Lambda$ and the inner product on the codomain of this map, the authors associated certain states with Λ and proved that when $\Lambda = \Lambda_1 \times \Lambda_2$ is a product submanifold then these states are separable. This motivated us to associate states a little differently and check if similar properties can be observed. Due to the use of the inner product on the codomain, the authors considered nice subsets over which we can integrate, such as submanifolds. Since the states $\rho_\Lambda^{\ker}$ and $\rho_\Lambda^{\ker^\perp}$ we associated in our setup are directly linked to subspaces of $H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N)$ and we are not using any additional structure of the co-domain other than it being a vector space, we don't restrict ourselves to submanifolds and take arbitrary subsets.

In an attempt to investigate similar properties of these newly associated states $\rho_\Lambda^{\ker}$ and $\rho_\Lambda^{\ker^\perp}$ with respect to product submanifolds, we proof a result (Proposition 4.4.6) that provides a nice description of the kernel of the restriction map. Our main result Theorem 4.4.7 extends Proposition 4.4.6 to provide a description of the kernel of the restriction map to even more generality, to any finite union of products. As a corollary of 4.4.7, we get that our states are also separable for product submanifolds. This is analogous to a similar result in [BW23]. In fact, we get a more general result that says the states are separable if Λ is a finite union of products.

In Section 4.4.4, we ask the question whether, for every state σ on $\mathcal{H}_A \otimes \mathcal{H}_B$, there exists a subset Λ of $M_1 \times M_2$ such that $\rho_\Lambda^{\ker} = \sigma$. As our constructed state is an orthogonal projection, clearly if σ is not an orthogonal projection, then the answer is no. We partially answer the question for quantum states that are orthogonal projections. The solution is straightforward for pure states by the projective embedding of $M_1 \times M_2$ using the quantum line bundle. This also affirmatively says that the states $\rho_\Lambda^{\ker}$ and $\rho_\Lambda^{\ker^\perp}$ associated this way with subsets are not always separable. For mixed states having a particular property, we use coherent states and the covariant symbol of σ to construct the subset.

4.4.3 Separability and products

The purpose of this section is to prove that $\rho_\Lambda^{\ker}$ and $\rho_\Lambda^{\ker^\perp}$ are separable when $\Lambda \subset M_1 \times M_2$ is a finite union of product. For that purpose, we show that the range space of the states contains an orthonormal basis consisting of only decomposable vectors. If Λ is a union of products, then we present a description of $\ker(\mathcal{R}_\Lambda)$ as a direct sum of Hilbert spaces each of which is a tensor product of Hilbert spaces that are orthogonal to one another. We get this in a few steps. First, we consider $\Lambda = \Lambda_1 \times \Lambda_2$ where one of Λ_1 or Λ_2 is a singleton set and prove Proposition 4.4.3. We use Proposition 4.4.3 to generalize it for products without the restriction of Λ_1 or Λ_2 being singleton to get Proposition 4.4.6.

Proposition 4.4.3 ([Saikia24])**.** *For $j \in \{1,2\}$, let Λ_j be a non-empty subset of M_j. If either Λ_1 or Λ_2 is a singleton set, then*

$$\ker(\mathcal{R}_{\Lambda_1\times\Lambda_2}) = A_1 \oplus A_2,$$

where

$$\begin{aligned} A_1 &= \mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2}) \\ A_2 &= \ker(\mathcal{R}_{\Lambda_1}) \otimes \ker(\mathcal{R}_{\Lambda_2})^\perp. \end{aligned}$$

We deduce that $\ker(\mathcal{R}_{\Lambda_1\times\Lambda_2})^\perp = \ker(\mathcal{R}_{\Lambda_1})^\perp \otimes \ker(\mathcal{R}_{\Lambda_2})^\perp$.

Proof. Suppose $\Lambda_2 = \{y\}$ be singleton.
Let $(x,y) \in \Lambda_1 \times \Lambda_2$ and $s \in [\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})] \oplus [\ker(\mathcal{R}_{\Lambda_1}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^\perp]$. Then for some $n_1, n_2 \geq 1$, we can write

$$s = \sum_{j=1}^{n_1} u_j \otimes v_j + \sum_{j=1}^{n_2} u'_j \otimes v'_j$$

where $v_j \in \ker(\mathcal{R}_{\Lambda_2})$ for all $j \in \{1, ..., n_1\}$ and $u'_j \in \ker(\mathcal{R}_{\Lambda_1})$ for all $j \in \{1, ..., n_2\}$. Take a trivializing open cover of the line bundle $L_1^N \boxtimes L_2^N \to M_1 \times M_2$. Then in an open neighbourhood of (x,y) in the trivializing cover, we get that $v_j(y) = 0$ for all $j \in \{1, ..., n_1\}$ and $u'_j(x) = 0$ for all $j \in \{1, ..., n_2\}$. Therefore,

$$s(x,y) = \sum_{j=1}^{n_1} u_j(x) \otimes v_j(y) + \sum_{j=1}^{n_2} u'_j(x) \otimes v'_j(y) = 0.$$

We get that $s \in \ker(\mathcal{R}_{\Lambda_1\times\Lambda_2})$. Therefore, $A_1 \oplus A_2 \subset \ker(\mathcal{R}_{\Lambda_1\times\Lambda_2})$.

For the inclusion from the other side, let $s \in \ker(\mathcal{R}_{\Lambda_1\times\Lambda_2})$. Then there exists $d \in \mathbb{N}$ such that we can write $s = \sum_{j=1}^{d} u_j \otimes v_j$ where $u_j \in \mathcal{H}_A$ and $v_j \in \mathcal{H}_B$ are non-zero. If for some $j \in \{1, ..., d\}$, we have $v_j \in \ker(\mathcal{R}_{\Lambda_2})$, then $u_j \otimes v_j \in \mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})$. So we assume that $v_j \in (\ker(\mathcal{R}_{\Lambda_2}))^\perp$ for all $j \in \{1, ..., d\}$, therefore $v_j(y) \neq 0$ for all $j \in \{1, ..., d\}$.

Take a trivializing open cover of the line bundle $L_2^N \to M_2$. In an open neighbourhood of y in the trivializing open cover, each of the sections v_j is given by a map with co-domain $\mathbb{C}$. Therefore $\{v_j(y) : j \in \{1, 2, ..., d\}\}$ is a set of non-zero complex numbers. There exists non-zero $\lambda_2, ..., \lambda_d \in \mathbb{C}$ such that $v_j(y) = \lambda_j v_1(y)$ for $j \in \{2, ..., d\}$, i.e. for each j, we have $v_j - \lambda_j v_1 \in \ker(\mathcal{R}_{\Lambda_2})$. Now, let $x \in \Lambda_1$. Take a trivializing open cover of the line bundle $L_1^N \to M_1$. In an open neighbourhood of x in the trivializing open cover, each of the sections u_j is given by a map with co-domain $\mathbb{C}$. By assumption, the section s vanishes at (x, y), therefore we have

$$\begin{aligned} \sum_{j=1}^{d} u_j(x) v_j(y) = 0 \\ \Rightarrow u_1(x) + \sum_{j=2}^{d} \lambda_j u_j(x) = 0 \\ \Rightarrow u_1 + \sum_{j=2}^{d} \lambda_j u_j \in \ker(\mathcal{R}_{\Lambda_1}) \end{aligned}$$

We can rearrange the terms to write s in the following way:

$$s = \sum_{j=1}^{d} u_j \otimes v_j = (u_1 + \sum_{j=2}^{d} \lambda_j u_j) \otimes v_1 + \sum_{j=2}^{s} u_j \otimes (v_j - \lambda_j v_1).$$

Note that the first term in the above expression is an element of $\ker(\mathcal{R}_{\Lambda_1}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}$ and the second term is an element of $\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})$. This finishes the proof of $\ker(\mathcal{R}_{\Lambda_1 \times \Lambda_2}) \subset A_1 \oplus A_2$. Hence $\ker(\mathcal{R}_{\Lambda_1 \times \Lambda_2}) = [\ker(\mathcal{R}_{\Lambda_1}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}] \oplus [\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})]$.

When Λ_1 is a singleton set, we can use a similar argument (with roles of Λ_1 and Λ_2 reversed) to show that $\ker(\mathcal{R}_{\Lambda_1 \times \Lambda_2}) = [\ker(\mathcal{R}_{\Lambda_1}) \otimes \mathcal{H}_B] \oplus [(\ker(\mathcal{R}_{\Lambda_1}))^{\perp} \otimes \ker(\mathcal{R}_{\Lambda_2})]$ which is equal to the space $[\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})] \oplus [\ker(\mathcal{R}_{\Lambda_1}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}]$.

Finally, we note that $A_1 \oplus A_2 \oplus [\ker(\mathcal{R}_{\Lambda_1})^{\perp} \otimes \ker(\mathcal{R}_{\Lambda_2})^{\perp}] = \mathcal{H}_A \otimes \mathcal{H}_B$ and $\langle u, v \rangle = 0$ for any $u \in \ker(\mathcal{R}_{\Lambda_1})^{\perp} \otimes \ker(\mathcal{R}_{\Lambda_2})^{\perp}$ and $v \in A_1 \oplus A_2$, therefore $\ker(\mathcal{R}_{\Lambda_1 \times \Lambda_2})^{\perp} = \ker(\mathcal{R}_{\Lambda_1})^{\perp} \otimes \ker(\mathcal{R}_{\Lambda_2})^{\perp}$. □

Now that we have our description when one of the subsets involved is a point, our idea is to write $\Lambda_1 \times \Lambda_2$ as the union $\bigcup_{x \in \Lambda_1} \{x\} \times \Lambda_2$, so that we can use the above to get $\ker(\mathcal{R}_{\Lambda_1 \times \Lambda_2})$ as intersections of subspaces. This allows us to extend the result to arbitrary Λ_1 and Λ_2. We keep in mind that the index set over which we have the intersection is an arbitrary index set and we need the direct sum to distribute over the intersection. This is not always true, not even for a finite index set (as an example take $V = \mathbb{C}^2$, $H_1 = \text{span}\{(1, 0)\}$, $H_2 = \text{span}\{(0, 1)\}$ and $H_3 = \text{span}\{(1, 1)\}$, then $(H_1 \oplus H_2) \cap (H_1 \oplus H_3) = \mathbb{C}^2$ but $H_1 \oplus (H_2 \cap H_3) = H_1 \neq \mathbb{C}^2$). However, if we put further conditions, which are satisfied in our case, then the direct sum distributes over the intersection. We provide a short proof of this fact here. The condition to make this distributive property hold is a crucial part that allows us to extend Proposition 4.4.3. Further, we also need the distributive property of tensor products over intersections, which is true for vector spaces. We state these two lemmas here.

Lemma 4.4.4. *Let $\mathcal{I}$ be an arbitrary index set. Let $\{V_j\}_{j\in\mathcal{I}}$ and $\{W_j\}_{j\in\mathcal{I}}$ be two sets of subspaces of a vector space X. Let there exist two subspaces V and W of X such that $\sum_{j\in\mathcal{I}} V_j \subset V$, $\sum_{j\in\mathcal{I}} W_j \subset W$ and $W \cap V = \{0\}$, then*

$$\bigcap_{j\in\mathcal{I}}(W_j \oplus V_j) = \left(\bigcap_{j\in\mathcal{I}} W_j\right) \oplus \left(\bigcap_{j\in\mathcal{I}} V_j\right).$$

Proof. It is straightforward to verify that $\left(\bigcap_{j\in\mathcal{I}} W_j\right) \oplus \left(\bigcap_{j\in\mathcal{I}} V_j\right) \subset \bigcap_{j\in\mathcal{I}}(W_j \oplus V_j)$. For the converse, let $u \in \bigcap_{j\in\mathcal{I}}(W_j \oplus V_j)$. Then for each $j \in \mathcal{I}$, there exists unique $w_j \in W_j$ and $v_j \in V_j$ such that $u = w_j \oplus v_j$. Due to the hypothesis $V \cap W = \{0\}$, we have a well-defined subspace $V \oplus W$ of X and we have $\bigcap_{j\in\mathcal{I}}(W_j \oplus V_j) \subset W \oplus V$. So, there exists unique $w \in W$ and $v \in V$ such that $u = w \oplus v$. For each j, since $w_j \in W_j \subset W$, $v_j \in V_j \subset V$ and $u = w_j \oplus v_j$, so by the uniqueness of the decomposition, we must have $w = w_j$ and $v = v_j$, i.e. $w \in W_j$ and $v \in V_j$ for all $j \in \mathcal{I}$, i.e. $w \in \bigcap_{j\in\mathcal{I}} W_j$ and $v \in \bigcap_{j\in\mathcal{I}} V_j$. Therefore, $u = w \oplus v \in \left(\bigcap_{j\in\mathcal{I}} W_j\right) \oplus \left(\bigcap_{j\in\mathcal{I}} V_j\right)$. □

Lemma 4.4.5. *Let $\mathcal{I}$ be an arbitrary index set and $\{V_j\}_{j\in\mathcal{I}}$ be a set of subspaces of a vector space V. For an arbitrary vector space W, we have*

$$\bigcap_{j\in\mathcal{I}}(V_j \otimes W) = \left(\bigcap_{j\in\mathcal{I}} V_j\right) \otimes W.$$

Proof. It is straightforward to verify that $\left(\bigcap_{j\in\mathcal{I}} V_j\right) \otimes W \subset \bigcap_{j\in\mathcal{I}}(V_j \otimes W)$. For the converse, let $u \in \bigcap_{i\in\mathcal{I}}(V_i \otimes W)$. Let $j_0 \in \mathcal{I}$ be fixed. As $u \in V_{j_0} \otimes W$, so there exists $\{v_1, ..., v_{n_0}\} \subset V_{j_0}$ and a linearly independent set $\{w_1, ..., w_{n_0}\}$ in W such that $u = \sum_{l=1}^{n_0} v_l \otimes w_l$. Now for any $j \in \mathcal{I}$, with $j \neq j_0$, again since $u \in V_j \otimes W$, there exists $\{v_{j1}, ..., v_{jm_j}\} \subset V_j$ and a set of vectors $\{z_{j1}, ..., z_{jm_j}\} \subset W$ such that $u = \sum_{l=1}^{m_j} v_{jl} \otimes z_{jl}$. Let $W_j = \operatorname{span}\{w_1, ..., w_{n_0}, z_{j1}, ..., z_{jm_j}\}$, then clearly $u \in V_j \otimes W_j$. We extend $\{w_1, ..., w_{n_0}\}$ to a basis $\{w_1, ..., w_{n_j}\}$ of W_j. Then there exists $\{x_{j1}, ..., x_{jn_j}\} \subset V_j$ such that $u = \sum_{l=1}^{n_j} x_{jl} \otimes w_l$.

Now we observe that $\sum_{l=1}^{n_0} v_l \otimes w_l = u = \sum_{l=1}^{n_j} x_{jl} \otimes w_l$, i.e. $\sum_{l=1}^{n_0}(v_l - x_{jl}) \otimes w_l + \sum_{l=n_0+1}^{n_j}(-x_{jl}) \otimes w_l = 0$. Using the fact that $\{w_1, ..., w_{n_j}\}$ is a linearly independent set, we get that for each $l \in \{1, ..., n_0\}$ we have $v_l = x_{jl} \in V_j$. But j is an arbitrary element of the index set $\mathcal{I}$, therefore for each $l \in \{1, ..., n_0\}$, $v_l \in \bigcap_{j\in\mathcal{I}} V_j$, i.e. $u = \sum_{l=1}^{n} v_l \otimes w_l \in \left(\bigcap_{j\in\mathcal{I}} V_j\right) \otimes W$ and we are done. □

We shall use Proposition 4.4.3 and the two lemmas to prove the following proposition.

Proposition 4.4.6 ([Saikia24])**.** *For $j \in \{1,2\}$, let Λ_j be a non-empty subset of M_j. Then,*

$$\ker(\mathcal{R}_{\Lambda_1\times\Lambda_2}) = A_1 \oplus A_2,$$

where

$$\begin{aligned} A_1 &= \mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2}) \\ A_2 &= \ker(\mathcal{R}_{\Lambda_1}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}. \end{aligned}$$

We deduce that $\ker(\mathcal{R}_{\Lambda_1\times\Lambda_2})^{\perp} = \ker(\mathcal{R}_{\Lambda_1})^{\perp} \otimes \ker(\mathcal{R}_{\Lambda_2})^{\perp}$.

