$SU(2)$-Irreducibly Covariant Quantum Channels and Some Applications

Muneerah Al Nuwairan

Thesis submitted to the Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics [1]

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

[1]The Ph.D. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

In this thesis, we introduce EPOSIC channels, a class of SU(2) -covariant quantum channels. For each of them, we give a Stinespring representation, a Kraus representation, its Choi matrix, a complementary channel, and its dual map. We show that these channels are the extreme points of all SU(2) -irreducibly covariant channels. As an application of these channels to the theory of quantum information, we study the minimal output entropy of EPOSIC channels, and show that a large class of these channels is a potential example of violating the well-known problem, the additivity problem. We determine the cases where their minimal output entropy is not zero, and obtain some partial results on the fulfillment of their entanglement breaking property. We find a bound of the minimal output entropy of the tensor product of two SU(2) -irreducibly covariant channels. We also get an example of a positive map that is not completely positive.

Résumé

Dans cette thèse, nous introduisons une classe de canaux quantiques, les canaux EPOSIC. Pour chacun d'entre eux, nous donnons leur représentation de Stinespring, leur décomposition de Kraus, leur matrice de Choi, leur canal complémentaire, et l'application duale. Nous montrons que ces canaux sont les points extrémaux de tous les canaux irréductibles SU(2)-covariants. En guise d'application de ces canaux à la théorie de l'information quantique, nous étudions l'entropie minimale de sortie des canaux EPOSIC, et montrons que beaucoup de ces canaux constituent des exemples potentiels de violation du célèbre problème d'additivité de l'entropie minimale de sortie. Nous déterminons les canaux pour lesquels l'entropie minimale de sortie est non nulle, et nous obtenons des résultats partiels pour la propriété de 'entanglement breaking' (cassage d'intrication). Nous trouvons une borne sur l'entropie minimale de sortie du produit tensoriel de deux canaux irréductibles SU(2)-covariants. Nous obtenons aussi un nouvel exemple d'application positive qui n'est pas complètement positive.

Acknowledgements

This thesis was done under the supervision of professors B. Collins and T. Giordano. I greatly appreciate their patient advice and help. I would also like to thank the Saudi Arabia government, and King Faisal University whose support enabled me to finish my studies and write this thesis.

Dedication

to my husband and children...

Contents

Introduction

According to Moore's law, the power of computers can be doubled for the same cost each two years [27, p.4]. Scientists believe that Moore's law might not apply by the 2020s, due to size difficulties. As a result, a lot of research efforts have been directed toward computing at the atomic level, where the classical laws don't apply, and the need for quantum laws appears. That was the birth of quantum information theory, which generalizes the classical one. Here is Holevo's description of quantum information theory in his address to the ICM in 2006 [17],

> The problem of data transmission and storage by quantum information carriers received increasing attention during past decade, owing to the burst of activity in the field of quantum information and computation. At present we are witnessing emergence of theoretical and experimental foundations of the quantum information science. It represents a new exciting research field addressing a number of fundamental issues in both quantum physics and in information and computer sciences. On the other hand, it provides a rich source of well-motivated mathematical problems.

In analogy to classical information theory, the quantum information one studies the protocols of quantum transmissions for quantum information. A *quantum channel* (a *channel*) is any method used to transfer the information from one or more quantum systems to other quantum systems. This transmission of information is not always accurate; the channel itself as well as the environment create noise which can cause information loss, and limit the efficiency of the quantum channel. *The classical capacity of the channel* is the maximum number of bits that can reliably be sent using the channel [35]. A fundamental problem in quantum information theory is to determine the classical capacity of a quantum channel. The additivity conjecture in quantum information is that the classical capacity of a quantum channel is additive, i.e, running two channels in parallel will not increase their total classical capacity. A fundamental result of quantum information theory, *The quantum coding theorem* [18, 32], shows that the additivity of the classical capacity can be inferred from the additivity of another quantity, known as *the Holevo bound* or *the Holevo capacity*. In 2000, C. King and M. Ruskai [25] introduced the notion of minimal output entropy, and P. Shor [36] (2004) showed that several conjectures in quantum information theory are all equivalent. In particular, the Holevo capacity is additive if and only if the minimal output entropy is. In 2008, Hastings [11] was able to show the existence of a counter-example to the additivity of the minimal output entropy, using a random construction. However, no explicit example was given.

In this thesis, we present an example of a new class of quantum channels, study their properties, and their minimal output entropy. The thesis consists of two parts. In Part I, we introduce the new channels, and study their properties. In Chapter 1, we review the basic definitions and state all the related propositions and lemmas from representation theory. In Chapter 2, we review the irreducible representations of the group $SU(2)$, and define an $SU(2)$-equivariant isometry. Chapter 3 contains all needed background results from quantum information theory. Chapter 4 is devoted to introducing and characterizing the new class of quantum channels, EPOSIC channels (the Extreme Points Of $SU(2)$-Irreducibly Covariant channels), to compute Kraus operators for them, and to find their Choi matrices. The chapter ends by giving an example of a positive map that is not completely positive, using EPOSIC channels. In Chapter 5, we study the $SU(2)$-irreducibly covariant channels, and show that EPOSIC channels are the extreme points of this set. Part II consist of three chapters, chapter 6 contains the definitions and all needed results about the minimal output entropy and the entanglement breaking property for a quantum channel (E.B.T). It also explains their relation to the additivity of classical capacity of quantum channel. In chapter 7, we study the minimal output entropy, and E.B.T property of the EPOSIC channels. Chapter 8 studies the minimal output entropy of the tensor product of two $SU(2)$-irreducibly covariant channels.