Proof. Let $x \in \Lambda_1$. Using Proposition 4.4.3, we have

$$\ker(\mathcal{R}_{\{x\}\times\Lambda_2}) = [\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})] \oplus [\ker(\mathcal{R}_{\{x\}}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}].$$

For any $s \in \mathcal{H}_A \otimes \mathcal{H}_B$,

$$s \in \ker(\mathcal{R}_{\Lambda_1\times\Lambda_2}) \iff s(x,y) = 0 \text{ for all } x \in \Lambda_1, y \in \Lambda_2 \iff s \in \bigcap_{x\in\Lambda_1} \ker(\mathcal{R}_{\{x\}\times\Lambda_2})$$

Therefore, $\ker(\mathcal{R}_{\Lambda_1\times\Lambda_2}) = \bigcap_{x\in\Lambda_1} \ker(\mathcal{R}_{\{x\}\times\Lambda_2})$. Similarly, it is easy to verify that $\ker(\mathcal{R}_{\Lambda_1}) = \bigcap_{x\in\Lambda_1} \ker(\mathcal{R}_{\{x\}})$. We notice that

$$\sum_{x\in\Lambda_1} (\ker(\mathcal{R}_{\{x\}}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}) \subset \mathcal{H}_A \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}$$

and $(\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})) \cap (\mathcal{H}_A \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}) = \{0\}$, so Lemma 4.4.4 can be applied to get:

$$\begin{aligned} \ker(\mathcal{R}_{\Lambda_1\times\Lambda_2}) &= \bigcap_{x\in\Lambda_1} \ker(\mathcal{R}_{\{x\}\times\Lambda_2}) \\ &= \bigcap_{x\in\Lambda_1} [(\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})) \oplus (\ker(\mathcal{R}_{\{x\}}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp})] \\ &= [\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})] \oplus \left[\bigcap_{x\in\Lambda_1} (\ker(\mathcal{R}_{\{x\}}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp})\right] \quad \text{(using Lemma 4.4.4)} \\ &= [\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})] \oplus \left[\left(\bigcap_{x\in\Lambda_1} \ker(\mathcal{R}_{\{x\}})\right) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}\right] \quad \text{(using Lemma 4.4.5)} \\ &= [\mathcal{H}_A \otimes \ker(\mathcal{R}_{\Lambda_2})] \oplus [\ker(\mathcal{R}_{\Lambda_1}) \otimes (\ker(\mathcal{R}_{\Lambda_2}))^{\perp}] \end{aligned}$$

□

We try to recognize the pattern in the product case to extend it to a finite union of products. For this purpose, if we have $\Lambda = \bigcup_{j\in[n]}(U_j \times V_j)$, we apply Proposition 4.4.6 to decompose the kernels of each of the products $U_j \times V_j$ in the union cleverly to arrive at a direct sum decomposition indexed by the subsets of $\{1, 2, ..., n\}$.

Theorem 4.4.7 ([Saikia24])**.** *Let $U_1, U_2, ..., U_n$ be non-empty subsets of M_1 and $V_1, V_2, ..., V_n$ be non-empty subsets of M_2. Denote $[n] = \{1, 2, , ..., n\}$. Let $\Lambda = \bigcup_{j\in[n]}(U_j \times V_j)$. Then*

$$\ker(\mathcal{R}_\Lambda) = \bigoplus_{S\subset[n]} \left(H_S^{(n)} \otimes K_S^{(n)}\right)$$

where

$$H_S^{(n)} = \begin{cases} \mathcal{H}_A & \text{if } S = \emptyset \\ \bigcap_{j\in S} \ker(\mathcal{R}_{U_j}) & \text{otherwise} \end{cases}$$

and $K_S^{(n)} = \bigcap_{j=1}^n W_{S,j}$ where

$$W_{S,j} = \begin{cases} \ker(\mathcal{R}_{V_j})^\perp & \text{if } j \in S \\ \ker(\mathcal{R}_{V_j}) & \text{if } j \notin S. \end{cases}$$

Proof. We shall use induction on n. The base case $n = 1$ is true by Proposition 4.4.6.
Suppose the statement is true for some $n \in \mathbb{N}$. Denote $\Lambda' = \bigcup_{j\in[n]}(U_j \times V_j)$ and $\Lambda = \bigcup_{j\in[n+1]}(U_j \times V_j)$. Then by the induction hypothesis, we have

$$\ker(\mathcal{R}_{\Lambda'}) = \bigoplus_{S\subset[n]} \left(H_S^{(n)} \otimes K_S^{(n)}\right). \tag{4.34}$$

Using Proposition 4.4.6, we have

$$\ker(\mathcal{R}_{U_{n+1}\times V_{n+1}}) = [\mathcal{H}_A \otimes \ker(\mathcal{R}_{V_{n+1}})] \oplus [\ker(\mathcal{R}_{U_{n+1}}) \otimes (\ker(\mathcal{R}_{V_{n+1}}))^\perp]. \tag{4.35}$$

Since $\Lambda = \Lambda' \cup (U_{n+1} \times V_{n+1})$, we get that

$$\ker(\mathcal{R}_\Lambda) = \ker(\mathcal{R}_{\Lambda'}) \cap \ker(\mathcal{R}_{U_{n+1}\times V_{n+1}}). \tag{4.36}$$

Note that if W and $W_1, ..., W_k$ are subspaces of a Hilbert space H such that $W_1, ..., W_k \subset W$, then

$$W = (W_1 + ... + W_k) \oplus W'_{1,...,k} \text{ for some } W'_{1,...,k} \subset W.$$

Note that there are infinitely many $W'_{1,...,k}$ that satisfy the above properties. We choose and fix one of them to define the following subspaces X_S, Y_S, Z_S, P and Q of $\mathcal{H}_A \otimes \mathcal{H}_B$ having the property:

$$\begin{aligned} H_S^{(n+1)} &= H_{S\cup\{n+1\}}^{(n+1)} \oplus X_S, \\ K_S^{(n)} &= K_S^{(n+1)} \oplus K_{S\cup\{n+1\}}^{(n+1)} \oplus Y_S, \\ H_{\{n+1\}}^{(n+1)} &= H_{S\cup\{n+1\}}^{(n+1)} \oplus Z_S \quad \text{for each subset } S \subset [n]; \\ \ker(\mathcal{R}_{V_{n+1}}) &= \left(\bigoplus_{S\subset[n]} K_S^{(n+1)} \right) \oplus P, \\ \ker(\mathcal{R}_{V_{n+1}})^{\perp} &= \left(\bigoplus_{S\subset[n]} K_{S\cup\{n+1\}}^{(n+1)} \right) \oplus Q. \end{aligned}$$

If $S_1, S_2 \subset [n+1]$ with $S_1 \neq S_2$, then $(S_1 \setminus S_2)$ or $(S_2 \setminus S_1)$ is non-empty. Say $(S_1 \setminus S_2)$ is non-empty, then there exists $j \in [n+1]$ such that $j \in S_1 \setminus S_2$, so $K_{S_1}^{(n+1)} \subset \ker(\mathcal{R}_{V_j})^{\perp}$ and $K_{S_2}^{(n+1)} \subset \ker(\mathcal{R}_{V_j})$, i.e. $K_{S_1}^{(n+1)}$ and $K_{S_2}^{(n+1)}$ are orthogonal to each other and we get that $K_{S_1}^{(n+1)} \cap K_{S_2}^{(n+1)} = \{0\}$. That is why we can write direct sum instead of sum in the equations involving P and Q.

Also note that for any $S \subset [n]$, if $v \in X_S \cap H_{\{n+1\}}^{(n+1)}$, then $v \in H_S^{(n+1)} \cap H_{\{n+1\}}^{(n+1)} = H_{S\cup\{n+1\}}^{(n+1)}$, i.e. $v \in X_S \cap H_{S\cup\{n+1\}}^{(n+1)} = \{0\}$, i.e. $v = 0$. Therefore we get that $X_S \cap H_{\{n+1\}}^{(n+1)} = \{0\}$ and $X_S \cap Z_S = \{0\}$.

Note that if $S \subset [n]$, then $H_S^{(n)} = H_S^{(n+1)}$, therefore for each $S \subset [n]$, we can have the decomposition

$$\begin{aligned} & H_S^{(n)} \otimes K_S^{(n)} \\ =& H_S^{(n+1)} \otimes \left[K_S^{(n+1)} \oplus K_{S\cup\{n+1\}}^{(n+1)} \oplus Y_S \right] \\ =& \left[H_S^{(n+1)} \otimes K_S^{(n+1)} \right] \oplus \left[(H_{S\cup\{n+1\}}^{(n+1)} \oplus X_S) \otimes K_{S\cup\{n+1\}}^{(n+1)} \right] \oplus \left[H_S^{(n+1)} \otimes Y_S \right] \\ =& \left[H_S^{(n+1)} \otimes K_S^{(n+1)} \right] \oplus \left[H_{S\cup\{n+1\}}^{(n+1)} \otimes K_{S\cup\{n+1\}}^{(n+1)} \right] \oplus \left[X_S \otimes K_{S\cup\{n+1\}}^{(n+1)} \right] \oplus \left[H_S^{(n+1)} \otimes Y_S \right] \end{aligned} \tag{4.37}$$

Now, we can decompose the two subspaces appearing in $\ker(\mathcal{R}_{U_{n+1}\times V_{n+1}})$ as follows

$$\begin{aligned} & \mathcal{H}_A \otimes \ker(\mathcal{R}_{V_{n+1}}) \\ =& \mathcal{H}_A \otimes \left[\left(\oplus_{S\subset[n]} K_S^{(n+1)} \right) \oplus P \right] \\ =& \left[H_{\emptyset}^{(n+1)} \otimes K_{\emptyset}^{(n+1)} \right] \oplus \left[\bigoplus_{\substack{S\subset[n] \\ S\neq\emptyset}} \left(H_S^{(n+1)} \otimes K_S^{(n+1)} \right) \right] \\ & \oplus \left[\bigoplus_{\substack{S\subset[n] \\ S\neq\emptyset}} \left(H_S^{(n+1)\perp} \otimes K_S^{(n+1)} \right) \right] \oplus [\mathcal{H}_A \otimes P] \end{aligned} \tag{4.38}$$

and

$$\begin{aligned}
&\ker(\mathcal{R}_{U_{n+1}}) \otimes (\ker(\mathcal{R}_{V_{n+1}}))^{\perp} \\
=&H^{(n+1)}_{\{n+1\}} \otimes \left[\left(\oplus_{S\subset[n]} K^{(n+1)}_{S\cup\{n+1\}}\right) \oplus Q\right] \\
=&\left[H^{(n+1)}_{\{n+1\}} \otimes K^{(n+1)}_{\{n+1\}}\right] \oplus \left[\bigoplus_{\substack{S\subset[n]\\ S\neq\emptyset}} \left(H^{(n+1)}_{S\cup\{n+1\}} \otimes K^{(n+1)}_{S\cup\{n+1\}}\right)\right] \\
&\qquad\qquad \oplus \left[\bigoplus_{\substack{S\subset[n]\\ S\neq\emptyset}} \left(Z_S \otimes K^{(n+1)}_{S\cup\{n+1\}}\right)\right] \oplus \left[H^{(n+1)}_{\{n+1\}} \otimes Q\right] \qquad (4.39)
\end{aligned}$$

Let $S_0, S \subset [n]$.

- Since $S \neq S_0 \cup \{n+1\}$ and so $K^{(n+1)}_{S_0\cup\{n+1\}}$ and $K^{(n+1)}_S$ are orthogonal, we have

$$\left[X_{S_0} \otimes K^{(n+1)}_{S_0\cup\{n+1\}}\right] \cap \left[H^{(n+1)\perp}_S \otimes K^{(n+1)}_S\right] = \{0\}.$$

- Since $K^{(n+1)}_{S_0\cup\{n+1\}} \subset \ker(\mathcal{R}_{V_{n+1}})^{\perp}$ and $P \subset \ker(\mathcal{R}_{V_{n+1}})$, we have

$$\left[X_{S_0} \otimes K^{(n+1)}_{S_0\cup\{n+1\}}\right] \cap [\mathcal{H}_A \otimes P] = \{0\}.$$

- When $S \neq S_0$ then $K^{(n+1)}_{S\cup\{n+1\}}$ and $K^{(n+1)}_{S_0\cup\{n+1\}}$ are orthogonal and when $S = S_0$ then $X_{S_0} \cap Z_{S_0} = \{0\}$, therefore we have

$$\left[X_{S_0} \otimes K^{(n+1)}_{S_0\cup\{n+1\}}\right] \cap \left[Z_S \otimes K^{(n+1)}_{S\cup\{n+1\}}\right] = \{0\}.$$

- Since $X_{S_0} \cap H^{(n+1)}_{\{n+1\}} = \{0\}$, we have

$$\left[X_{S_0} \otimes K^{(n+1)}_{S_0\cup\{n+1\}}\right] \cap \left[H^{(n+1)}_{\{n+1\}} \otimes Q\right] = \{0\}.$$

- When $S = S_0$, then $Y_{S_0} \cap K^{(n+1)}_{S_0} = \{0\}$ by definition of Y_{S_0}. When $S \neq S_0$ then either $S \setminus S_0$ or $S_0 \setminus S$ is non-empty. Say $S \setminus S_0$ is non-empty, then there exists $j \in S \setminus S_0$ with $j \in [n]$ so that $K^{(n+1)}_S \subset \ker(\mathcal{R}_{V_j})^{\perp}$ and $Y_{S_0} \subset \ker(\mathcal{R}_{V_j})$ and so $Y_{S_0} \cap K^{(n+1)}_S = \{0\}$. Therefore, we have

$$\left[H^{(n+1)}_{S_0} \otimes Y_{S_0}\right] \cap \left[H^{(n+1)\perp}_S \otimes K^{(n+1)}_S\right] = \{0\}.$$

- If $v \in Y_{S_0} \cap P$, then $v \in K_{S_0} \cap \ker(\mathcal{R}_{V_{n+1}}) = K^{(n+1)}_{S_0}$, i.e. $v \in Y_{S_0} \cap K^{(n+1)}_{S_0} = \{0\}$. Therefore, we have

$$\left[H_{S_0}^{(n+1)} \otimes Y_{S_0}\right] \cap [\mathcal{H}_A \otimes P] = \{0\}.$$

- When $S = S_0$, then $Y_{S_0} \cap K_{S_0 \cup \{n+1\}}^{(n+1)} = \{0\}$ by definition of Y_{S_0}. When $S \neq S_0$ then either $S \setminus S_0$ or $S_0 \setminus S$ is non-empty. Say $S \setminus S_0$ is non-empty, then there exists $j \in S \setminus S_0$ with $j \in [n]$ so that $K_{S \cup \{n+1\}}^{(n+1)} \subset \ker(\mathcal{R}_{V_j})^{\perp}$ and $Y_{S_0} \subset \ker(\mathcal{R}_{V_j})$ and so $Y_{S_0} \cap K_{S\{n+1\}}^{(n+1)} = \{0\}$. Therefore, we have

$$\left[H_{S_0}^{(n+1)} \otimes Y_{S_0}\right] \cap \left[Z_S \otimes K_{S \cup \{n+1\}}^{(n+1)}\right] = \{0\}.$$

- If $v \in Y_{S_0} \cap Q$, then $v \in K_{S_0} \cap \ker(\mathcal{R}_{V_{n+1}})^{\perp} = K_{S_0 \cup \{n+1\}}^{(n+1)}$, i.e. $v \in Y_{S_0} \cap K_{S_0 \cup \{n+1\}}^{(n+1)} = \{0\}$. Therefore, we have

$$\left[H_{S_0}^{(n+1)} \otimes Y_{S_0}\right] \cap \left[H_{\{n+1\}}^{(n+1)} \otimes Q\right] = \{0\}.$$

Therefore, using these information and Equations 4.34, 4.35, 4.36, 4.37, 4.38 and 4.39, we see that we can write

$$\ker(\mathcal{R}_\Lambda) = \left[\left(\bigoplus_{S \subset [n+1]} \left(H_S^{(n+1)} \otimes K_S^{(n+1)}\right)\right) \oplus F\right] \cap \left[\left(\bigoplus_{S \subset [n+1]} \left(H_S^{(n+1)} \otimes K_S^{(n+1)}\right)\right) \oplus F'\right]$$

where

$$F = \bigoplus_{S \subset [n]} \left(\left[X_S \otimes K_{S \cup \{n+1\}}^{(n+1)}\right] \oplus \left[H_S^{(n+1)} \otimes Y_S\right]\right),$$

$$F' = \left[\bigoplus_{\substack{S \subset [n] \\ S \neq \emptyset}} \left(H_S^{(n+1)\perp} \otimes K_S^{(n+1)}\right)\right] \oplus [\mathcal{H}_A \otimes P]$$

$$\oplus \left[\bigoplus_{\substack{S \subset [n] \\ S \neq \emptyset}} \left(Z_S \otimes K_{S \cup \{n+1\}}^{(n+1)}\right)\right] \oplus \left[H_{\{n+1\}}^{(n+1)} \otimes Q\right]$$

with the property that $F \cap F' = \{0\}$, which implies

$$\ker(\mathcal{R}_\Lambda) = \bigoplus_{S \subset [n+1]} \left(H_S^{(n+1)} \otimes K_S^{(n+1)}\right).$$

Hence we are done with the induction proof. □

Example 4.4.8. To see the decomposition better, we provide the subspaces involved for the case $n = 2$ here:

$$\begin{aligned}
H^{(2)}_{\emptyset} \otimes K^{(2)}_{\emptyset} &= \mathcal{H}_A \otimes (\ker(\mathcal{R}_{V_1}) \cap \ker(\mathcal{R}_{V_2})) \\
H^{(2)}_{\{1\}} \otimes K^{(2)}_{\{1\}} &= \ker(\mathcal{R}_{U_1}) \otimes [\ker(\mathcal{R}_{V_1})^{\perp} \cap \ker(\mathcal{R}_{V_2})] \\
H^{(2)}_{\{2\}} \otimes K^{(2)}_{\{2\}} &= \ker(\mathcal{R}_{U_2}) \otimes [\ker(\mathcal{R}_{V_1}) \cap \ker(\mathcal{R}_{V_2})^{\perp}] \\
H^{(2)}_{\{1,2\}} \otimes K^{(2)}_{\{1,2\}} &= [\ker(\mathcal{R}_{U_1}) \cap \ker(\mathcal{R}_{U_2})] \otimes [\ker(\mathcal{R}_{V_1})^{\perp} \cap \ker(\mathcal{R}_{V_2})^{\perp}] .
\end{aligned}$$