Contributions

In this section, we list the contributions of the thesis. We hope that our results will be a significant addition to the field of operator algebra and quantum information theory. Our main contributions can be summarized as follows:

1. Constructing EPOSIC channels (Proposition 4.1.1), a new class of quantum channels that form the extreme points of all $SU(2)$-irreducibly covariant channels (Corollary 5.1.5).

2. Giving a full description of the EPOSIC channel, by obtaining a Stinespring representation, a Kraus representation, the Choi matrix of the EPOSIC channel (Definition 4.2.1, and Proposition 4.3.5), computing a channel complementary to EPOSIC channel, and computing its dual map (Proposition 4.4.4, and Proposition 4.5.6).

3. Showing that any $SU(2)$-irreducibly covariant channel is an orthogonal direct sum of operators (Corollary 5.2.4).

4. For an $SU(2)$-irreducible subspace H, we give explicit formulae for the projections of $End(H)$ into its $SU(2)$-irreducible invariant subspaces (Proposition 2.4.2).

5. Proving that any completely positive $SU(2)$-irreducibly equivariant map is a multiple of an $SU(2)$-covariant channel (Corollary 5.1.6).

6. Obtaining an example of a positive, non-completely positive map (Proposition 4.6.3, and Proposition 4.6.5).

7. As applications in quantum information theory, we were able to

   (a) Determine the EPOSIC channels with zero minimal output entropy (Proposition 7.1.1, and Corollary 7.1.7).

   (b) Find a lower bound of the minimal output entropy of some of $SU(2)$-irreducibly covariant channels (Proposition 7.2.13).

   (c) Examine the entanglement breaking property of EPOSIC channel (Section 7.3).

   (d) Obtain an upper bound on the minimal output entropy for the tensor product of two $SU(2)$-irreducibly covariant channels (Corollary 8.2.4).

Part I

The Extreme Points of $SU(2)$-Irreducibly Covariant Quantum Channels

Chapter 1

Preliminaries in Representation Theory

The construction and study of the channels we present in this thesis depend heavily on the representations of the group $SU(2)$. The present chapter contains background definitions and results from representation theory that are needed for the thesis. For more details, we refer the reader to [3], [9], [13], [29], [33] and [38]. The definition of Hilbert spaces, and all related basic mathematical results are in Appendix **A**. In this thesis, we assume all vector spaces to be complex vector spaces of finite dimension.

1.1 Representations of compact groups

Definition 1.1.1. *A topological group is a set G which has both the structure of a group and a topological space, such that the group operations $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous. A compact group is a topological group whose topology is compact.*

Examples 1.1.2.

1. Any finite group endowed with the discrete topology is a compact group.

2. The unit circle under complex multiplication, and with the usual topology is an infinite compact group.

3. The real numbers $\mathbb{R}$ under the usual addition $+$, and with the usual topology is a non-compact topological group.

4. Let H be a finite dimensional complex vector space. The set of all invertible linear maps $A : H \longrightarrow H$ forms a group under composition, called *the general linear group*, denoted by $GL(H)$.

5. For $n \in \mathbb{N}$, let $\mathbb{M}_n(\mathbb{C})$ denote the set of $n \times n$-complex matrices. The subsets

   $U(n) = \{T \in \mathbb{M}_n(\mathbb{C}) : TT^* = I_n\}$ and $SL(n) = \{T \in \mathbb{M}_n(\mathbb{C}) : det(T) = 1\}$, form subgroups of $GL(n, \mathbb{C})$, called *the unitary group* and *the special linear group*, respectively. The unitary group $U(n)$, and its subgroup, *the special unitary group* $SU(n) = U(n) \cap SL(n)$, are compact topological groups.

Following [30, p.13, 128] and [37, p.21], we have:

Definition 1.1.3. *Let G be a group, and H be a vector space.*

1. *A representation of G in H is a group homomorphism $\pi_H : G \longrightarrow GL(H)$.*

   If H is a Hilbert space, and $\pi_{H(g)}$ is a unitary operator for each $g \in G$, we say π_H is a unitary representation.

2. *If G is a topological group, and H is a Banach space, then a continuous representation of G is a representation π_H such that the map*

$$G \times H \longrightarrow H$$

$$(g, h) \longmapsto \pi_{H(g)}(h), \qquad h \in H$$

   is continuous.

The space H is called *the representation space* of π_H. If H is finite dimensional, we say the representation is finite dimensional. The dimension of H is called the degree of the representation [37, p.21].

Notation 1.1.4. We denote a representation π_H of a group G in a Hilbert space H by $(H, \pi_H)_G$. If the group G is clear from context then we may omit the subscript G.

Examples 1.1.5.

1. Let G be a group, and H be a vector space. *The trivial representation* of G is the map $\pi_H : G \longrightarrow End(H)$ defined by taking any element $g \in G$ to the identity map on H.

2. For a locally compact group G there exist a left invariant (Haar) measure μ on G, where $L^2(G, d\mu) = \{f : G \longrightarrow \mathbb{C} : \int |f|^2 \, d\mu < \infty\}$ is a Hilbert space. The *left regular representation* of G in $L^2(G, d\mu)$ [30, p.132], is a unitary faithful representation of G.

3. Let $n \in \mathbb{N}$. By representing the vectors in $\mathbb{C}^n$ as $n \times 1$ matrices, the groups $U(n)$ and $SU(n)$ have representations in $\mathbb{C}^n$ given by matrix multiplication. These representations are called *the standard representations* of $U(n)$ and $SU(n)$ respectively [3, p.69].

Example 1.1.6. Let (H, π_H) be a representation of a group G. The following are representations of G in $\overline{H}$, where $\overline{H}$ denotes the conjugate space of H (see Appendix **A** for definition of $\overline{H}$).

1. $\check{\pi}_H : G \longrightarrow GL(\overline{H})$ by $\check{\pi}_{H(g)} = \pi^t_{H(g^{-1})}$, for $g \in G$.

2. $\overline{\pi}_H : G \longrightarrow GL(\overline{H})$ by $\overline{\pi}_{H(g)} = \overline{\pi_{H(g)}}$, for $g \in G$.

The representations $\check{\pi}_H$ and $\overline{\pi}_H$ are called *the contragredient*, and *the conjugate representation* of π_H respectively. They coincide when π_H is unitary.

Definition 1.1.7. *Let (H, π_H) be a representation of a group G. Then*

1. *A subspace W of H is called G* -invariant *if $\pi_{H(g)}(W) \subseteq W$ for each $g \in G$. The restriction of π_H to a G-invariant subspace is called a subrepresentation of π_H.*

2. *The space H is G-irreducible if it has no proper nonzero G-invariant subspaces. In this case, the representation π_H is called an* irreducible representation.

We restrict the use of the symbol ρ to irreducible representations.

Examples 1.1.8.

1. Any irreducible representation of an abelian group is one dimensional [8, p.71].

2. For $n \in \mathbb{N}$, let $\mathcal{S}_n$ be the symmetric group of $\{1, 2, ..., n\}$. The irreducible representations of $\mathcal{S}_n$ are in one-to-one correspondence with the partitions of n [9, p.44-54].

3. For $m, n \in \mathbb{N}$, let $\mathcal{P}(m, n)$ be the space of homogenous polynomials of degree m in n variables $x = (x_1, x_2, ..., x_n)$ over $\mathbb{C}$. The group $GL(n, \mathbb{C})$ has a representation in $\mathcal{P}(m, n)$ given by

$$\pi(g)(f(x)) = f(xg)$$

for $f \in \mathcal{P}(m, n)$ and $g \in GL(n, \mathbb{C})$, where xg denotes matrix multiplication.

For Hilbert spaces H and K, let $End(H, K)$ denote the vector space of linear maps from H to K. If H and K are finite-dimensional, then $End(H, K)$ is a Hilbert space endowed with the Hilbert-Schmidt inner product given by $\langle A \,|B \rangle_{End(H,K)} = tr(A^*B)$ for $A, B \in End(H, K)$. As usual, we write $End(H)$ for $End(H, H)$, and I_H for the identity map on H.

Proposition 1.1.9. *Let* (H, π_H) *and* (K, π_K) *be two representations of a group* G*. The map*

$$\pi_{H,K} : G \longrightarrow End(End(H, K))$$

$$g \longmapsto \pi_{K(g)} A \pi_{H(g^{-1})}$$

defines a representation of G *in* $End(H, K)$*. The representation* $\pi_{H,K}$ *is unitary if both* π_H *and* π_K *are.*

Proof:

It is straightforward to show that $\pi_{H,K}$ is a group homomorphism, given that π_H and π_K are. For $A, B \in End(H, K)$, we have:

$$\begin{aligned}\langle A \,|\pi_{H,K(g)}\, B\rangle_{End(H,K)} &= tr(A^* \pi_{K(g)} B \pi_{H(g^{-1})}) = tr(\pi_{H(g^{-1})} A^* \pi_{K(g)} B) \\ &= tr\left((\pi_{H,K(g^{-1})} A)^* \, B\right) = \langle \pi_{H,K(g^{-1})} A \,|B\rangle_{End(H,K)}\end{aligned}$$

By the uniqueness of the adjoint map, we have

$$(\pi_{H,K(g)})^* = \pi_{H,K}(g^{-1})$$

∎

Remark 1.1.10. If (H, π_H) and (K, π_K) are two representations of a group G, then unless specified otherwise, the representation of G on $End(H, K)$ will be taken to be the one as given in Proposition 1.1.9.

1.2 G-equivariant maps

In this section, we provide all needed information about G-equivariant maps. The first subsection contains the definitions and propositions. The second one presents a list of examples of G-equivariant maps that are required for the thesis.

1.2.1 Basic definitions and results

Definition 1.2.1. *[29, p.13] Let (H, π_H) and (K, π_K) be two representations of a group G. A linear map $\alpha : H \longrightarrow K$ is said to be G-equivariant if*

$$\pi_{K(g)}\alpha = \alpha\pi_{H(g)}$$

for all $g \in G$.

The set of G-equivariant maps forms a vector space, denoted $End(H, K)^G$, and called *the space of intertwining operators.* The space $End(H, H)^G$ is abbreviated to $End(H)^G$. Following [3, p.67], we have

Definition 1.2.2. *Let (H, π_H) and (K, π_K) be two representations of a group G. We say that the two representations are G-equivalent if there exists a G-equivariant isomorphism $\alpha : H \longrightarrow K$. In such a case, the spaces H and K are called G-equivalent, or G-isomorphic.*

Proposition 1.2.3. *Let G be a compact group. Then*

1. *Every representation of G in a Hilbert space is equivalent to a unitary representation [30, p.15].*

2. *Every representation of G in a Hilbert space is equivalent to a direct sum of irreducible representations [37, p.155-157], and [3, p.68].*

3. *Every irreducible representation of G in a Banach space is finite-dimensional [30, p.46].*

Henceforth, we assume all vector spaces to be complex vector spaces of finite dimension.