Corollary 4.4.9 ([Saikia24]). *Let $\Lambda \subset M_1 \times M_2$ be such that Λ is the union of finitely many subsets of $M_1 \times M_2$ all of which are products, i.e. $\Lambda = \bigcup_{j=1}^{n}(U_j \times V_j)$ for $U_j \subset M_1$ and $V_j \subset M_2$, then $\rho_{\Lambda}^{\ker}$ and $\rho_{\Lambda}^{\ker^{\perp}}$ are separable.*

Proof. Using Theorem 4.4.7, we see that when $\Lambda = \bigcup_{j=1}^{n}(U_j \times V_j)$ then $\ker(\mathcal{R}_{\Lambda})$ is direct sum of tensor product of Hilbert spaces. Further notice that for $S_1, S_2 \subset [n]$ with $S_1 \neq S_2$, the subspaces $H^{(n)}_{S_1} \otimes K^{(n)}_{S_1}$ and $H^{(n)}_{S_2} \otimes K^{(n)}_{S_2}$ are orthogonal to each other. This can be seen as $K^{(n)}_{S_1}$ and $K^{(n)}_{S_2}$ are orthogonal to each other when $S_1 \neq S_2$ as mentioned in the proof of Theorem 4.4.7. Therefore $\ker(\mathcal{R}_{\Lambda})$ contains an orthonormal basis consisting of separable vectors. Hence, $\rho_{\Lambda}^{\ker}$, being the orthogonal projection onto the subspace $\ker(\mathcal{R}_{\Lambda})$, can be written as a convex sum of the pure states in this orthonormal basis. But all these pure states in this orthonormal basis are separable, hence $\rho_{\Lambda}^{\ker}$ is separable. From Observation 4.4.2, we get that $\rho_{\Lambda}^{\ker^{\perp}}$ is also separable. □

4.4.4 Subsets coming from states

Corollary 4.4.9 is not very useful if for every subset the states associated this way become separable. So, one can ask whether we can find subsets such that the associated states are not separable. The answer is yes. In this section, we see that the states associated with subsets this way are not always separable. As a consequence of the following theorem, if we start with a holomorphic section s_0 that is itself not separable, to begin with, then the corresponding state $\rho_{\mathcal{V}(s_0)}^{\ker}$ is not separable.

Theorem 4.4.10 ([Saikia24]). *Let N be large enough so that $L_1^N \boxtimes L_2^N \to M_1 \times M_2$ is very ample. Let $s_0 \in H^0(M_1 \times M_2, L_1^N \boxtimes L_2^N)$ be a pure state and $\mathcal{V}(s_0) = \{x \in M_1 \times M_2 : s_0(x) = 0\}$ be the zero set of s_0, then $\rho_{\mathcal{V}(s_0)}^{\ker} = |s_0\rangle\langle s_0|$. We deduce that the states $\rho_{\mathcal{V}(s_0)}^{\ker}$ and $\rho_{\mathcal{V}(s_0)}^{\ker^{\perp}}$ are separable if and only if s_0 is separable.*

Proof. Since $L_1^N \boxtimes L_2^N \to M_1 \times M_2$ is very ample, we know that using this line bundle we can embed $\iota : M_1 \times M_2 \to \mathbb{P}^N$ for some $N \in \mathbb{N}$ and that $L_1^N \boxtimes L_2^N \cong \iota^*(\mathcal{O}(1))$ (as holomorphic line bundle), the pullback of the hyperplane line bundle on $\mathbb{P}^N$ [BS00, page 7]. Let $s \in \ker(\mathcal{R}_{\mathcal{V}_{s_0}})$. There exist holomorphic sections τ_0 and τ of $\mathcal{O}(1) \to \mathbb{P}^N$ such that $s_0 = \iota^*(\tau_0)$ and $s = \iota^*(\tau)$.

Let $\{(U_\alpha, \emptyset_{U_\alpha})\}$ be a trivializing open cover of the line bundle $L_1^N \boxtimes L_2^N \to M_1 \times M_2$. Let $f_{0\alpha}$ and f_α be the local representing functions on U_α that determines the sections s_0 and s. Since s_0 and s are pullbacks of sections τ_0 and τ of $O(1)$, therefore the order of vanishing of all the zeroes of $f_{0\alpha}$ and f_α is 1.

For each α, we define $h_\alpha : U_\alpha \to \mathbb{C}$ given by $h_\alpha(x) = \frac{f_\alpha(x)}{f_{0\alpha}(x)}$. Since the order of vanishing of both $f_{0\alpha}$ and f_α is 1 and the vanishing set of $f_{0\alpha}$ is a subset of the vanishing set of f_α, therefore h_α is a holomorphic function on U_α. Also for α and β with $U_\alpha \cap U_\beta \neq \emptyset$ we have

$$h_\alpha(x) = \frac{f_\alpha(x)}{f_{0\alpha}(x)} = \frac{g_{\alpha\beta}(x) f_\beta(x)}{g_{\alpha\beta}(x) f_\beta(x)} = \frac{f_\beta(x)}{f_{0\beta}(x)} = h_\beta(x) \quad \text{for all } x \in U_\alpha \cap U_\beta$$

where $g_{\alpha\beta}$ is the transition function (so $g_{\alpha\beta}(x) \in GL_1(\mathbb{C})$ is non-zero). Therefore h given by h_α on U_α is a holomorphic function on $M_1 \times M_2$. But since $M_1 \times M_2$ is compact and connected, we see that h is constant. Therefore, we get that s is a constant multiple of s_0. Hence

$$\ker(\mathcal{R}_{\mathcal{V}_{s_0}}) = \{\lambda s_0 : \lambda \in \mathbb{C}\} \text{ and } \rho^{\ker}_{\mathcal{V}(s_0)} = |s_0\rangle \langle s_0| .$$

□

In the previous theorem, we considered some particular subsets that are related to pure state s_0 and showed that the state $\rho^{\ker}_{\mathcal{V}(s_0)}$ is the same as the original pure state to begin with. We want to find some special subsets that have this property with respect to some mixed state. We define these subsets using coherent states [see Kir07; BS00] and covariant symbols associated with the mixed state.

Let us briefly recollect the notion of coherent states. Consider a compact connected manifold M with quantum line bundle L. Let $\{\theta_j\}_{j=1}^d$ be an orthonormal basis for $H^0(M, L)$. The reproducing kernel known as the generalized Bergman kernel is the section K of $\overline{L} \boxtimes L \to M \times M$, where $\overline{L} \cong L^*$ using the hermitian structure of the line bundle L, given by

$$K(x, y) := \sum_{j=1}^{d} \overline{\theta_j(x)} \otimes \theta_j(y) \quad \text{for } x, y \in M.$$

For each $x \in M$, we define $\Phi_x \in \overline{L_x} \otimes H^0(M, L)$ by

$$\Phi_x = \sum_{j=1}^{d} \overline{\theta_j(x)} \otimes \theta_j.$$

Using appropriate trivialization and identifying $1 \otimes \theta_j$ with θ_j, we can think of Φ_x as a holomorphic section of $L \to M$. Using the reproducing property of the Bergman kernel, we have $\langle \Phi_x | s \rangle = s(x)$ for all $x \in M$ and $s \in H^0(M, L)$. Then the *coherent state* localized at $x \in M$, denoted by $|x\rangle$, is given by

$$|x\rangle = \begin{cases} 0 & \text{when } \|\Phi_x\| = 0 \\ \frac{\Phi_x}{\|\Phi_x\|} & \text{otherwise.} \end{cases}$$

The *covariant symbol* $\hat{\sigma}$ associated to the operator σ of $H^0(M, L)$ is given by

$$\hat{\sigma}(x) := \langle x|\sigma|x\rangle \text{ for all } x \in M.$$

Theorem 4.4.11 ([Saikia24]). *Let σ be a mixed state which is an orthogonal projection such that* Ran$(\sigma)^{\perp}$ *has a basis consisting of coherent states and $\hat{\sigma}$ be the covariant symbol associated with σ. Let $\mathcal{V}(\sigma) = \{x \in M_1 \times M_2 : \hat{\sigma}(x) = 0\}$, then $\rho^{\ker}_{\mathcal{V}(\sigma)} = \sigma$.*

Proof. There exists an orthonormal set $\{v_1, ..., v_k\}$ of $\mathcal{H}_A \otimes \mathcal{H}_B$ consisting of pure states such that $\sigma = \frac{1}{k}\sum_{j=1}^{k} \left|v_j\right\rangle \left\langle v_j\right|$. Denote the range span$\{v_1, ..., v_k\}$ of σ by Ran(σ). Then

$$\mathcal{V}(\sigma) = \{x \in M_1 \times M_2 : \langle x|\sum_{j=1}^{k} \left|v_j\right\rangle \left\langle v_j\right||x\rangle = 0\}$$

$$\begin{aligned} &= \{x \in M_1 \times M_2 : \sum_{j=1}^{k} |\left\langle x\middle|v_j\right\rangle|^2 = 0\} \\ &= \{x \in M_1 \times M_2 : \left\langle x\middle|v_j\right\rangle = 0 \text{ for all } j\} \\ &= \{x \in M_1 \times M_2 : \text{ the coherent state } |x\rangle \text{ is in } \mathrm{Ran}(\sigma)^{\perp}\} \end{aligned}$$

Due to the hypothesis that Ran$(\sigma)^{\perp}$ has a basis consisting of coherent states, the above set $\mathcal{V}(\sigma)$ is non-empty. Now we find the kernel of the restriction map to $\mathcal{V}(\sigma)$. We have

$$\begin{aligned} \ker(\mathcal{R}_{\mathcal{V}(\sigma)}) &= \{s \in \mathcal{H}_A \otimes \mathcal{H}_B : s(x) = 0 \text{ for all } x \in \mathcal{V}(\sigma)\} \\ &= \{s \in \mathcal{H}_A \otimes \mathcal{H}_B : \langle x|s\rangle = 0 \text{ for all coherent states } |x\rangle \text{ in } \mathrm{Ran}(\sigma)^{\perp}\} \end{aligned}$$

Let $s \in$ Ran(σ), then $\langle s'|s\rangle = 0$ for all $s' \in$ Ran$(\sigma)^{\perp}$. In particular, $\langle x|s\rangle = 0$ for all coherent states $|x\rangle \in$ Ran$(\sigma)^{\perp}$, i.e. $s \in \ker(\mathcal{R}_{\mathcal{V}(\sigma)})$, i.e. Ran$(\sigma) \subset \ker(\mathcal{R}_{\mathcal{V}(\sigma)})$.

Conversely, suppose $s \in \ker(\mathcal{R}_{\mathcal{V}(\sigma)})$, i.e. $\langle x|s\rangle = 0$ for all coherent states $|x\rangle \in$ Ran$(\sigma)^{\perp}$. Because there is a basis for Ran$(\sigma)^{\perp}$ consisting of coherent states, we see that $\langle s'|s\rangle$ for all $s' \in$ Ran$(\sigma)^{\perp}$, i.e. $s \in$ Ran(σ).

Therefore, we see that $\ker(\mathcal{R}_{\mathcal{V}(\sigma)}) =$ Ran(σ). Hence $\rho^{\ker}_{\mathcal{V}(\sigma)}$ and σ both being the orthogonal projection onto the same subspace are equal. ◻

Chapter 5

Quantum Circuit Synthesis

In this chapter, we present an exact synthesis algorithm for qutrit unitaries in $\mathcal{U}_{3^n}(\mathbb{Z}[1/3, e^{2\pi i/3}])$ over the Clifford+T gate set with at most one ancilla. Further, using catalytic embeddings, we present an algorithm to exactly synthesize unitaries $\mathcal{U}_{3^n}(\mathbb{Z}[1/3, e^{2\pi i/9}])$ over the Clifford+T gate set with at most 2 ancillae. The work presented in this chapter is the contents of the paper [KSaikia+]. We acknowledge that the figures were made using the software TikZit and open-source style files available on ArXiv [Gla+22].

5.1 Introduction

The circuit model of computation uses networks consisting of wires and electrical switches (gates) that carry operations on bit values. The gates in the classical model of circuit computation are Boolean functions $f : \{0, 1\}^n \to \{0, 1\}^m$. A computer architecture should be able to perform any vector-valued Boolean transformation. However, to have a feasible architecture, we should be able to generate all such gates using a small amount of gates. A *functionally complete* or *universal gate set* is a set of gates that can generate all Boolean functions. The set {AND, NOT} is a famous example of a universal gate set in classical computation.

In quantum computing, the elementary units of computation are qudits (pure state in a d-level quantum system). As mentioned in Chapter 2, we can manipulate pure states in a quantum system using unitary operators on the quantum Hilbert space. In other words, quantum gates are unitary operators $U \in \mathcal{U}_{d^n}(\mathbb{C})$, when there are n qudits involved. Here $\mathcal{U}_k(\mathcal{R})$ denotes the group of $k \times k$ unitary with entries from the ring $\mathcal{R}$. Note that $\mathcal{U}_{d^n}(\mathbb{C})$ is an uncountable set and therefore any physical quantum computing architecture with finite resources can not implement all quantum gates. The next best thing could be to find a way to approximate gates using a dense subset of $\mathcal{U}_{d^n}(\mathbb{C})$. However, no finite set is dense in $\mathcal{U}_{d^n}(\mathbb{C})$. Therefore, what is desirable is that we need to have a finite set of physically implementable gates that can generate (as a word) a subgroup of $\mathcal{U}_{d^n}(\mathbb{C})$ which is dense inside $\mathcal{U}_{d^n}(\mathbb{C})$. The choice of such a finite set and decomposing any unitary in $\mathcal{U}_{d^n}(\mathbb{C})$ approximately into a word in this finite set is informally known as the problem of quantum circuit synthesis. Roughly, quantum circuit synthesis involves the following steps:

- **Choice of a generating set:** We choose a finite set $\mathcal{S}$ such that $\mathcal{S}$ generates a subgroup $\mathcal{G}$ that is topologically dense in $\mathcal{U}_{d^n}(\mathbb{C})$.
- **Approximate synthesis:** Given $\epsilon > 0$ and a unitary $U \in \mathcal{U}_{d^n}(\mathbb{C})$, we choose an unitary $U' \in \mathcal{G}$ such that $\|U - U'\| < \epsilon$.
- **Exact synthesis:** Write U' as a word with letters in $\mathcal{S}$, i.e. write $U' = U_1 U_2 ... U_k$ such that $U_j \in \mathcal{S}$ for all j.

Definition 5.1.1 (Universal gate set in quantum computing)**.** The finite set $\mathcal{S}$ that we choose according to the above properties is called a *universal gate set* in quantum computing.

The problem of exact synthesis in quantum computing asks for an algorithm to solve the word problem in the group $\mathcal{G}$ in terms of the universal gate set $\mathcal{S}$. Many of the famous universal gate sets are chosen due to practical reasons, such as fault tolerance architecture. Several well-known universal gate sets such as Clifford+T, Clifford+R, Clifford+V etc. are defined over number fields, often a field of cyclotomic numbers.

There are various synthesis algorithms for single-qubit unitaries in different localized number rings over single-qubit gate sets, such as the Clifford+T, Clifford+V etc. These algorithms use methods from number theory such as quaternion factorization [KMM13; GS13; Kli+15; KY15] and more recently catalytic embedding [Amy+23]. The first instance of a synthesis algorithm for a single-qubit unitary over the Clifford+T case was shown in [KMM13]. The main result of [KMM13] states that the set of single-qubit unitaries exactly implementable over the Clifford+T gate set is precisely $\mathcal{U}_2(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$. Moreover, the proof of this yields an efficient algorithm to solve the word problem for Clifford+T.

The next thing is to decompose n-qubit unitary from a dense group $\mathcal{G}$ into a desirable universal set. For example, an extension of the main result in [KMM13] will be to decompose unitaries from the group $\mathcal{U}_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ into multi-qubit Clifford+T. This was extended to multi-qubits by Giles and Selinger [GS13], however, for the algorithm to work for each unitaries in $\mathcal{U}_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$, we need an *ancillary* qubit. The use of ancilla is also a common technique, even in classical computation and reversible computation, to convert irreversible gates into a circuit that has all reversible gates. Informally, an *ancilla* means an auxiliary system that is added to the original system to facilitate the purpose we are interested in. Figure 5.1 shows a schematic diagram of the usage of an ancilla. The Figure shows more wires for the desired output than the input, but it does not mean that this is always the case. In general, the distribution of the number of wires for the desired output and the garbage output varies depending on the problem at hand.