Proposition 1.2.4. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G.* The map $\Phi : End(H) \longrightarrow End(K)$ is *G-equivariant if and only if*

$$\Phi(\pi_{H(g)}A\pi^*_{H(g)}) = \pi_{K(g)}\Phi(A)\pi^*_{K(g)}$$

for all $A \in End(H)$ *and* $g \in G$.

Proposition 1.2.5. *For* $i = 1, 2$, *let* (H_i, π_{H_i}) *and* (K_i, π_{K_i}) *be representations of a group* G, *and* $\Phi_i : End(H_i) \longrightarrow End(K_i)$ *be* G*-equivariant maps. The tensor product and the direct sum of* Φ_1 *and* Φ_2 *are* G*-equivariant maps with respect to the actions on the tensor product and the direct sum respectively. If* Φ_1 *and* Φ_2 *are composable then their composition is also* G*-equivariant.*

See Appendix **A** for definitions of the tensor product, the direct sum of two maps, and the actions defined on their representation spaces.

Definition 1.2.6. *Let* H *and* K *be Hilbert spaces, and* $\alpha \in End(H, K)$. *Conjugation by* α *is the linear map*

$$Ad_\alpha : End(H) \longrightarrow End(K)$$

$$A \longmapsto \alpha A \alpha^*$$

where α^* *is the conjugate map of* α.

Proposition 1.2.7. *Let* (H, π_H) *and* (K, π_K) *be two unitary representations of a group* G, *and* $\alpha : H \longrightarrow K$ *be a* G*-equivariant map. Then*

1. *The image under* α *of a* G*-invariant subspace of* H *is* G*-invariant.*
2. *The conjugate of* α *is* G*-equivariant.*
3. *Conjugation by* α *is* G*-equivariant.*
4. *If* α *is an injective map then the image under* α *of any* G*-irreducible subspace of* H *is* G*-irreducible.*

Notation 1.2.8. For a subspace W of a Hilbert space H, let ι_W denote the inclusion map of W, and q_W denote the orthogonal projection onto W.

Both maps are elements in $End(H)$ (redefine ι_W to be the identity map on W and the zero on the orthogonal complement of W). With this definition, the inclusion map ι_W is the conjugate of q_W.

Remark 1.2.9. If (H, π_H) is a unitary representation of a group G then the orthogonal complement of any G-invariant subspace is also G-invariant. For more details, see [37, p.24], and [8, p.70].

Lemma 1.2.10. *Let (H, π_H) be a representation of a group G. The subspace W of H is G-invariant if and only if q_W (resp. ι_W) is a G-equivariant map.*

Proof:

Suppose that W is G-invariant, and $g \in G$. Since any element $h \in H$ can be written as $x + y$ such that $x \in W$ and $y \in W^{\perp}$, then by the remark above, we have

$$q_W \pi_{H(g)}(h) = q_W (\pi_{H(g)}(x) + \pi_{H(g)}(y)) = \pi_{H(g)}(x) = \pi_{H(g)} q_W(h)$$

i.e. q_W is G-equivariant. On other hand, if q_W is G-equivariant then for $w \in W$ and $g \in G$, we have:

$$\pi_{H(g)}(w) = \pi_{H(g)} q_W(w) = q_W \pi_{H(g)}(w) \in W.$$

Since $\iota_W = q_W^*$, the equivalent follows for ι_W. ∎

Remark 1.2.11. Let H be a Hilbert space. If W is a subspace of H, given by the orthogonal projection q_W, then $End(W)$ is isomorphic to a subspace of $End(H)$, given by the projection Ad_{q_W}. It follows that if (H, π_H) is a representation of a group G with a G-invariant subspace W then $End(W)$ is G-isomorphic to a G-invariant subspace of $End(H)$.

The following proposition is one of the main pillars in the study of group representations. It is stated and proved in [9, p.7] for finite groups, but the method of the proof is valid in the general case.

Proposition 1.2.12. *(Schur's Lemma) Let (H_1, ρ_1) and (H_2, ρ_2) be two irreducible representations of a group G. If $\alpha : H_1 \longrightarrow H_2$ is a G-equivariant map then either $\alpha \equiv 0$ or α is a G-isomorphism. In case of $\rho_1 = \rho_2$ and $H_1 = H_2$ then α is a multiple of the identity.*

Corollary 1.2.13. *Let (H, π_H) be a unitary representation of a group G. Any two non isomorphic G-irreducible subspaces of H are mutually orthogonal.*

Proof:

Let W_1 and W_2 be two G-invariant irreducible subspaces of H. By Lemma 1.2.10, the associated orthogonal projections q_{W_1} and q_{W_2} are G-equivariant, hence so is the map $q_{W_1} q_{W_2}^* = q_{W_1} \iota_{W_2} : W_2 \longrightarrow W_1$. By Schur's Lemma 1.2.12, the map $q_{W_1} q_{W_2}^* = q_{W_1} q_{W_2}$ is either the zero map or an isomorphism. ∎

The proof of the next lemma is given in [9, p.7] for the case of finite groups (see also [13, p.333 (21.40)]). However, the same statement and proof are valid for the finite dimensional representation of compact group. Recall that we assumed that all vector spaces are finite dimensional.

Lemma 1.2.14. *Let (H, π_H) be a representation of a compact group G. There exists a decomposition*

$$H = U_1^{\oplus a_1} \oplus ... \oplus U_k^{\oplus a_k}$$

where U_i are G-irreducible distinct subspaces. The decomposition of H into a direct sum of the k factors is unique, as are the U_i occur and their multiplicities a_i.

Definition 1.2.15. *The number a_i in Lemma 1.2.14, is called the multiplicity of the subspace U_i.*

Corollary 1.2.16. *Let (H, π_H) be a representation of a compact group G. If $\bigoplus_{i=1}^{n} U_i$ and $\bigoplus_{j=1}^{m} V_j$ are two decompositions of H into G-irreducible subspaces of distinct dimensions* *then $m = n$, and for each $1 \leq i \leq n$, there exists a permutation $\sigma \in \mathcal{S}_n$ such that $U_i = V_{\sigma(i)}$.*

Proof:

Fix $1 \leq i \leq n$, by Lemma 1.2.14, $m = n$, and there exists a permutation $\sigma \in \mathcal{S}_n$ such that $U_i \simeq V_{\sigma(i)}$. Since all V_j have distinct dimensions then by Schur's Lemma, the subspaces U_i and V_j are orthogonal for each $j \neq \sigma(i)$. Hence

$$U_i \subseteq \left(\bigoplus_{j \neq \sigma(i)} V_j \right)^{\perp} = V_{\sigma(i)}.$$

Since U_i and $V_{\sigma(i)}$ have the same dimension then $U_i = V_{\sigma(i)}$. ∎

Proposition 1.2.17. *Let (H, π_H) be a representation of a group G, such that $H = \bigoplus_{i=1}^{m} W_i$, where W_i are G-irreducible subspaces of H of multiplicity one. The space $End(H)^G$ is a commutative algebra, that is spanned by the G-equivariant projections on $\{W_i : 1 \leq i \leq m\}$.*

Proof:

Let $q_i : H \longrightarrow W_i$ be the orthogonal projection onto the G-invariant subspace W_i, and $\iota_s : W_s \longrightarrow H$ be the inclusion map of W_s. By Lemma 1.2.10, the maps q_i and ι_s are G-equivariant. Hence, for $T \in End(H)^G$, the map $q_s T \iota_i : W_i \longrightarrow W_s$ is a G-equivariant map, intertwining the G-irreducible representations W_s and W_i. As the multiplicity of each W_i is one, by Schur's Lemma 1.2.12, we have

$$q_s T \iota_i = \begin{cases} 0 & s \neq i \\ \lambda_i I_i & s = i \end{cases}$$

where I_i is the identity map on W_i. As for $h \in H$, we can write $h = w_1 + w_2 + ... + w_m$ where $w_i = q_i(h)$, hence

$$T(h) = T(w_1 + w_2 + ... + w_m)$$

$$= \lambda_1 w_1 + \lambda_2 w_2 + ... + \lambda_m w_m$$

$$= \lambda_1 q_1(h) + \lambda_2 q_2(h) + ... + \lambda_m q_m(h)$$

$$= \sum_{i=1}^{m} \lambda_i q_i(h).$$

To see that $End(H)^G$ is commutative, let T_1 and T_2 are two elements in $End(H)^G$, such that $T_1 = \sum_{i=1}^{m} \lambda_i q_i$ and $T_2 = \sum_{s=1}^{m} \mu_s q_s$. Since $\{q_i : 1 \leq i \leq m\}$ are mutually orthogonal projections, then

$$T_1 T_2 = \sum_{i=1}^{m} \sum_{i=1}^{m} \lambda_i \mu_s q_i q_s = \sum_{i=1}^{m} \lambda_i \mu_i q_i q_i$$

$$= \sum_{i=1}^{m} \mu_i \lambda_i q_i = \sum_{s=1}^{m} \sum_{i=1}^{m} \mu_s \lambda_i q_s q_i = T_2 T_1.$$

∎

Proposition 1.2.18. *Let (H, π_H), (K, π_K) and (E, π_E) be unitary representations of a group G, and $\alpha : H \longrightarrow K \otimes E$ be a G-equivariant map. The map*

$$T : E \longrightarrow End(H, K)$$

$$u \longmapsto (I_K \otimes u^*)\, \alpha$$

is G-equivariant, where u^* denote the linear form on E given by $u^*(z) = \langle u \,|z \rangle_E$.

Proof:

Let $g \in G$, and $u \in E$ arbitrary elements. As $\pi_{K(g)} \otimes u^* = \pi_{K(g)}(I_K \otimes u^*)$ (check on $x \otimes y$), we have

$$T\left(\pi_{E(g)}(u)\right) = \left(I_K \otimes u^* \pi^*_{E(g)}\right) \alpha = \left(I_K \otimes u^* \pi^*_{E(g)}\right)\left(\left(\pi_{K(g)} \otimes \pi_{E(g)}\right) \alpha \pi^*_{H(g)}\right)$$

$$= \left(\pi_{K(g)} \otimes u^*\right) \alpha \pi^*_{H(g)} = \pi_{K(g)} \left(I_K \otimes u^*\right) \alpha \pi^*_{H(g)} = \pi_{K(g)} T(u) \pi^*_{H(g)}$$

i.e. T is G-equivariant. ∎

Corollary 1.2.19. *Let (H, π_H), (K, π_K), and (E, π_E) be representations of a group G such that π_E is irreducible, and let $\alpha : H \longrightarrow K \otimes E$ be a G-equivariant isometry. If $\{e_j : 1 \le j \le d_E\}$ is an orthonormal basis for E, then the set*

$$\{T_j = \left(I_K \otimes e_j^*\right)\alpha \ : 1 \le j \le d_E\} \subseteq End(H, K)$$

satisfies

$$\langle T_{j_1} \,|T_{j_2}\rangle_{End(H,K)} = \tfrac{d_H}{d_E}\delta_{j_1 j_2}$$

for $1 \le j_1, j_2 \le d_E$.