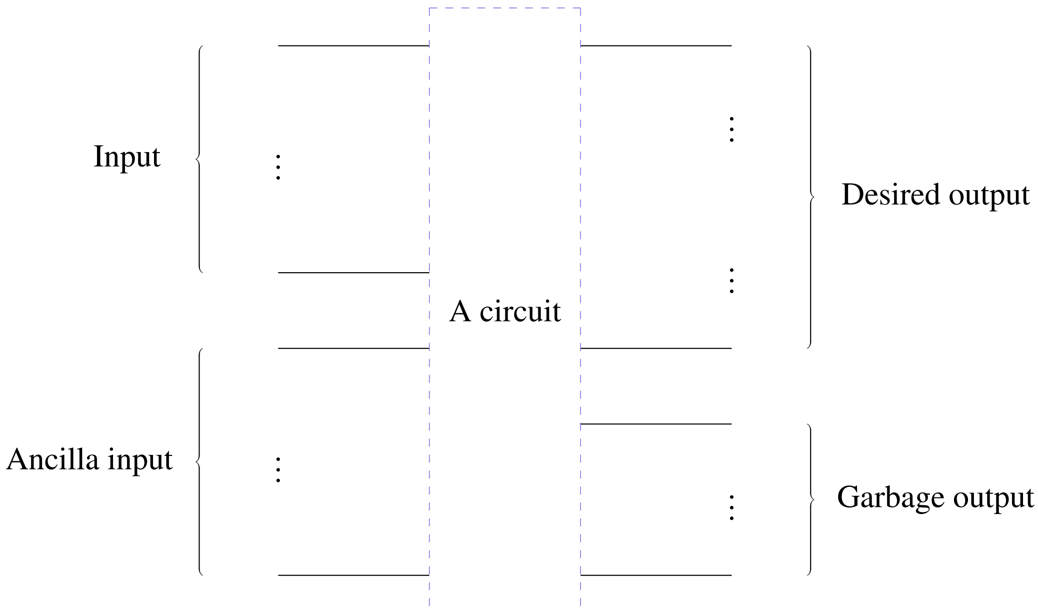


Figure 5.1: The use of an ancilla

Similar to classical computers relying on bits, most quantum computers are based on the quantum counterpart of bits, which are qubits. However, many of the different kinds of physical qubits used are higher-level qudits restricted to two-level quantum systems. The idea behind the growing popularity of research in higher-level qudits is that if we already have higher dimensional qudits, why not use the extra space and freedom? The use of higher-level qudits also has potential advantages in runtime efficiency, resource requirements etc [Wan+20]. To this end, we discuss circuit synthesis of unitaries of the next higher-level quantum system, which are qu*trits* (3-level quantum system).

For qutrits, a synthesis algorithm is already known for single qutrit Clifford+R gates as studied in [Boc+16] and later in [KVM23]. More precisely, the group $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ is generated by the Clifford gates and $R = \mathrm{diag}(1, 1, -1)$ gate. The proof of this yields an efficient algorithm to solve the word problem over Clifford+R gate set, that is given an arbitrary unitary U in $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ there is a sequence of unitaries from the finite set of Clifford unitaries and the R gate whose product is U. It was recently conjectured in [KVM23] and proved in [EP24] that $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ is generated by Clifford+$\mathcal{D}$ gates. Due to various practical reasons, the gate set Clifford+T is considered more desirable for most purposes.

The single-qutrit Clifford+T group forms a proper subgroup of $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$, meaning that we can not have an exact synthesis algorithm for the group $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ over the single-qutrit Clifford+T. It is also known that the R gate which is an element of $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ is not an element of the single-qutrit Clifford+T gate set [Gla+22], meaning that we can not have an exact synthesis algorithm for the group $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ over the single-qutrit Clifford+T either. However, it is shown in [Gla+22] that with the help of a borrowed ancilla, any unitary in the ring $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ can be implemented over 2-qutrit Clifford+T. This naturally asks for an extension of synthesis to the multi-qutrit gates in $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ and $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ over the multi-qutrit Clifford+T gate set. In this chapter, we answer these questions. Theorem 5.3.1 provides an algorithm to exactly synthesis a circuit for any unitary in $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ over the multi-qutrit Clifford+T with the help of a borrowed ancilla. Theorem 5.4.1 provides an algorithm to exactly synthesize any unitary in $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ over multi-qutrit synthesis with two ancillae by means of a catalytic embedding of $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ in $\mathcal{U}_{3^{n+1}}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$, and subsequent application of the algorithm of Theorem 5.3.1. To the best of our knowledge, these algorithms are among the first for multi-qutrit synthesis, along with another multi-qutrit synthesis algorithm developed, simultaneously and independently, by a different group of researchers using the Toffoli+Hadamard gate set in [Gla+24].

5.2 Preliminaries

In this section, we introduce basic definitions and fix some notations. We recall some properties of cyclotomic ring extensions, the concept of denominator exponents and the catalytic embeddings recently introduced in [Amy+23].

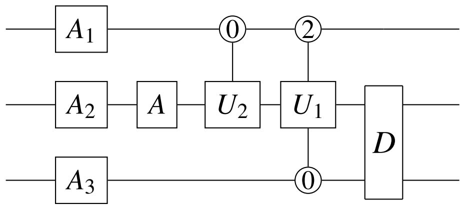
5.2.1 Some basic definitions and notations

Definition 5.2.1 (Qu*dit*)**.** Pure states in a quantum Hilbert space $\mathcal{H}$ are called *qudit* if the dimension of $\mathcal{H}$ is d. We write the standard orthonormal basis of $\mathcal{H} \cong \mathbb{C}^d$ as $\{|0\rangle, |1\rangle, ..., |d-1\rangle\}$. In particular, when the dimensions are 2 and 3, we call the pure states *qubits* and *qutrits* respectively.

As the main focus of this chapter is qutrits, from now on we shall base most of our discussions on qutrits, rather than general qudits.

Notation 5.2.2. *Let $U \in \mathcal{U}_{d^n}(\mathbb{C})$, then corresponding to a decomposition of $U = U_1...U_k$, we can make a circuit diagram representation of that particular decomposition. The input of the circuit diagram starts at the left-hand side and the output is at the right-hand side and this is why the circuit diagram has the reverse order to matrix multiplication.*

For illustration, we provide a circuit of a unitary in $\mathcal{U}_{3^3}(\mathbb{C})$ as a decomposition of various sizes unitaries in Figure 5.2. The figure covers the most common types of notations used in this *chapter. Note that* $A_1, A_2, A_3, A, U_1, U_2 \in \mathcal{U}_3(\mathbb{C})$, $D \in \mathcal{U}_{3^2}(\mathbb{C})$, *the controlled gate* $U_1 \in \mathcal{U}_{3^3}(\mathbb{C})$ *and the controlled gate* $U_2 \in \mathcal{U}_{3^2}(\mathbb{C})$.



$$= (I \otimes D)(C_1)(C_2 \otimes I)(I \otimes A \otimes I)(A_1 \otimes A_2 \otimes A_3)$$

Figure 5.2: An illustration of a circuit corresponding to a matrix decomposition

Definition 5.2.3 (Controlled gates)**.** Let $U \in \mathcal{U}_3(\mathbb{C})$ be a single-qutrit gate and $x_1, ..., x_n \in \{0, 1, 2\}$. Then the n-qutrit gate $\left|x_1....x_{j-1}\right\rangle \otimes \left|x_{j+1}...x_n\right\rangle$-*controlled-U* is defined to be the unitary having the following action:

$$|y_1...y_n\rangle \mapsto \begin{cases} \left|x_1....x_{j-1}\right\rangle \otimes (U\left|y_j\right\rangle) \otimes \left|x_{j+1}...x_n\right\rangle & \text{when } (y_1, ..., y_{j-1}, y_{j+1}, ..., y_n) \\ & \quad = (x_1, ..., x_{j-1}, x_{j+1}, ..., x_n) \\ |y_1...y_n\rangle & \text{otherwise.} \end{cases}$$

Alternatively, we also call this gate as the $(n-1)$-controlled-U gate with j-th target wire and with controls $x_1, ..., x_{j-1}, x_{j+1}, ..., x_n$.

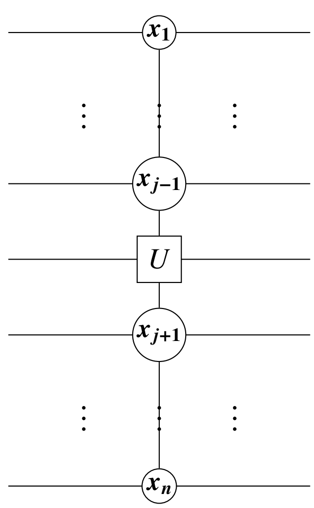


Figure 5.3: Controlled-U gate with controls $x_1, ..., x_{j-1}, x_{j+1}, ..., x_n$ and target at j-th wire

Notation 5.2.4 (Single-qutrit permutation gates)**.** *The permutation matrix corresponding to* $\sigma \in S_3$ *is called a permutation gate and is denoted by* X_σ. *When* $\sigma = (1\ 2\ 3)$, *then we get the* *standard X gate for qutrit, that is*

$$X = X_{(1\ 2\ 3)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Remark 5.2.5. Note that $H^2 = X_{(2\ 3)}$ (where H is the Hadamard gate defined in Notation 5.2.10) and as we know a 2-cycle and a 3-cycle generate the whole group S_3, so X and H^2 generate all the permutation gates.

Remark 5.2.6. Note that if the control qutrit is $|0\rangle$, then conjugating the control wire with X^2 and if the control qutrit is $|1\rangle$, then conjugating the control wire with X, we can convert any controlled gate to a $|2\rangle$-controlled gate (as illustrated in Figure 5.4).

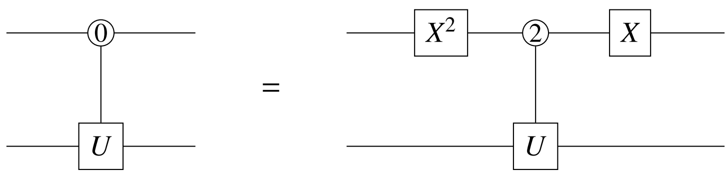


Figure 5.4: Change of control from $|0\rangle$ to $|2\rangle$

Definition 5.2.7 (Borrowed ancilla)**.** A *borrowed ancilla* is an ancilla input that can be in any state and the garbage output is the same as the ancilla input after all the operations are done. Mathematically, instead of decomposing U over a desired gate set, we decompose $U \otimes I$. Figure 5.5 shows the use of a borrowed ancilla.

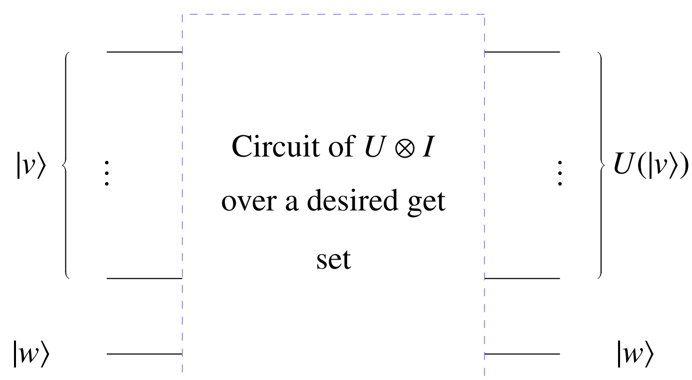


Figure 5.5: A borrowed ancilla

Throughout this chapter, we have kept using the concept of single-qudit and multi-qudit gates. The single-qudit gates mean a unitary in $U_d(\mathbb{C})$ and a multi-qudit gate means a unitary in $\mathcal{U}_{d^n}(\mathbb{C})$ for some $n \geq 2$ (we also specify them as n-qudit gate whenever a specification is needed). We also keep using some specific gate set $\mathcal{S}$ and the group $\mathcal{G}$ generated by the gate set. The definition of a single-qudit group $\mathcal{G}$ generated by a set is straightforward: it is the set of all possible words in the elements of $\mathcal{S}$. However, for multi-qudit cases, the elements of the set $\mathcal{S}$ can be matrices of different sizes. We define the group explicitly below to avoid confusion.

Definition 5.2.8 (n-qudit group generated by a set $\mathcal{S}$)**.** Let $\mathcal{S}$ be a set of unitaries of size $d^l \times d^l$ for some $1 \leq l \leq n$. Note that the set may contain unitaries of varying sizes. Then by the *n-qudit group generated by $\mathcal{S}$*, we actually mean the group generated by the unitaries of the form $I_{d^{l_1}} \otimes U \otimes I_{d^{l_2}}$ where $U \in \mathcal{S} \cap \mathcal{U}_{d^l}(\mathbb{C})$ and $0 \leq l_1, l_2$ with $l_1 + l + l_2 = n$.

Notation 5.2.9. *The roots of unity frequently appear in this chapter. We denote the primitive k-th root of unity $e^{2\pi i/k}$ by the symbol ζ_k. From now on when the subscript is not specified, then by ζ we mean $e^{2\pi i/9}$, a primitive 9th root of unity. Also we denote $\omega = e^{2\pi i/3}$, a primitive 3rd root of unity.*

Notation 5.2.10. *Here are some important single-qutrit gates and their notations:*

$$\text{Hadamard gate, } H = \frac{1}{\sqrt{-3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \quad \text{Phase gate, } S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{pmatrix}$$

$$\text{Metaplectic gate, } R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^{-1} \end{pmatrix}$$

Definition 5.2.11 (Pauli Group)**.** The *qutrit Pauli group $\mathcal{P}_n$* (a subgroup of $\mathcal{U}_{3^n}(\mathbb{C})$) is generated by the following:

$$\text{Pauli } X = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{Pauli } Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$$

Definition 5.2.12 (Clifford group)**.** The *Clifford group C_n* is defined to be the normalizer of the Pauli group $\mathcal{P}_n$ quotiented by $\mathcal{U}_1(\mathbb{C})$, that is

$$C_n = \{V \in \mathcal{U}_{3^n}(\mathbb{C}) : V^{-1}\mathcal{P}_n V = \mathcal{P}_n\}/\mathcal{U}_1(\mathbb{C}).$$

This is a finite group and any element of this group is said to be a Clifford gate.

Notation 5.2.13. *One of the most important 2-qutrit gate is the gate known as CSUM (or CX) given by*

$$CSUM(|x\rangle |y\rangle) = |x\rangle |x + y \ (mod\ 3)\rangle .$$

This gate is an element of the multi-qutrit Clifford group. Note that CSUM is the composition of $|1\rangle$*-controlled-X gate and* $|2\rangle$*-controlled-*X^2 *gate.*

$CSUM =$

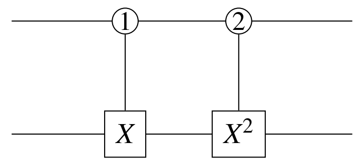


Figure 5.6: The $CSUM$ (or CX) gate

Proposition 5.2.14. *The single-qutrit Clifford group is generated by the set* $\{X, H, S\}$.

Proposition 5.2.15. *The multi-qutrit Clifford group is generated by the set* $\{X, H, S, CSUM\}$.

5.2.2 Important Gate Sets

In this section, we introduce a few important gate sets and the group generated by the gate set that appears commonly in this chapter.

Definition 5.2.16. The *single-qutrit Clifford+$\mathcal{D}$ group* is defined as the group generated by the set $\{H, X, R, \mathcal{D}\}$ where

$$\mathcal{D} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta \end{pmatrix}.$$

Definition 5.2.17. The *single-qutrit Clifford+T group* is defined as the group generated by the set $\{H, S, X, T\}$.

Definition 5.2.18. The *single-qutrit Clifford+R group* is defined as the group generated by the set $\{H, S, X, R\}$.

Similar to extending the multi-qutrit Clifford group from the single-qutrit Clifford group, we can extend these to multi-qutrit cases [NC10] by adjoining the gate $CSUM$.

Definition 5.2.19. The *multi-qutrit Clifford+$\mathcal{D}$ group* is defined as the group generated by the set $\{H, X, R, \mathcal{D}, CSUM\}$.

Definition 5.2.20. The *multi-qutrit Clifford+T group* is defined as the group generated by the set $\{H, S, X, T, CSUM\}$. In this chapter, we use $(Clif + T)^{(n)}$ to denote the n-qutrit Clifford+T group (i.e. the group where all the unitaries are of size $3^n \times 3^n$).

Definition 5.2.21. The *multi-qutrit Clifford+R group* is defined as the group generated by the set $\{H, S, X, R, CSUM\}$.

Note that both Clifford+T and Clifford+R groups are subgroups of Clifford+$\mathcal{D}$.

Remark 5.2.22. Note that by the terms Clifford+$\mathcal{D}$ gate set, Clifford+T gate set and Clifford+R gate set, we mean the finite set $C_n \cup \{\mathcal{D}\}$, $C_n \cup \{T\}$ and $C_n \cup \{R\}$ respectively. However, by the terms Clifford+$\mathcal{D}$ group, Clifford+T group and Clifford+R group, we mean the group generated by the corresponding gate set as defined above. This is the same difference as the set $\mathcal{S}$ and $\mathcal{G}$ mentioned in the introduction of this chapter. As the main focus of this chapter is exact synthesis, the final circuit will consist of words with letters from the gate set Clifford+T.

5.2.3 Catalytic Embedding

In this section, we recall the concept of catalytic embedding, in the sense of [Amy+23], which will be used in the proof of Theorem 5.4.1.

Definition 5.2.23 (Catalytic embedding)**.** Let $\mathcal{G}_1$ be a subgroup of $\mathcal{U}_n(\mathbb{C})$ and $\mathcal{G}_2$ be a subgroup of $\mathcal{U}_{nd}(\mathbb{C})$. We call a group homomorphism $\Phi : \mathcal{G}_1 \to \mathcal{G}_2$ a *d-dimensional catalytic embedding* with respect to a quantum state $|\lambda\rangle \in \mathbb{C}^d$ (known as the catalyst) if

$$\Phi(U)(|u\rangle \otimes |\lambda\rangle) = (U\,|u\rangle) \otimes |\lambda\rangle \qquad \text{for all } |u\rangle \in \mathbb{C}^n$$

Let $R = \mathbb{Z}[\frac{1}{d}]$. We explicitly describe a catalytic embedding of $\mathcal{U}_n(R[\zeta_{d^k}])$ into $\mathcal{U}_{nd}(R[\zeta_{d^{k-1}}])$. For $U \in \mathcal{U}_n(R[\zeta_{d^k}])$, there exist unique $A_1, A_2, ..., A_d \in \mathcal{M}_n(R[\zeta_{d^{k-1}}])$ such that:

$$U = \sum_{j=0}^{d-1} \zeta_{d^k}^j A_j.$$

We define $\Phi_n^{(k)} : \mathcal{U}_n(R[\zeta_{d^k}]) \to \mathcal{U}_{nd}(R[\zeta_{d^{k-1}}])$ by:

$$\Phi_k(U) = \sum_{j=0}^{d-1} A_j \otimes \Lambda_k^j,$$

where $\Lambda_k = \left(\begin{array}{c|c} 0 & \zeta_{d^{k-1}} \\ \hline I_{d-1} & 0 \end{array}\right)$. It is easy to verify that $\Phi_n^{(k)}$ satisfies the requirements of a catalytic embedding with respect to the catalyst $|\lambda_k\rangle = (\zeta_{d^k}^{d-1}, \zeta_{d^k}^{d-2}, ..., 1)^t$.

In particular, for each $n \in \mathbb{N}$, we have a catalytic embedding $\Phi_n : \mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \zeta]) \hookrightarrow \mathcal{U}_{3^{n+1}}(\mathbb{Z}[\frac{1}{3}, \omega])$ with $\Lambda = \begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and the catalyst $|\lambda\rangle = (\zeta^2, \zeta, 1)^t$.

5.2.4 Smallest denominator exponent

Proposition 5.2.24. *Let p be a prime number. For $l \in \mathbb{N}$, let ζ_{p^l} be a primitive p^l-th root of unity and $\chi_{p^l} = 1 - \zeta_{p^l}$. Then $\mathbb{Z}\left[\frac{1}{p}, \zeta_{p^l}\right] = \mathbb{Z}\left[\frac{1}{\chi_{p^l}}, \zeta_{p^l}\right]$.*

Proof. It is well known that the value of the p^l-th cyclotomic polynomial at 1 is p, so

$$p = \prod_{\substack{1 \le k \le p^l \\ \gcd(k,p)=1}} (1 - \zeta_{p^l}^k) = (1 - \zeta_{p^l})^{\phi(p^l)} \prod_{\substack{1 \le k \le p^l \\ \gcd(k,p)=1}} \frac{1 - \zeta_{p^l}^k}{1 - \zeta_{p^l}}.$$

We know that for all k with $\gcd(k, p) = 1$, the term $\frac{1-\zeta_{p^l}^k}{1-\zeta_{p^l}}$ is a unit in $\mathbb{Z}[\zeta_{p^l}]$. Therefore $p = \chi_{p^l}^{\phi(p^l)} u$ for some unit $u \in \mathbb{Z}[\zeta_{p^l}]$. Hence we can write

$$\frac{1}{p} = \frac{u^{-1}}{\chi_{p^l}^{\phi(p^l)}} \in \mathbb{Z}\left[\frac{1}{\chi_{p^l}}, \zeta_{p^l}\right] \text{ and } \frac{1}{\chi_{p^l}} = \frac{(1 - \zeta_{p^l})^{(\phi(p^l)-1)} u}{p} \in \mathbb{Z}\left[\frac{1}{p}, \zeta_{p^l}\right]$$

□

Notation 5.2.25. *From now on, when the subscript is not specified, we denote $\chi = 1 - \omega$.*

As a consequence of Proposition 5.2.24, we get that localizing the element 3 and localizing the element χ produces the same ring $\mathbb{Z}[\frac{1}{3}, \omega]$. Further note that $\frac{1}{\sqrt{-3}} = \frac{\omega^2}{\chi}$ and ω^2 is a unit, therefore localizing at $\frac{1}{\sqrt{-3}}$ also produces the same ring i.e:

$$\mathbb{Z}\left[\frac{1}{3}, \omega\right] = \mathbb{Z}\left[\frac{1}{\sqrt{-3}}, \omega\right] = \mathbb{Z}\left[\frac{1}{\chi}, \omega\right].$$

Therefore, the ring $\mathbb{Z}\left[\frac{1}{3}, \omega\right]$ has an infinite $\mathbb{Z}[\omega]$-basis $\{1, \frac{1}{\chi}, \frac{1}{\chi^2}, ...\}$ and so we can talk about denominator exponent and smallest denominator exponents of an element $x \in \mathbb{Z}[\frac{1}{3}, \omega]$ with respect to χ. We formally define them below:

Definition 5.2.26 (sde of an element w.r.t. χ)**.** Let $x \in \mathbb{Z}[\frac{1}{3}, \omega]$, then $f \in \mathbb{N} \cup \{0\}$ is said to be a *denominator exponent* of x with respect to χ if $\chi^f x \in \mathbb{Z}[\omega]$. Further if $\chi^f x \in \mathbb{Z}[\omega]$ but $\chi^{f-1} x \notin \mathbb{Z}[\omega]$, then f is said to be the *smallest denominator exponent* or *sde* of x (with respect to χ).

Definition 5.2.27 (sde of a column)**.** Let $\mathbf{u} \in \mathbb{Z}[\frac{1}{3}, \omega]^m$ be a $m \times 1$ column, then $f \in \mathbb{N} \cup \{0\}$ is said to be a *denominator exponent* of $\mathbf{u}$ with respect to χ if $\chi^f \mathbf{u} \in \mathbb{Z}[\omega]^m$. Further if $\chi^f \mathbf{u} \in \mathbb{Z}[\omega]^m$ but $\chi^{f-1} \mathbf{u} \notin \mathbb{Z}[\omega]^m$, then f is said to be the *smallest denominator exponent* or *sde* of $\mathbf{u}$ (with respect to χ).

5.3 Unitaries with entries from $\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}]$

In this section, we prove one of the main two theorems in this chapter. The proof of the theorem yields an algorithm to make an exact circuit for any unitary with entries from $\mathbb{Z}[\frac{1}{3}, \omega]$ over the multi-qutrit Clifford+T gate set. This result is an extension of [Gla+22, Corollary 23], which basically says that any unitary from $\mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, \omega])$ can be exactly synthesized over the 2-qutrit Clifford+T gate set.

The proof of the theorem goes through a series of steps. The first step is to express $U \in \mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega])$ as a product of 3-level unitaries, which are then further decomposed into (multiply)-controlled single qutrit Clifford+R gates. Finally, these controlled gates are implemented over the $(n+1)$-Clifford gate set using a borrowed ancilla. Figure 5.7 shows a schematic diagram of the steps involved in the algorithm given by Theorem 5.3.1.

Theorem 5.3.1. *[KSaikia+] Let $U \in \mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega])$. Then U can be exactly represented by a quantum circuit over Clifford+T, using at most one borrowed ancilla. To be precise, we have the following embedding of groups $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega]) \hookrightarrow (Clif + T)^{(n+1)}$ given by*

$$U \mapsto U \otimes I$$

of $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega])$ inside $(n+1)$-qutrit Clifford+T group.

In the following subsections, we define the necessary tools and prove a few important lemmas that are required for the proof of Theorem 5.3.1.

5.3.1 Reduction to 3-level unitaries

Definition 5.3.2 (3-level matrices)**.** Let $\mathcal{R}$ be a ring. Let $U \in \mathcal{M}_3(\mathcal{R})$ be given by the matrix:

$$U = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}$$

A matrix $M \in \mathcal{M}_m(R)$ (with $m \geq 3$) is said to be a *3-level matrix of type U* if there is a coordinate subspace of dimension 3, say with indices j_1, j_2, and j_3, on which M acts by U, and such that M acts trivially on its orthogonal complement. In other words: say the indices have

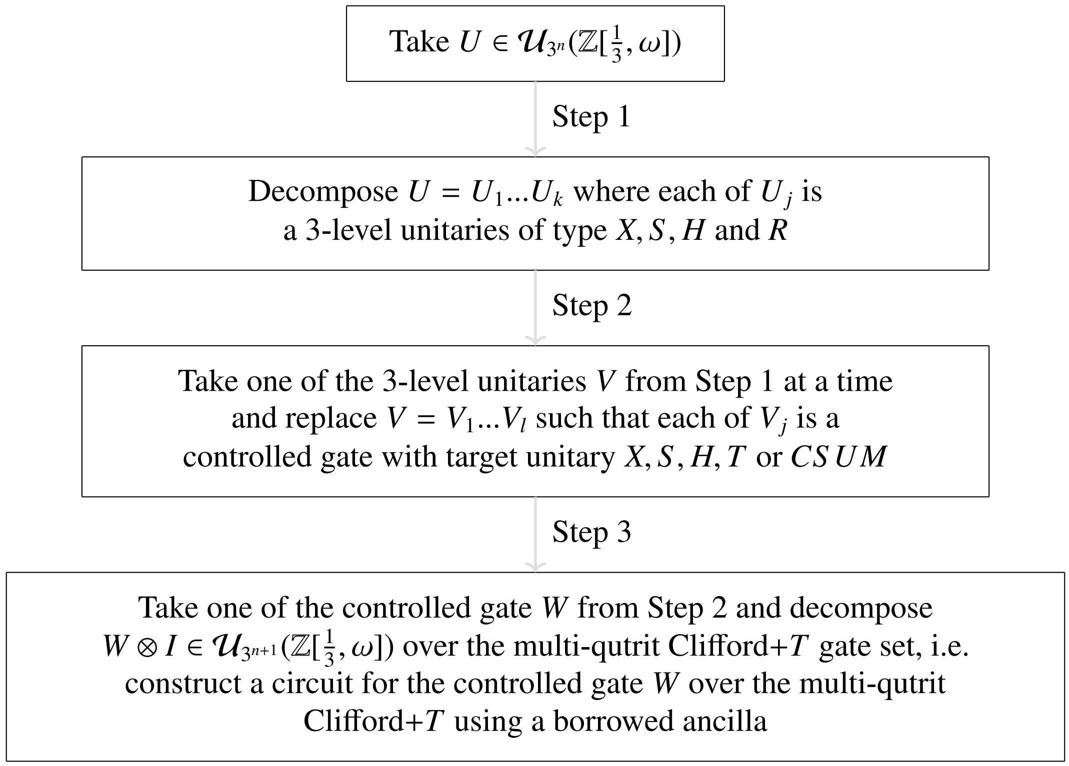


Figure 5.7: Roadmap for the algorithm in Theorem 5.3.1

the relationship $j_2 \leq j_1 \leq j_3$, then

$$M = \begin{array}{c|c|c|c|c|c|c|c} & & j_2 & & j_1 & & j_3 & \\ \hline & I & & & & & & \\ j_2 & & b_2 & & b_1 & & b_3 & \\ & & & I & & & & \\ j_1 & & a_2 & & a_1 & & a_3 & \\ & & & & & I & & \\ j_3 & & c_2 & & c_1 & & c_3 & \\ & & & & & & & I \end{array}$$

We denote the above matrix as $U_{[j_1, j_2, j_3]}$.

Definition 5.3.3 (1 and 2-level matrices)**.** We define *1-level* and *2-level matrices* similarly to the above definition. For $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2$, a 1-level matrix of type a and 2-level matrices U

has the form:

$$[a]_{[j]} = \begin{array}{c} \\ j \\ \\ \end{array}\!\!\overset{\begin{array}{ccc} & j & \end{array}}{\left(\begin{array}{c|c|c} I & & \\ \hline & a & \\ \hline & & I \end{array}\right)}, \qquad U_{[j,l]} = \begin{array}{c} \\ j \\ \\ l \\ \\ \end{array}\!\!\overset{\begin{array}{ccccc} & j & & l & \end{array}}{\left(\begin{array}{c|c|c|c|c} I & & & & \\ \hline & a & & b & \\ \hline & & I & & \\ \hline & c & & d & \\ \hline & & & & I \end{array}\right)}$$

respectively.

Remark 5.3.4. Note that by definition, if the size of the matrix is greater than or equal to 3, then all 1-level and 2-level are also 3-level matrices. In particular, if the size of the matrix is greater than or equal to 3, then a 3-level unitary of type S or R is equivalent to a 1-level unitary of type ω or -1 respectively.

We use the map $\mathcal{P} : \mathbb{Z}[\omega] \to \mathbb{Z}/3\mathbb{Z}$ defined by $g(\omega) \mapsto g(1) \pmod 3$. Recall that $g \in \chi\mathbb{Z}[\omega]$ iff $\mathcal{P}(g) = 0$, and additionally, $g \in \chi^2\mathbb{Z}[\omega]$ iff $\mathcal{P}(g) = g(1) = 0$ and $\mathcal{P}(g') = g'(1) = 0$ where $g'(\omega)$ is the formal derivative of g with respect to the formal variable ω [KVM23].

Lemma 5.3.5. *Let* $\mathbf{u} \in \mathbb{Z}[\frac{1}{3}, \omega]^m$ *be an m-dimensional column vector of norm 1 and sde 0. Then* $\mathbf{u}$ *is some permutation of* $(\pm\omega^a, 0, ..., 0)^t$ *for some* $a \in \mathbb{Z}$.

Proof. As $\text{sde}(\mathbf{u}) = 0$, so $\mathbf{u} = (u_1, ..., u_m) \in \mathbb{Z}[\omega]^m$. Let $u_j = a_j\omega + b_j$ for some $a_j, b_j \in \mathbb{Z}$. Using the fact that the norm of $\mathbf{u}$ is 1, we get the equation

$$\sum_{j=1}^{m} a_j^2 + b_j^2 - a_j b_j = 1.$$

Clearly, up to permutation the only solutions for the above equation are i) $a_1 = \pm 1$ and all the other variables are 0, ii) $b_1 = \pm 1$ and all the other variables are 0, and iii) $(a_1, b_1) = (1, 1)$ or $(-1, -1)$ and all other variables are 0. In all these cases, we see that $u_1 = \pm\omega^a$ for some $a \in \mathbb{Z}$. This proves our statement. □

Lemma 5.3.6. *Let* $m = 1$ *or* 2. *If* $\mathbf{u} \in \mathbb{Z}[\frac{1}{3}, \omega]^m$ *is a unit vector then* $\text{sde}(\mathbf{u}) = 0$.

Proof. To the contrary, suppose $\text{sde}(\mathbf{u}) = f > 0$ and $\mathbf{u}$ is a unit vector. Then we have $\chi^f \mathbf{u} = \mathbf{v}$ for some $\mathbf{v} = (v_1, ..., v_m)^t \in \mathbb{Z}[\omega]^m$ but $\chi^{f-1}\mathbf{u} \notin \mathbb{Z}[\omega]^m$. Applying $\mathcal{P}$ to both sides of $\sum_{j=1}^{m} |v_j|^2 = |\chi|^{2f}$, we obtain:

$$\sum_{j=1}^{m} \mathcal{P}(v_j)^2 = 0.$$

Since $\mathcal{P}(v_j)^2$ can be either 0 or 1 and $m < 3$, so we get that $\mathcal{P}(v_j)$ must be 0 for all j, i.e. $v_j \in \chi\mathbb{Z}[\omega]$, i.e. $\mathbf{v} \in \chi\mathbb{Z}[\omega]^m$. Then $\chi^{f-1}\mathbf{u} = \mathbf{v} \in \chi\mathbb{Z}[\omega]^m$, a contradiction. □

Corollary 5.3.7. *Let $m \in \{1, 2\}$ and $\mathbf{u} \in \mathbb{Z}[\frac{1}{3}, \omega]^m$ be a column vector of norm 1. Then there exists a sequence $U_1, ..., U_k$ of 2-level unitaries of type $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; and 1-level unitaries of type ω and -1 such that $U_1...U_k\mathbf{u} = (1)$ for $m = 1$ and $U_1...U_k\mathbf{u} = (1, 0)^t$ for $m = 2$.*

Proof. By Lemma 5.3.6 we get that $\text{sde}(\mathbf{u}) = 0$. Using Lemma 5.3.5, we get that $\mathbf{u} = (\pm\omega^a)$ or $\mathbf{u} = (\pm\omega^a, 0)$ or $(0, \pm\omega^a)$ respectively for $m = 1$ and 2. Therefore, we can use a sequence of unitaries of the form $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or 1-level unitaries of type ω and -1 to convert $\mathbf{u}$ into $(1, 0)$ or (1) respectively for $m = 1$ and 2. □

Lemma 5.3.8. *Let $m \geq 3$ and $\mathbf{u} \in \mathbb{Z}[\frac{1}{3}, \omega]^m$ be a unit vector with sde $f > 0$. Then there exists a sequence $U_1, ..., U_k$ of 3-level unitaries of type X, H and S; and 1-level unitaries of type -1 such that the sde of all the entries of the resulting column $U_1, ..., U_k\mathbf{u}$ is at most $f - 1$.*

Proof. We have $\chi^f\mathbf{u} = \mathbf{v}$ for some $\mathbf{v} = (v_1, ..., v_m)^t \in \mathbb{Z}[\omega]^m$ but $\chi^{f-1}\mathbf{u} \notin \mathbb{Z}[\omega]^m$, i.e. there exists at least one j such that $v_j \notin \chi\mathbb{Z}[\omega]$. Since $||\mathbf{u}|| = 1$, we have

$$\sum_{j=1}^{m} |v_j|^2 = |\chi|^{2f}.$$

We apply the map $\mathcal{P}$ to get that

$$\sum_{j=1}^{m} \mathcal{P}(v_j)^2 = 0.$$

Since $\mathcal{P}(v_j)^2$ can be 0 or 1, therefore we see that the number of $j \in \{1, ..., m\}$ such that $\mathcal{P}(v_j)^2 = 1$ is a multiple of 3, i.e. the number of j such that $v_j \notin \chi\mathbb{Z}[\omega]$ is $3l$ for some $l \geq 1$. In other words, the number of entries of $\mathbf{u}$ which has sde strictly greater than $f - 1$ is of the form $3l$ for some $l \geq 1$.