Proof: Consider the G-equivariant map $T : E \longrightarrow End(H, K)$, defined in Proposition 1.2.18. By Schur's Lemma 1.2.12, the map $T^*T : E \longrightarrow E$ is a multiple of the identity on E. Thus, there exist $\lambda \in \mathbb{C}$ such that

$$\langle T(u) \,|T(v)\rangle_{End(H,K)} = \langle u \,|T^*T(v)\rangle_E = \langle u \,|\lambda v\rangle_E$$

for any $u, v \in E$. Since

$$T(e_{j_1}) = T_{j_1}, \text{ and} \quad T(e_{j_2}) = T_{j_2} \quad \text{for } 0 \le j_1, j_2 \le d_E.$$

then

$$\begin{aligned}\langle T_{j_1} \,|T_{j_2}\rangle_{End(H,K)} &= \langle T(e_{j_1}) \,|T(e_{j_2})\rangle_{End(H,K)} \\ &= \lambda \langle e_{j_1} \,|e_{j_2}\rangle_E = \lambda\delta_{j_1 j_2}\end{aligned}$$

As $T_j = \left(I_K \otimes e_j^*\right)\alpha$, the map α is equal to $\sum_{j=1}^{d_E} T_j \otimes e_j$. Let $\{f_i : 1 \le i \le d_H\}$ be an orthonormal basis of H, then

$$\begin{aligned}d_H &= \sum_{i=1}^{d_H} \|\alpha(f_i)\|^2 = \sum_{i=1}^{d_H} \left\| \sum_{j=1}^{d_E} T_j(f_i) \otimes e_j \right\|^2 \\ &= \sum_{i=1}^{d_H}\sum_{j=1}^{d_E} \|T_j(f_i)\|^2 = \sum_{j=1}^{d_E} \|T_j\|^2 = \sum_{j=1}^{d_E} \lambda = d_E\lambda\end{aligned}$$

i.e. $\lambda = \frac{d_H}{d_E}$. ∎

1.2.2 Examples of G-equivariant maps

In this subsection, we provide examples, and standard constructions of G-equivariant maps. Recall that if (H, π_H) and (K, π_K) are representations of a group G, then $\pi_H \otimes \pi_K$ is a representation of G in the space $H \otimes K$. The new representation is defined naturally by linearly extending $\pi_H \otimes \pi_{K(g)}(h \otimes k) = \pi_{H(g)}(h) \otimes \pi_{K(g)}(k)$ for $g \in G$, and $h, k \in H, K$. For two matrices $A = (a_{ij})$ and $B = (b_{lk})$, the Kronecker product of A and B is defined to be $A \otimes B = (Ab_{lk})$.

I. The partial trace:

Definition 1.2.20. *Let H and K be Hilbert spaces. The linear map*

$$Tr_H : End(H \otimes K) \longrightarrow End(K)$$

$$A \otimes B \longmapsto tr(A)B$$

defined for $A \otimes B \in End(H \otimes K)$, and extended by linearity is called the partial trace over H.

In similar way, we define the partial trace over K by taking the trace over the second component of $A \otimes B$.

Lemma 1.2.21. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G. The partial trace over H is a G-equivariant map.*

Proof:

Let $g \in G$, and $A_1 \otimes A_2 \in End(H \otimes K)$. Then

$$Tr_H\left(\left(\pi_{H(g)} \otimes \pi_{K(g)}\right)\left(A_1 \otimes A_2\right)\left(\pi^*_{H(g)} \otimes \pi^*_{K(g)}\right)\right)$$

$$= Tr_H(\pi_{H(g)} A_1 \pi^*_{H(g)} \otimes \pi_{K(g)} A_2 \pi^*_{K(g)})$$

$$= tr(\pi_{H}(g) A_1 \pi^*_{H}(g)) \pi_{K}(g) A_2 \pi^*_{K}(g)$$

$$= tr(A_1) \pi_{K}(g) A_2 \pi^*_{K}(g) = \pi_{K}(g) Tr_{H}(A_1 \otimes A_2) \pi^*_{K}(g)$$

∎

II. The flipping map (swap map):

Our second example of G-equivariant maps is defined on the tensor product of two vector spaces H and K. It is called the flipping map (swap map), and denoted by $flip^H_K$.

Definition 1.2.22. *Let H and K be Hilbert spaces. We define the linear map*

$$flip^H_K : H \otimes K \longrightarrow K \otimes H$$

via

$$h \otimes k \longmapsto k \otimes h$$

on the set $\{h \otimes k : h \in H, k \in K\}$ and then extended linearly.

Lemma 1.2.23. *Let (H, π_H) and (K, π_K) be two representations of a group G. The map $flip^H_K$ is a unitary G-equivariant map satisfying $(flip^H_K)^* = flip^K_H$ and*

$$Tr_K(flip^H_K \, A \, flip^K_H) = Tr_K(A)$$

for $A \in End(H \otimes K)$.