We use induction on l to prove this lemma.

- **Base case** $l = 1$: There exists $j_1, j_2, j_3 \in \{1, ..., m\}$ (denote $\mathcal{I} = \{j_1, j_2, j_3\}$) such that $\mathcal{P}(v_j)^2 = 1$ for all $j \in \mathcal{I}$ and $\mathcal{P}(v_j)^2 = 0$ for all $j \notin \mathcal{I}$ (i.e. $v_j \in \chi\mathbb{Z}[\omega]$ for all $j \notin \mathcal{I}$). First notice that $\mathcal{P}(v_j) = 1$ or -1 for all $j \in \mathcal{I}$. If $\mathcal{P}(v_{j_i}) = -1$ for some $j_i \in \mathcal{I}$, we can use a one level unitary $[-1]_{[j_i]}$ so that $\mathcal{P}(v_{j_i}) = 1$. Therefore after the application of the above 3-level matrices, we have $\mathcal{P}(v_j) = 1$ for all $j \in \mathcal{I}$. Let $\tilde{\mathbf{v}}$ be the column of the column of size 3 having the entries v_{j_1}, v_{j_2} and v_{j_3} in its 1st, 2nd and 3rd entries respectively. Let

$\tilde{\mathbf{u}} = \frac{1}{\chi^f}\tilde{\mathbf{v}}$, then

$$HS^a\tilde{\mathbf{u}} = \frac{\omega^2}{\chi^{f+1}}\begin{pmatrix} v_{j_1} + v_{j_2} + \omega^a v_{j_3} \\ v_{j_1} + \omega v_{j_2} + \omega^{a+2} v_{j_3} \\ v_{j_1} + \omega^2 v_{j_2} + \omega^{a+1} v_{j_3} \end{pmatrix}$$

Let $g_1 = v_{j_1} + v_{j_2} + \omega^a v_{j_3}, g_2 = v_{j_1} + \omega v_{j_2} + \omega^{a+2} v_{j_3}$ and $v_{j_1} + \omega^2 v_{j_2} + \omega^{a+1} v_{j_3}$ in $\mathbb{Z}[\omega]$. Then we see that $\mathcal{P}(g_1) = \mathcal{P}(g_2) = \mathcal{P}(g_3) = 0$. We will choose $a \in \mathbb{Z}/3\mathbb{Z}$ such that $g_j \in \chi^2\mathbb{Z}[\omega]$ for each $j \in \{1, 2, 3\}$. We have

$$\begin{aligned}
g_1'(\omega) &= v_{j_1}' + v_{j_2}' + a\omega^{a-1} v_{j_3} + \omega^a v_{j_3}' \\
\mathcal{P}(g_1') &= a + \sum_{j\in\mathcal{I}} \mathcal{P}(v_j') \\
g_2'(\omega) &= v_{j_1}' + v_{j_2} + \omega v_{j_2}' + (a+2)\omega^{a+1} v_{j_3} + \omega^{a+2} v_{j_3}' \\
\mathcal{P}(g_2') &= a + 3 + \sum_{j\in\mathcal{I}} \mathcal{P}(v_j') = \mathcal{P}(g_1') \\
g_3'(\omega) &= v_{j_1}' + 2\omega v_{j_2} + \omega^2 v_{j_2}' + (a+1)\omega^a v_{j_3} + \omega^{a+1} v_{j_3}' \\
\mathcal{P}(g_3') &= a + 3 + \sum_{j\in\mathcal{I}} \mathcal{P}(v_j') = \mathcal{P}(g_1')
\end{aligned}$$

We choose $a \in \mathbb{Z}/3\mathbb{Z}$ such that $a + \sum_{j\in\mathcal{I}} \mathcal{P}(v_j') = 0$, then $\mathcal{P}(g_j') = 0$ for $j \in \{1, 2, 3\}$. Combining with $\mathcal{P}(g_j) = 0$, we see that $g_j \in \chi^2\mathbb{Z}[\omega]$. Therefore we have

$$HS^a\tilde{\mathbf{u}} = \frac{\omega^2}{\chi^{f-1}}\begin{pmatrix} \frac{g_1}{\chi^2} \\ \frac{g_2}{\chi^2} \\ \frac{g_3}{\chi^2} \end{pmatrix} \text{ with } g_j \in \chi^2\mathbb{Z}[\omega], \text{ i.e } \chi^{f-1} HS^a\tilde{\mathbf{u}} \in \mathbb{Z}[\omega]^m.$$

Therefore all entries of $HS^a\tilde{\mathbf{u}}$ have sde at most $f - 1$. Hence l decreased from 1 to 0 and our base case of the inner induction is done.

- **Induction step:** For the induction step we pick any 3 of the indices $j_1, j_2, j_3 \in \{1, ..., m\}$ such that $\mathcal{P}(v_{j_1}), \mathcal{P}(v_{j_2})$ and $\mathcal{P}(v_{j_3})$ are non-zero and use the base case algorithm to lower l by 1. Then from the induction hypothesis, the statement of the lemma follows.

□

Lemma 5.3.9. *Let $m \geq 3$ and $\mathbf{u} \in \mathbb{Z}[\frac{1}{3}, \omega]^m$ be an m-dimensional column vector of norm 1. Then there exists a sequence $U_1, ..., U_k$ of 3-level unitaries of type X, S and H; and 1-level unitaries of type ω and -1 such that $U_1 ... U_k\mathbf{u} = (1, 0, ..., 0)^t$.*

Proof. Suppose the sde of $\mathbf{u} = (u_1, ..., u_m)^t \in \mathbb{Z}[\frac{1}{3}, \omega]^m$ is f. If f is non-zero, by Lemma 5.3.8, there exists a sequence $U_1, ..., U_{k'}$ of 3-level and 1-level unitaries such that sde of $U_1 ... U_{k'}\mathbf{u}$ is at least 1 less than that of **u** . We can inductively proceed this way to find 3-level and 1-level unitaries $U_1, \ldots, U_k$ such that sde of $U_1 \ldots U_k\mathbf{u}$ is 0. By Lemma 5.3.5, this column of sde 0 is equal to $(\pm\omega^a, 0, 0, ..., 0)$ up to permutation. We use a 3-level unitary of type H^2 and 1-level unitaries of type ω and -1 to get $(1, 0, ..., 0)^t$. □

Lemma 5.3.10. *Let $U \in \mathcal{U}_m(\mathbb{Z}[\frac{1}{3}, \omega])$. Then there exists a sequence $U_1, ..., U_k$ of 3-level unitaries of type X, S and H; 2-level unitaries of type $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; and 1-level unitaries of type ω and -1 such that $U_1....U_kU = I$.*

Proof. We prove this using induction on m. By Lemma 5.3.7, the base case is done. Now, let **u** be the first column of U. Then using Corollary 5.3.7 and Lemma 5.3.9, there exists a sequence $U_1, ..., U_{k_1}$ of 3-level unitaries of type X, S and H; 2-level unitaries of type $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; and 1-level unitaries of type ω and -1 such that

$$U_1...U_{k_1}\mathbf{u} = (1, 0, ..., 0)^t.$$

Therefore we have

$$U_1...U_{k_1}U = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & U' \end{array}\right).$$

Using the induction hypothesis on the unitary U' of size $m - 1$, the statement of the lemma follows. □

Lemma 5.3.11. *Let $U \in \mathcal{U}_m(\mathbb{Z}[\frac{1}{3}, \omega])$. Then there exists a sequence $U_1, ..., U_k$ of 3-level unitaries of type X, S and H; 2-level unitaries of type $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; and 1-level unitaries of type ω and -1 such that $U = U_1....U_k$.*

Proof. A consequence of Lemma 5.3.10 after observing that $X^{-1} = X^2, S^{-1} = S^2, H^{-1} = H^3, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \omega^{-1} = \omega^2$ and $(-1)^{-1} = -1$. □

5.3.2 Conversion to controlled gates

Our next task is to convert these level-unitaries to controlled gates. Let us first define what they are and observe that when the level-unitaries are of a particular form, they already are useful controlled gates.

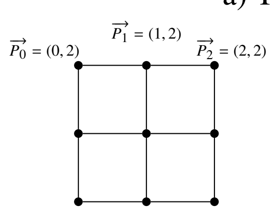
Observation 5.3.12. *Let $M \in \mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega])$ be a 3-level unitary of type $U \in \mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, \omega])$. We rename the row and column indices of the matrix M as a n-tuple $\vec{P} = (p_1, ..., p_n) \in \{0, 1, 2\}^n$ with lexicographic ordering.*

Define Δ^n to be the graph in $\mathbb{R}^n$ with the set of vertices $\{(x_1, ..., x_n) : x_1, ..., x_n \in \{0, 1, 2\}\}$ and there is an edge between two vertices if and only if the two vertices differ exactly at one coordinate and where they differ, the difference between the coordinates is exactly 1. This graph is nothing but the higher-dimensional grid with 3-points in each coordinate direction (Δ^2, for example, is the grid shown in Figures 5.8 5.9, 5.10 and 5.11). We associate the data '$(\Delta^n, \overrightarrow{P_0}, \overrightarrow{P_1}, \overrightarrow{P_2})$' with the 3-level unitary $M = U_{[\overrightarrow{P_0}, \overrightarrow{P_1}, \overrightarrow{P_2}]}$. For example, the picture of Figure 5.8 b) is associated with the 3-level unitary $U_{[(0,2),(1,2),(2,2)]}$ shown in Figure 5.8 a).

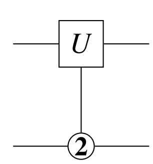
We observe that if the three points $\overrightarrow{P_0}, \overrightarrow{P_1}$, and $\overrightarrow{P_2}$ are in a straight line along an edge of Δ^n (i.e. $n-1$ of the corresponding coordinates are the same for all the three points), then M is an $(n-1)$-multiply-controlled-$(X_{\sigma^{-1}} U X_\sigma)$ gate for some $\sigma \in S_3$. If the three points are already in the correct order corresponding to the rows of U, then M is already a controlled-U gate (as illustrated in Figure 5.8 for $n = 2$). However, if the three points are in a straight line, but the order of the rows and columns is incorrect, we just need to conjugate it with a controlled-X_σ gate to get a controlled-U gate (as illustrated in Figure 5.9 for $n = 2$).

$$U_{[(0,2),(1,2),(2,2)]} = \left(\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_1 & 0 & 0 & a_2 & 0 & 0 & a_3 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & b_1 & 0 & 0 & b_2 & 0 & 0 & b_3 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & c_1 & 0 & 0 & c_2 & 0 & 0 & c_3 \end{array}\right)$$

a) The initial 3-level unitary



b) The points are already in a straight line and the rows and the columns are already in the correct order

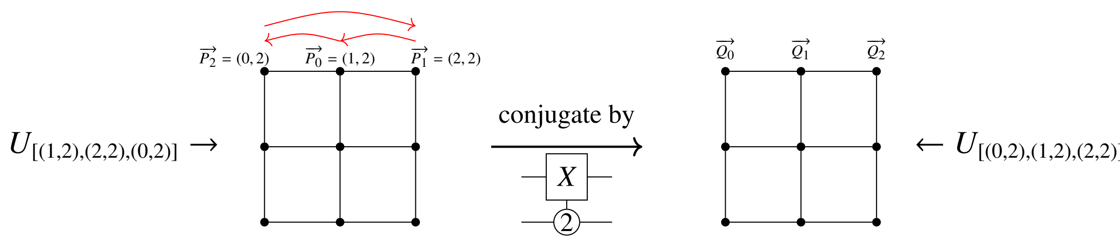


c) The 3-level unitary is equal to the above controlled-U gate

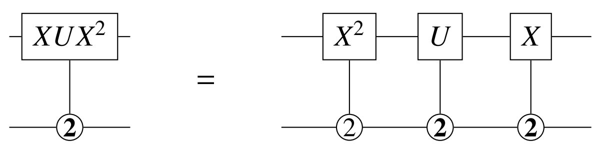
Figure 5.8: The 3-level unitary $U_{[(0,2),(1,2),(2,2)]}$ is already a controlled-U gate

$$U_{[(1,2),(2,2),(0,2)]} = \left(\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c_3 & 0 & 0 & c_1 & 0 & 0 & c_2 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_3 & 0 & 0 & a_1 & 0 & 0 & a_2 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b_3 & 0 & 0 & b_1 & 0 & 0 & b_2 \end{array}\right)$$

a) The initial 3-level unitary



b) Permute the rows and columns to the correct order



c) The final circuit for $U_{[(1,2),(2,2),(0,2)]}$

Figure 5.9: The equivalent circuit for $U_{[(1,2),(2,2),(0,2)]}$ using controlled gates

Lemma 5.3.13. *[KSaikia+] Let $M \in \mathcal{U}_m(\mathbb{Z}[\frac{1}{3}, \omega])$ be a 3-level unitary of type $U \in \mathcal{U}_3(\mathbb{Z}[\frac{1}{3}, \omega])$ such that $3^{n-1} < m \leq 3^n$ for some $n \geq 2$. Let $m' = 3^n - m$, then the unitary $I_{m'} \oplus M \in \mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega])$ can be decomposed into n-qutrits gates consisting of $|2\rangle^{\otimes(n-1)}$-controlled-X, $|2\rangle^{\otimes(n-1)}$-controlled-H and a controlled-U gate.*

Proof. Let $M' = I_{m'} \oplus M$. Then M' is also a 3-level unitary of type U. We rename the row and column indices of the matrix M' as a n-tuple $\vec{P} = (p_1, ..., p_n) \in \{0, 1, 2\}^n$ with lexicographic ordering. Suppose $M' = U_{[\vec{P_0}, \vec{P_1}, \vec{P_2}]}$.

Suppose $\{\vec{P_0}, \vec{P_1}, \vec{P_2}\}$ and $\{\vec{Q_0}, \vec{Q_1}, \vec{Q_2}\}$ are two set vertices of Δ^n such that there are two common points in these sets, without loss of generality say $\vec{P_1} = \vec{Q_1}$ and $\vec{P_2} = \vec{Q_2}$. Further assume that $(n-1)$ corresponding coordinates of $\vec{P_0}$ and $\vec{Q_0}$ are the same, wlog assume that only the n-th coordinate of $\vec{P_0}$ and $\vec{Q_0}$ differ. Then observe that $VU_{[\vec{P_0}, \vec{P_1}, \vec{P_2}]}V^{-1} = U_{[\vec{Q_0}, \vec{Q_1}, \vec{Q_2}]}$ where V is the multi-controlled-X^j gate with target at n-th wire and $j \in \{1, 2\}$ is chosen such that X^j takes the n-th coordinate of $\overrightarrow{P_0}$ to the n-th coordinate of $\overrightarrow{Q_0}$.

Therefore, movements of a point along the paths of Δ^n from one vertex to another vertex that changes only one of the coordinates of the point corresponds to conjugating M' by an $(n-1)$-multiply-controlled-permutation gate with the target on the wire where the coordinate changes and controls on all other $n-1$ wires (as illustrated in Figure 5.10).

The idea is to travel along the edges of the graph Δ^n to start from $\overrightarrow{P_j}$ and end up in $\overrightarrow{P'_j}$ such that the points $\overrightarrow{P'_0}, \overrightarrow{P'_1}$ and $\overrightarrow{P'_2}$ are in a straight line along an edge of Δ^n so that we get the cases of the Observation 5.3.12 (as illustrated in Figures 5.10 and 5.11 for $n = 2$).

Finally, by Remark 5.2.5 and 5.2.6, the statement of the lemma follows. □

Remark 5.3.14. The procedure in the above lemma is an analogue of the Gray code construction [NC10, Section 4.5.2] for qutrits. Further, note that we can extend the same procedure to convert any d-level unitaries (similar to 3-level unitaries) into controlled-qudit gates. In that case, we replace Δ^n by the graph Δ^n_d where Δ^n_d is the graph in $\mathbb{R}^n$ with the set of vertices $\{(x_1, ..., x_n) : x_1, ..., x_n \in \{0, 1, ..., d-1\}\}$ and there is an edge between two vertices if and only if the two vertices differ exactly at one coordinate and where they differ, the difference between the coordinates is exactly 1. All other arguments used in the proof of Lemma 5.3.13 can also be mimicked for qudits.

5.3.3 Exact synthesis over Clifford+T

Lemma 5.3.15. *Let $U \in \mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega])$ and $n \geq 2$. Then U can be decomposed into a sequence of $|2\rangle^{\otimes(n-1)}$-controlled gates with target unitaries X, S, H and R.*

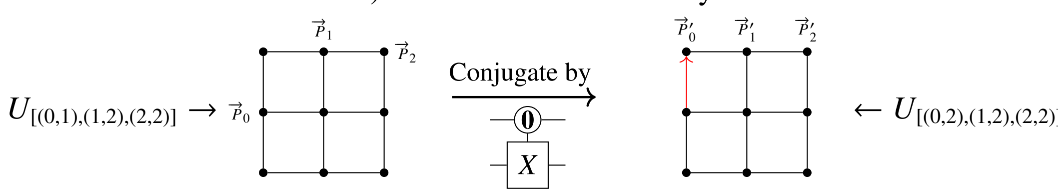
Proof. Using Lemma 5.3.11 we see that $U \in \mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega])$ can be decomposed into 3-level unitaries of type X, S and H; 2-level unitaries of type $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; and 1-level unitaries of type ω and -1. Since $3^n \geq 3^2 > 3$, so a 1-level unitary of type -1 or ω is equivalent to a 3-level unitary of type $X^j R X^{3-j}$ or $X^j S X^{3-j}$ respectively for some $j \in \{1, 2\}$. Further, a two-level unitary of type $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is equivalent to a 3-level unitary of type H^2. Therefore, U can be decomposed into a sequence of 3-level unitaries of type X, S, H and R.

Using Lemma 5.3.13, we see that any such 3-level unitaries can be decomposed into $|2\rangle^{\otimes(n-1)}$-controlled gates with target unitaries X, S, H and R. □

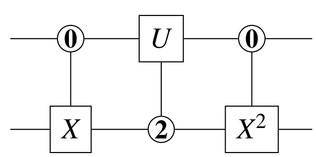
At this point, we are in the final stage of the algorithm of Theorem 5.3.1. The final stage is to decompose the controlled gates we have in the above lemma (Lemma 5.3.15) over the multi-qutrit Clifford+T gate set.

$$U_{[(0,1),(1,2),(2,2)]} = \left(\begin{array}{ccc|ccc|ccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a_1 & 0 & 0 & 0 & a_2 & 0 & 0 & a_3 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & b_1 & 0 & 0 & 0 & b_2 & 0 & 0 & b_3 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & c_1 & 0 & 0 & 0 & c_2 & 0 & 0 & c_3
\end{array}\right)$$

a) The initial 3-level unitary



b) Put the three points onto a line of the grid

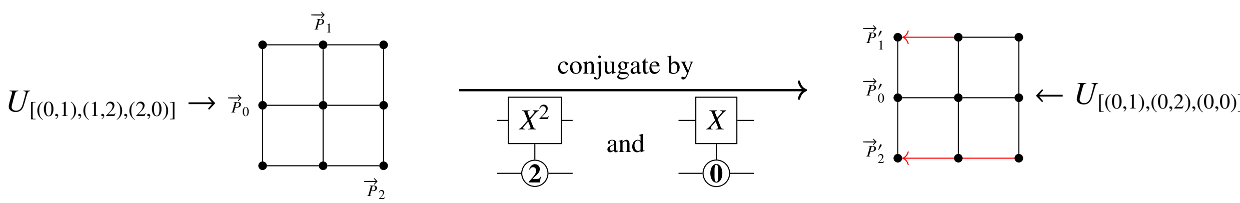


c) The final circuit for $U_{[(0,1),(1,2),(2,2)]}$

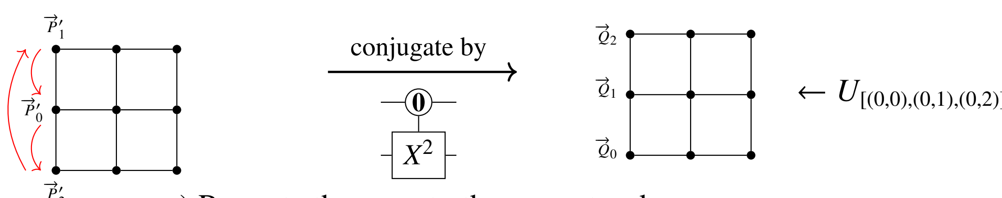
Figure 5.10: The equivalent circuit for $U_{[(0,1),(1,2),(2,2)]}$ using controlled gates

$$
U_{[(0,1),(1,2),(2,0)]} = \left(\begin{array}{ccc|ccc|ccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a_1 & 0 & 0 & 0 & a_2 & a_3 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & b_1 & 0 & 0 & 0 & b_2 & b_3 & 0 & 0 \\
\hline
0 & c_1 & 0 & 0 & 0 & c_2 & c_3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

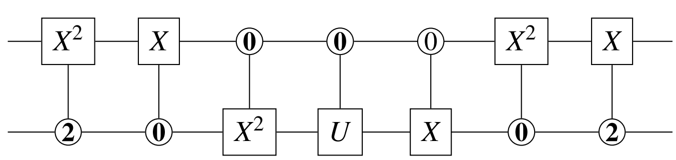
a) The initial 3-level unitary



b) First put the three points onto a line of the grid



c) Permute the rows to the correct order



d) Final circuit for $U_{[(0,1),(1,2),(2,0)]}$

Figure 5.11: The equivalent circuit for $U_{[(0,1),(1,2),(2,0)]}$ using controlled gates

Observation 5.3.16. *Note that the $|2\rangle^{\otimes(n-1)}$-controlled-X with target unitary X at n-th wire can be made using multi-qutrit Clifford+T (as shown in [YW22, Lemma 6]). Here we provide the explicit circuit with our notations for $n = 3$ in Figure 5.12. The position of the target unitary X does not change the decomposition over Clifford+T by much (as illustrated in Figures 5.13 and 5.14).*

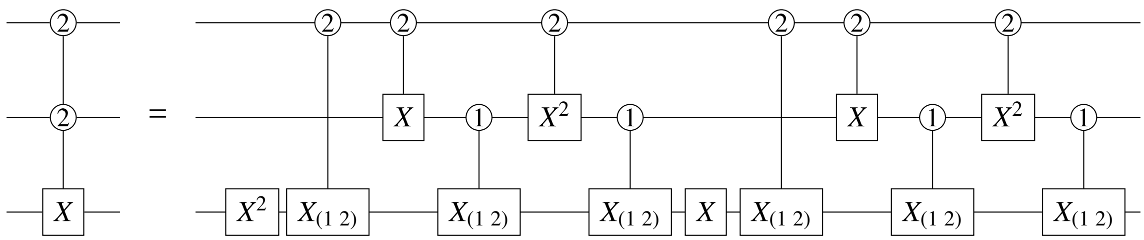


Figure 5.12: Decomposition of controlled-X gate with target at 3rd wire over Clifford+T

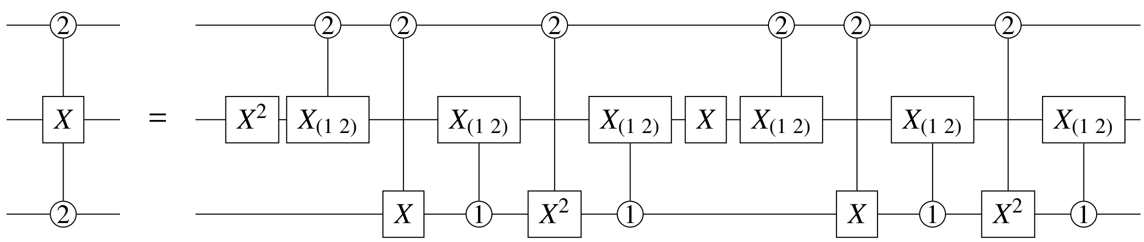


Figure 5.13: Decomposition of controlled-X gate with target at 2nd wire over Clifford+T

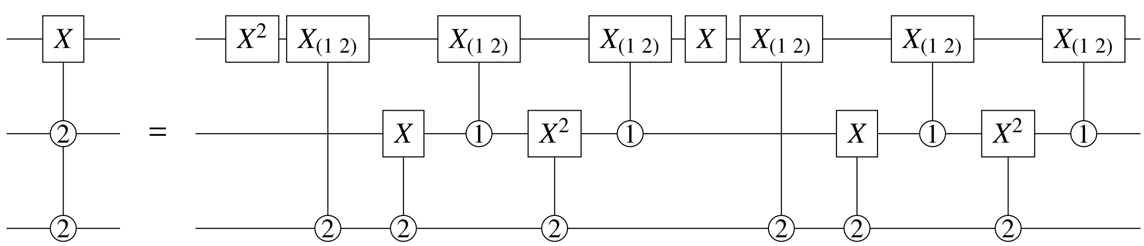


Figure 5.14: Decomposition of controlled-X gate with target at 1st wire over Clifford+T

As seen in the above observation, note that if we know a decomposition of a controlled-X gate over the multi-qutrit Clifford+T gate set, we can easily decompose all the other controlled-X gates over the multi-qutrit Clifford+T gate set. Therefore, finding the decomposition of the controlled-X gate with the target at n-th wire is sufficient for our purpose. We shall use this knowledge to see that the analogous statement for controlled-U gates for an arbitrary U also holds. This can be seen easily as the target unitary can be pushed to any wire by conjugating with appropriate controlled-X gates (as illustrated in Figure 5.15 for $n = 2$). Note that this can *be achieved using the same procedure described in Lemma 5.3.13 by choosing the appropriate straight line for the target unitary.*

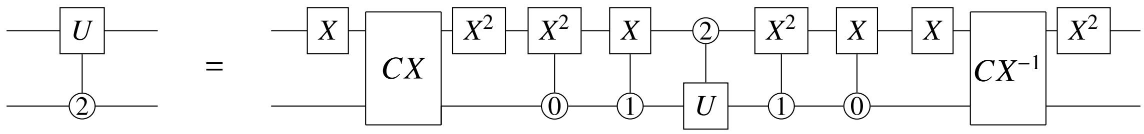


Figure 5.15: Relationship between different target positions for arbitrary U

Proof of Theorem 5.3.1. When $n = 1$, we have $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega]) =$ Clifford+R [KVM23] and so the statement of the theorem for $n = 1$ is essentially the same as [Gla+22, Corollary 23].

When $n \geq 2$, using Lemma 5.3.15, U can be decomposed into a sequence of $|2\rangle^{\otimes(n-1)}$-controlled gates with target unitaries X, S, H and R. Using Observation 5.3.16, it is enough to show that we can decompose $|2\rangle^{\otimes(n-1)}$-controlled gates with target unitaries S, H and R at the n-th wire over the multi-qutrit Clifford+T gate set.

- Using [YW22, Lemma 12], we can exactly decompose $|2\rangle^{\otimes(n-1)}$-controlled gates of type H into a multi-qutrit Clifford+T.
- If U' is a $|2\rangle^{\otimes(n-1)}$-controlled-S gate, then using [YW22, Lemma 11] we can exactly decompose $U' \otimes I$ into a multi-qutrit Clifford+T. Note that in [YW22], the authors use the language of borrowed ancilla, which is mathematically the same as decomposing $U' \otimes I$ into multi-qutrit Clifford+T using the ancillary system rather than decomposing U' itself.
- Using [Gla+22, Theorem 22], we can decompose $R \otimes I$ into a word in the set $\{H, X, S, T, CSUM\}$. Therefore, a $|2\rangle^{\otimes(n-1)}$-controlled-R gate is equal to composition of a few $|2\rangle^{\otimes n}$-controlled gates of type H, X, S, T and $|2\rangle^{\otimes(n-1)}$-controlled $CSUM$. Each of these controlled gates can be decomposed over the $(n+1)$-qutrit Clifford+T gate set [YW22, Lemma 12, Lemma 6, Lemma 11, Lemma 8, Lemma 7].

Hence we see that $U \in U_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega])$ can be decomposed into a circuit consisting of qutrit multi-qutrit Clifford+T gates with at most one borrowed ancilla. Mathematically equivalent to saying we have the embedding of groups $\Phi_n : \mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \omega]) \hookrightarrow (Clif + T)^{(n+1)}$ given by $U \mapsto U \otimes I$. □

5.4 Unitaries with entries from $\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}]$

In this section, we prove the second main theorem of this chapter. The proof of the theorem yields an algorithm to make an exact circuit for any unitary with entries from the ring $\mathbb{Z}[\frac{1}{3}, \zeta]$

over the multi-qutrit Clifford+T gate set. The theorem is a complete analogue for qutrits of the main result in [GS13] with the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$ replaced by the ring $\mathbb{Z}[\frac{1}{3}, \zeta]$ for single-qutrit Clifford+T.

Given a n-qutrit gate U with entries in the ring $\mathbb{Z}[\frac{1}{3}, \zeta]$, we will create a circuit equivalent to U using multi-qutrit Clifford+T gate set. We already know that single-qutrit Clifford+T is not enough to decompose single-qutrit gates with entries from $\mathbb{Z}[\frac{1}{3}, \zeta]$ (this is the same as single-qutrit Clifford+$\mathcal{D}$). Theorem 5.4.1, in particular $n = 1$, gives an algorithm to implement unitaries in single-qutrit Clifford+$\mathcal{D}$ over the multi-qutrit Clifford+T gate set, given we have two more ancillae.

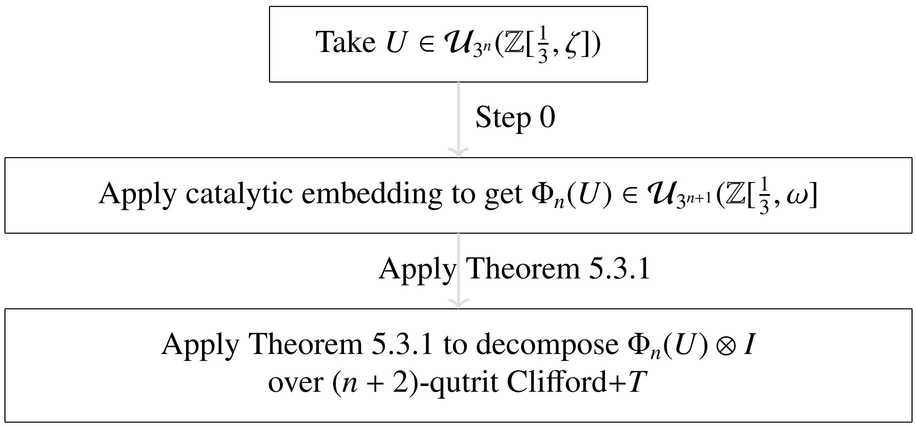


Figure 5.16: Roadmap for the algorithm of Theorem 5.4.1

Theorem 5.4.1. *[KSaikia+] Let U be a unitary $3^n \times 3^n$ matrix. Then U can be exactly represented by a quantum circuit over Clifford+T gate set, possibly using at most two ancillae if and only if the entries of U belong to the ring $\mathbb{Z}[\frac{1}{3}, \zeta]$. To be precise, there exists an embedding $\Psi_n : \mathcal{U}_{3^n}(\mathcal{R}) \hookrightarrow (Clif + T)^{n+2}$ and $|w\rangle \in (\mathbb{C}^3)^{\otimes 2}$ with the property*

$$\Psi_n(U)(|v\rangle \otimes |w\rangle) = (U\,|v\rangle) \otimes |w\rangle \quad \text{for all } |v\rangle \in (\mathbb{C}^3)^{\otimes n} \tag{5.1}$$

if and only if $\mathcal{R} = \mathbb{Z}[\frac{1}{3}, \zeta]$.

Proof. For the forward implication: note that $(Clif + T)^{n+2} \subset \mathcal{U}_{3^{n+2}}(\mathbb{Z}[\frac{1}{3}, \zeta])$. For $1 \leq j \leq 3^n$, we take $|v\rangle = |e_j\rangle$, the j-th standard basis element of $(\mathbb{C}^3)^{\otimes n}$ in Equation 5.1. Then we see that the j-th column of U is the first 3^n entries of the j-th column of $\Psi_n(U)$. Therefore the entries of the j-th column of U are from the ring $\mathbb{Z}[\frac{1}{3}, \zeta]$ and the the statement follows.