Proof:

Let $g \in G$. For $h \otimes k \in H \otimes K$, we have

$$(\pi_{K}(g) \otimes \pi_{H}(g)) \, flip^H_K(h \otimes k) = (\pi_{K}(g) \otimes \pi_{H}(g)) \, (k \otimes h)$$

$$= \pi_{K(g)}(k) \otimes \pi_{H(g)}(h) = flip_K^H(\pi_{H(g)}(h) \otimes \pi_{K(g)}(k))$$

$$= flip_K^H\left(\pi_{H(g)} \otimes \pi_{K(g)}\right)(h \otimes k)$$

G-equivariance follows by linearity. Since for $(h \otimes k) \in H \otimes K$, $\|h \otimes k\| = \|k \otimes h\|$, $flip_K^H$ is a unitary map such that $(flip_K^H)^* = (flip_K^H)^{-1} = flip_H^K$.

To prove the second assertion, let $B_1 \in End(H)$ and $B_2 \in End(K)$. By direct computations on arbitrary element $k \otimes h$, we have

$$flip_K^H\left(B_1 \otimes B_2\right) flip_H^K = B_2 \otimes B_1$$

Hence,

$$Tr_K(flip_K^H\left(B_1 \otimes B_2\right)(flip_K^H)^*) = tr(B_2)B_1 = Tr_K(B_1 \otimes B_2).$$

The result follows by linearity. ∎

III. The map Vec:

Recall that $\{xy^* : x \in K, y \in H\}$ forms a set of generators of $End(H,K)$, where y^* denotes the linear form on H given by $y^*(z) = \langle y\,|z\rangle_H$, and xy^* denotes the map $xy^*(z) = \langle y\,|z\rangle_H\, x$ for any $z \in H$. The following is a reformulation of the definition of the map vec in [41, p.23].

Definition 1.2.24. *Let H and K be Hilbert spaces, let* Vec : $End(H,K) \longrightarrow K \otimes \overline{H}$ *be the linear map defined on the elements xy^* of $End(H,K)$ via*

$$xy^* \longmapsto x \otimes \overline{y}$$

extended linearly.

The map Vec represents any element in $End(H,K)$ as a vector in the tensor product space $K \otimes \overline{H}$.

Lemma 1.2.25. *Let (H, π_H) and (K, π_K) be two representations of a group G. By considering the conjugate representation on $\overline{H}$, the map*

$$\mathrm{Vec} : End(H, K) \longrightarrow K \otimes \overline{H}$$

is a G-equivariant unitary map.

Proof:

Let $\{e_i : 1 \leq i \leq d_H\}$ and $\{e'_j : 1 \leq j \leq d_K\}$ be orthonormal bases for H and K respectively, hence the set $\{E_{ij} = e_i e'^*_j : 1 \leq i \leq d_H, 1 \leq j \leq d_K\}$ is an orthonormal basis for $End(H, K)$. For $g \in G$ and $E_{ij} \in End(H, K)$, we have

$$\mathrm{Vec}(\pi_{K(g)} E_{ij} \pi^*_{H(g)}) = \mathrm{Vec}\left(\pi_{K(g)} e_i \left(\pi_{H(g)} e'_j\right)^*\right) = \pi_{K(g)} e_i \otimes \overline{\pi_{H(g)} e'_j}$$

$$= (\pi_K \otimes \overline{\pi}_H)_{(g)}(e_i \otimes e'_j) = (\pi_K \otimes \overline{\pi}_H)_{(g)} \mathrm{Vec}(E_{ij}).$$

The G-equivariant follows by linearity of the map Vec. Clearly Vec is a linear bijection which is unitary since

$$\langle A \,|B \rangle_{End(H,K)} = \langle \mathrm{Vec}(A) \,|\mathrm{Vec}(B) \rangle_{K \otimes \overline{H}}$$

for $A, B \in End(H, K)$. ∎

IV. The Choi-Jamiolkowski map:

The following is an equivalent definition of the Choi-Jamiolkowski map in [41, p.49]; we show this equivalence in Lemma 1.2.30.

Definition 1.2.26. *Let H and K be Hilbert spaces. The linear map*

$$C : End(End(H), End(K)) \longrightarrow End(K \otimes \overline{H})$$

$$AB^* \longmapsto A \otimes \overline{B}$$

defined for $A \in End(K)$ *and* $B \in End(H)$ *and extended linearly is called the* Choi-Jamiolkowski map. *The map* $B^* : End(H) \longrightarrow \mathbb{C}$ *is given by* $B^*X = \langle B \,|X \rangle_{End(H)}$ *for* $X \in End(H)$.

Lemma 1.2.27. *Let* (H, π_H) *and* (K, π_K) *be two representations of a group* G. *The natural isomorphism* $T : End(K) \otimes End(\overline{H}) \longrightarrow End(K \otimes \overline{H})$ *defined by taking* $A \otimes B$ *to* $T(A \otimes B)(k \otimes h) = A(k) \otimes B(h)$ *and extending linearly is a* G*-equivariant map.*

Recall that for finite-dimensional Hilbert spaces H and K, the spaces $End(End(H), End(K))$, $End(K) \otimes End(H)^*$, $End(K) \otimes \overline{End(H)}$, and $End(K \otimes \overline{H})$ are all algebraically isomorphic. The spaces $End(\overline{H})$ and $\overline{End(H)}$ are equal. See Appendix **A**, for more details.