For the converse implication, we first use the catalytic embedding described in Section 5.2.3 to embed $\mathcal{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, \zeta])$ inside $\mathcal{U}_{3^{n+1}}(\mathbb{Z}[\frac{1}{3}, \omega])$. This step adds one ancilla (the catalyst involved in the embedding becomes the ancilla). Then we use Theorem 5.3.1 to construct a circuit over Clifford+T with at most one more ancilla. This concludes the theorem. ◻

Bibliography

[Amy+23] M. Amy, M. Crawford, A. N. Glaudell, M. L. Macasieb, S. S. Mendelson, and N. J. Ross. *Catalytic Embeddings of Quantum Circuits*. 2023. arXiv: 2305.07720 [quant-ph].

[Bal06] Werner Ballmann. *Lectures on Kähler Manifolds*. 2006. ISBN: 9783037195253. URL: https://api.semanticscholar.org/CorpusID:119824458.

[Ben+96a] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels". In: *Phys. Rev. Lett.* 76 (5 Jan. 1996), pp. 722–725. DOI: 10.1103/PhysRevLett.76.722.

[Ben+96b] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. "Mixed-state entanglement and quantum error correction". In: *Physical Review A* 54.5 (Nov. 1996), pp. 3824–3851. ISSN: 1094-1622. DOI: 10.1103/physreva.54.3824. URL: http://dx.doi.org/10.1103/PhysRevA.54.3824.

[Boc+16] Alex Bocharov, Xingshan Cui, Vadym Kliuchnikov, and Zhenghan Wang. "Efficient topological compilation for a weakly integral anyonic model". In: *Physical Review A* 93.1 (2016). DOI: 10.1103/physreva.93.012313. URL: https://doi.org/10.1103%2Fphysreva.93.012313.

[BP17] Tatyana Barron and Timothy Pollock. "Kähler quantization and entanglement". In: *Reports on Mathematical Physics* 80.2 (Oct. 2017), pp. 217–231. ISSN: 0034-4877. DOI: 10.1016/s0034-4877(17)30077-0.

[BPU95] D. Borthwick, T. Paul, and A. Uribe. "Legendrian distributions with applications to relative Poincaré series." In: *Inventiones mathematicae* 122.2 (1995), pp. 359–402.

[BS00] Stefan Berceanu and Martin Schlichenmaier. "Coherent state embeddings, polar divisors and Cauchy formulas". In: *Journal of Geometry and Physics* 34.3–4

(July 2000), pp. 336–358. ISSN: 0393-0440. DOI: 10.1016/s0393-0440(99)00075-3. URL: http://dx.doi.org/10.1016/S0393-0440(99)00075-3.

[BSaikia23] Tatyana Barron and Manimugdha Saikia. "Semiclassical asymptotics and entropy". In: *J. Phys.: Conf. Ser.* 2667 (2023). URL: https://arxiv.org/abs/2309.16881.

[BSaikia24] Tatyana Barron and Manimugdha Saikia. "Average entropy and asymptotics". In: *Journal of Korean Mathematical Society* 61.1 (2024), pp. 91–107. URL: https://arxiv.org/abs/2303.14629.

[BU96] David Borthwick and Alejandro Uribe. "Almost complex structures and geometric quantization". In: *Mathematical Research Letters* 3 (1996), pp. 845–861. URL: https://api.semanticscholar.org/CorpusID:2461008.

[BW00] Sean Bates and Alan Weinstein. *Lectures on the geometry of Quantization*. Vol. 8. Berkeley Mathematical Lecture Notes. American Mathematical Society, 2000.

[BW23] Tatyana Barron and Noah Wheatley. "Entanglement and products". In: *Linear and Multilinear Algebra* 71.5 (2023), pp. 756–767. URL: https://doi.org/10.1080/03081087.2022.2043817.

[BZ06] Ingemar Bengtsson and Karol Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2006.

[Car18] Andrea Carosso. *Geometric Quantization*. 2018. arXiv: 1801.02307 [math-ph].

[CC08] Lin Chen and Yi-Xin Chen. "Rank-three bipartite entangled states are distillable". In: *Physical Review A* 78.2 (Aug. 2008). ISSN: 1094-1622. DOI: 10.1103/physreva.78.022318.

[CD16] Lin Chen and Dragomir Ž. Doković. "Distillability of non-positive-partial-transpose bipartite quantum states of rank four". In: *Physical Review A* 94.5 (Nov. 2016). ISSN: 2469-9934. DOI: 10.1103/physreva.94.052318. URL: http://dx.doi.org/10.1103/PhysRevA.94.052318.

[CD23] Lin Chen and Tianyi Ding. "Entanglement distillation in terms of Schmidt rank and matrix rank". In: (2023). arXiv: 2304.05563 [quant-ph].

[CE19] Laurent Charles and Benoit Estienne. "Entanglement Entropy and Berezin–Toeplitz Operators". In: *Communications in Mathematical Physics* 376.1 (Nov. 2019), pp. 521–554. ISSN: 1432-0916. DOI: 10.1007/s00220-019-03625-y. URL: http://dx.doi.org/10.1007/s00220-019-03625-y.

[Cla05] Lieven Clarisse. "Characterization of distillability of entanglement in terms of positive maps". In: *Physical Review A* 71.3 (2005). ISSN: 1094-1622. DOI: 10.1103/physreva.71.032332. URL: http://dx.doi.org/10.1103/PhysRevA.71.032332.

[CLL21] Kwokwai Chan, Naichung Conan Leung, and Qin Li. "Quantization of Kähler manifolds". In: *Journal of Geometry and Physics* 163 (2021), p. 104143. ISSN: 0393-0440. DOI: 10.1016/j.geomphys.2021.104143. URL: http://dx.doi.org/10.1016/j.geomphys.2021.104143.

[DiV+00] David P. DiVincenzo, Peter W. Shor, John A. Smolin, Barbara M. Terhal, and Ashish V. Thapliyal. "Evidence for bound entangled states with negative partial transpose". In: *Physical Review A* 61.6 (May 2000). ISSN: 1094-1622. DOI: 10.1103/physreva.61.062312.

[Dok16] Dragomir Doković. "On Two-Distillable Werner States". In: *Entropy* 18.6 (June 2016), p. 216. ISSN: 1099-4300. DOI: 10.3390/e18060216.

[DP06] Marco Debernardi and Roberto Paoletti. "Equivariant Asymptotics for Bohr-Sommerfeld Lagrangian Submanifolds". In: *Communications in Mathematical Physics* 267.1 (Oct. 2006), pp. 227–263. DOI: 10.1007/s00220-006-0039-8.

[Dür+00] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß. "Distillability and partial transposition in bipartite systems". In: *Physical Review A* 61.6 (May 2000). ISSN: 1094-1622. DOI: 10.1103/physreva.61.062313. URL: http://dx.doi.org/10.1103/PhysRevA.61.062313.

[EP24] Shai Evra and Ori Parzanchevski. "Arithmeticity and covering rate of the 9-cyclotomic Clifford+ $\mathcal{D}$ gates in $PU(3)$". In: *arXiv preprint arXiv:2401.16120* (2024).

[FZ22] Pierre Flurin and Steve Zelditch. "Entropy of Bergman measures of a toric Kaehler manifold". In: *Pure Appl. Math.* 18.1 (2022). arXiv: 1909.08650 [math.CV].

[GH78] Phillip Griffiths and Joe Harris. *Principles of Algebraic Geometry*. 1978.

[GKM05] Janusz Grabowski, Marek Kuś, and Giuseppe Marmo. "Geometry of quantum systems: density states and entanglement". In: *Journal of Physics A: Mathematical and General* 38.47 (Nov. 2005), pp. 10217–10244. ISSN: 1361-6447. DOI: 10.1088/0305-4470/38/47/011. URL: http://dx.doi.org/10.1088/0305-4470/38/47/011.

[Gla+22] Andrew N. Glaudell, Neil J. Ross, John van de Wetering, and Lia Yeh. "Qutrit Metaplectic Gates Are a Subset of Clifford+T". en. In: Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. DOI: 10.4230/LIPICS.TQC.2022.12. URL: https://drops.dagstuhl.de/opus/volltexte/2022/16519/.

[Gla+24] Andrew N. Glaudel, Neil J. Ross, John van de Wetering, and Lia Yeh. *Exact Synthesis of Multiqutrit Clifford-Cyclotomic Circuits*. 2024. arXiv: 2405.08136 [quant-ph].

[GMT14] M. Greenfield, M. Marcolli, and K. Teh. "Twisted spectral triples and quantum statistical mechanical systems". In: *P-Adic Num Ultrametr Anal Appl* 6 (2014), pp. 81–104.

[GS13] Brett Giles and Peter Selinger. "Exact synthesis of multiqubit Clifford+ T circuits". In: *Physical Review A* 87.3 (2013), p. 032332.

[GUW16] V. Guillemin, A. Uribe, and Z. Wang. "Semiclassical States Associated with Isotropic Submanifolds of Phase Space". In: *Letters in Mathematical Physics* 106.12 (May 2016), pp. 1695–1728. ISSN: 1573-0530. DOI: 10.1007/s11005-016-0853-7.

[HHH96] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Separability of mixed states: necessary and sufficient conditions". In: *Physics Letters A* 223.1 (1996), pp. 1–8. ISSN: 0375-9601. DOI: https://doi.org/10.1016/S0375-9601(96)00706-2. URL: https://www.sciencedirect.com/science/article/pii/S0375960196007062.

[HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?" In: *Physical Review Letters* 80.24 (June 1998), pp. 5239–5242. ISSN: 1079-7114. DOI: 10.1103/physrevlett.80.5239.

[Hor+03] Pawel Horodecki, John A Smolin, Barbara M Terhal, and Ashish V Thapliyal. "Rank two bipartite bound entangled states do not exist". In: *Theoretical Computer Science* 292.3 (2003), pp. 589–596.

[HRŽ20] Paweł Horodecki, Łukasz Rudnicki, and Karol Życzkowski. *Five open problems in quantum information*. 2020. arXiv: 2002.03233 [quant-ph].

[Kir07] William D Kirwin. "Coherent states in geometric quantization". In: *Journal of Geometry and Physics* 57.2 (2007), pp. 531–548.

[Kli+15] Vadym Kliuchnikov, Alex Bocharov, Martin Roetteler, and Jon Yard. *A Framework for Approximating Qubit Unitaries*. 2015. arXiv: 1510.03888 [quant-ph].

[KMM13] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. “Fast and Efficient Exact Synthesis of Single-Qubit Unitaries Generated by Clifford and T Gates”. In: *Quantum Info. Comput.* 13.7–8 (2013), pp. 607–630. ISSN: 1533-7146.

[Kos70] Bertram Kostant. “Quantization and unitary representations”. In: *Lectures in Modern Analysis and Applications III*. Ed. by C. T. Taam. Berlin, Heidelberg: Springer Berlin Heidelberg, 1970, pp. 87–208. ISBN: 978-3-540-36417-7.

[KSaikia+] Amolak Ratan Kalra, Manimugdha Saikia, Dinesh Valluri, Sam Winnick, and Jon Yard. *Multi-qutrit exact synthesis*. 2024. arXiv: 2405.08147 [quant-ph].

[KVM23] Amolak Ratan Kalra, Dinesh Valluri, and Michele Mosca. “Synthesis and Arithmetic of Single Qutrit Circuits”. In: *arXiv preprint arXiv:2311.08696* (2023).

[KY15] Vadym Kliuchnikov and Jon Yard. “A framework for exact synthesis”. In: *arXiv preprint arXiv:1504.04350* (2015).

[Mei98] Eckhard Meinrenken. “Symplectic surgery and the Spinc–Dirac operator”. In: *Advances in mathematics* 134.2 (1998), pp. 240–277.

[Mir95] Rick Miranda. *Algebraic Curves and Riemann Surfaces*. 1995. DOI: 10.1090/gsm/005.

[MM00] Xiaonan Ma and George Marinescu. *Holomorphic Morse inequalities and Bergman kernels*. Vol. 8. Berkeley Mathematical Lecture Notes. American Mathematical Society, 2000.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[Pag93] Don N. Page. “Average entropy of a subsystem”. In: *Phys. Rev. Lett.* 71 (9 Aug. 1993), pp. 1291–1294. DOI: 10.1103/PhysRevLett.71.1291.

[Pao08] Roberto Paoletti. “A note on scaling asymptotics for Bohr-Sommerfeld Lagrangian submanifolds”. In: *Proceedings of the American Mathematical Society* 136.11 (2008), pp. 4011–4017.

[Per96] Asher Peres. “Separability Criterion for Density Matrices”. In: *Phys. Rev. Lett.* 77 (8 1996), pp. 1413–1415. DOI: 10.1103/PhysRevLett.77.1413. URL: https://link.aps.org/doi/10.1103/PhysRevLett.77.1413.

[Saikia24] Manimugdha Saikia. *Restrictions of holomorphic sections to products*. 2024. arXiv: 2403.17435 [math.DG].

[Sen96] Siddhartha Sen. “Average Entropy of a Quantum Subsystem”. In: *Phys. Rev. Lett.* 77 (1 July 1996), pp. 1–3. DOI: 10.1103/PhysRevLett.77.1.

[SHK11] Adam Sawicki, Alan Huckleberry, and Marek Kuś. “Symplectic Geometry of Entanglement”. In: *Communications in Mathematical Physics* 305.2 (May 2011), pp. 441–468. ISSN: 1432-0916. DOI: 10.1007/s00220-011-1259-0. URL: http://dx.doi.org/10.1007/s00220-011-1259-0.

[Sou67] Jean-Marie Souriau. “Quantification géométrique. Applications”. fre. In: *Annales de l’I.H.P. Physique théorique* 6.4 (1967), pp. 311–341. URL: http://eudml.org/doc/75556.

[SZ12] Jian Song and Steve Zelditch. “Test configurations, large deviations and geodesic rays on toric varieties”. In: *Advances in Mathematics* 229.4 (2012), pp. 2338–2378.

[SZ99] Bernard Shiffman and Steve Zelditch. “Distribution of Zeros of Random and Quantum Chaotic Sections of Positive Line Bundles”. In: *Communications in Mathematical Physics* 200.3 (Feb. 1999), pp. 661–683. ISSN: 1432-0916. DOI: 10.1007/s002200050544.

[Uhl10] Armin Uhlmann. “Roofs and Convexity”. In: *Entropy* 12.7 (July 2010), pp. 1799–1832. ISSN: 1099-4300. DOI: 10.3390/e12071799. URL: http://dx.doi.org/10.3390/e12071799.

[Wan+20] Yuchen Wang, Zixuan Hu, Barry C. Sanders, and Sabre Kais. “Qudits and High-Dimensional Quantum Computing”. In: *Frontiers in Physics* 8 (2020). ISSN: 2296-424X. DOI: 10.3389/fphy.2020.589504. URL: http://dx.doi.org/10.3389/fphy.2020.589504.

[Wer89] Reinhard F. Werner. “Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model”. In: *Phys. Rev. A* 40 (8 1989), pp. 4277–4281. DOI: 10.1103/PhysRevA.40.4277. URL: https://link.aps.org/doi/10.1103/PhysRevA.40.4277.

[Wil13] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[YW22] Lia Yeh and John van de Wetering. “Constructing All Qutrit Controlled Clifford+T gates in Clifford+T”. In: *Lecture Notes in Computer Science*. Springer International Publishing, 2022, pp. 28–50. ISBN: 9783031090059. DOI: 10.1007/978-3-031-09005-9_3. URL: http://dx.doi.org/10.1007/978-3-031-09005-9_3.

[Zel09] Steve Zelditch. “Bernstein polynomials, Bergman kernels and toric Kähler varieties”. In: *Journal of Symplectic Geometry* 7.2 (2009), pp. 51–76.

[Zhe00] F. Zheng. *Complex Differential Geometry*. AMS/IP studies in advanced mathematics. American Mathematical Society, 2000. ISBN: 9780821829608.

[ZZ21] Steve Zelditch and Peng Zhou. "Central limit theorem for toric Kähler manifolds". In: *Pure and Applied Mathematics Quarterly* 17.3 (2021), pp. 843–864.

Curriculum Vitae

Name:	Manimugdha Saikia
Post-Secondary Education and Degrees:	University of Western Ontario London, ON 2020 - 2024 PhD Candidate Mathematics.
	University of Western Ontario London, ON, Canada 2019-2020 MSc Mathematics.
	Indian Institute of Technology Guwahati Guwahati, Assam, India 2017-19 MSc Mathematics and Computing.
	Tezpur University Tezpur, Assam, India BSc (Major in Mathematics)
Related Work Experience:	Teaching Assistant, 2019-2024 University of Western Ontario

Publications:

1. A. R. Kalra, M. Saikia, D. Valluri, S. Winnick, J. Yard, Multi-qutrit exact synthesis over Clifford+T, arXiv: https://arxiv.org/abs/2405.08147

2. M. Saikia, Restrictions of holomorphic sections to products, arXiv: https://arxiv.org/abs/2403.17435.

3. T. Barron and M. Saikia, Semiclassical asymptotics and entropy, J. Phys.: Conf. Ser. 2667 (2023) 012050. DOI: doi.org/10.1088/1742-6596/2667/1/012050.

4. T. Barron and M. Saikia, Average entropy and asymptotics, J. Korean Math. Soc. 61 (2024), No. 1, pp. 91–107. DOI: doi.org/10.4134/JKMS.j230152