Remark 1.2.28. The Choi-Jamiolkowski map is the composition of the maps

$$\text{Vec} : End(End(H), End(K)) \longrightarrow End(K) \otimes \overline{End(H)} = End(K) \otimes End(\overline{H})$$

with the natural isomorphism $T : End(K) \otimes End(\overline{H}) \longrightarrow End(K \otimes \overline{H})$, defined in Lemma 1.2.27.

By Lemma 1.2.25, and the remark above, we have:

Corollary 1.2.29. *Let* (H, π_H) *and* (K, π_K) *be two representations of a group* G. *The Choi-Jamiolkowski map is unitarily* G*-equivariant.*

The Choi-Jamiolkowski map assigns to each $\Phi \in End(End(H), End(K))$ a unique matrix $C(\Phi) \in End(K \otimes \overline{H})$, called the Choi matrix of Φ. The next lemma shows the equivalency of Definition 1.2.26, and the original definition of Choi-Jamiolkowski map in [23, p.276], and [41, p.49].

Lemma 1.2.30. *Let* H *and* K *be Hilbert spaces. For* $\Phi \in End(End(H), End(K))$, *the Choi matrix of* Φ *is given by*

$$C(\Phi) = \sum_{i,j} \Phi(E_{ij}) \otimes E_{ij}$$

where $\{E_{ij} : 0 \leq i, j \leq d_H\}$ *is the standard orthonormal basis for* $End(H)$.

Proof:

It suffices to show the equality for $\Phi = AB^*$, where $A \in End(K)$ and $B \in End(H)$.

Let $B = \sum_{k,l}^{d_H} \lambda_{kl} E_{kl}$, then

$$\sum_{ij}^{d_H} AB^*(E_{ij}) \otimes E_{ij} = \sum_{ij}^{d_H} A \langle B \,| E_{ij} \rangle \otimes E_{ij} = \sum_{ij}^{d_H} A\bar{\lambda}_{ij} \otimes E_{ij}$$
$$= A \otimes \sum_{ij}^{d_H} \bar{\lambda}_{ij} E_{ij} = A \otimes \sum_{ij}^{d_H} \overline{\lambda_{ij} E_{ij}}$$
$$= A \otimes \overline{B} = C(AB^*)$$

∎

Next we determine the conditions on the Choi matrix of a linear map that are equivalent to G-equivariance. The idea of the proof is taken from [7, p.5].

Lemma 1.2.31. *Let H and K be Hilbert spaces. For $\Phi \in End(End(H), End(K))$, $\alpha_K \in End(K)$, and $\alpha_H \in End(H)$ we have:*

1. $C(Ad_{\alpha_K} \circ \Phi) = (\alpha_K \otimes I_{\overline{H}})C(\Phi)(\alpha_K \otimes I_{\overline{H}})^*$.

2. $C(\Phi \circ Ad_{\alpha_H}) = (I_K \otimes \overline{\alpha}_H)^* C(\Phi)(I_K \otimes \overline{\alpha}_H)$.

Proof:

Let $\{E_{ij} : 0 \leq i, j \leq d_H\}$ be the standard orthonormal basis for $End(H)$. By Lemma 1.2.30, we have

$$(\alpha_K \otimes I_{\overline{H}})C(\Phi)(\alpha_K \otimes I_{\overline{H}})^* = (\alpha_K \otimes I_{\overline{H}}) \left(\sum_{i,j} \Phi(E_{ij}) \otimes E_{ij} \right) (\alpha_K \otimes I_{\overline{H}})^*$$

$$= \sum_{i,j} (\alpha_K \otimes I_{\overline{H}}) (\Phi(E_{ij}) \otimes E_{ij}) (\alpha_K \otimes I_{\overline{H}})^*$$
$$= \sum_{i,j} (\alpha_K \Phi(E_{ij}) \alpha_K^*) \otimes (I_{\overline{H}} E_{ij} I_{\overline{H}}^*)$$
$$= \sum_{i,j} (Ad_{\alpha_K} \circ \Phi(E_{ij})) \otimes E_{ij} = C(Ad_{\alpha_K} \circ \Phi)$$

establishing the first equality. For the second equality, let $A \in End(K)$ and $B \in End(H)$, it suffices to show that the equality holds for $\Phi = AB^*$. Let $D \in End(H)$, we have:

$$AB^* \circ Ad_{\alpha_H}(D) = AB^* (\alpha_H D \alpha_H^*) = A \langle B \mid \alpha_H D \alpha_H^* \rangle_{End(H)}$$
$$= tr(\alpha_H D \alpha_H^* B^*) A = tr(D(\alpha_H^* B \alpha_H)^*) A$$
$$= A \langle \alpha_H B \alpha_H^* \mid D \rangle_{End(H)} = A(\alpha_H^* B \alpha_H)^*(D)$$

that is,

$$AB^* \circ Ad_{\alpha_H} = A(\alpha_H^* B \alpha_H)^*$$

consequently,

$$C(AB^* \circ Ad_{\alpha_H}) = C(A(\alpha_H^* B \alpha_H)^*) = A \otimes \overline{\alpha_H^* B \alpha_H}$$
$$= I_K A I_K \otimes \overline{\alpha_H^* B \alpha_H} = (I_K \otimes \overline{\alpha}_H)^* \left(A \otimes \overline{B}\right) (I_K \otimes \overline{\alpha}_H)$$
$$= (I_K \otimes \overline{\alpha}_H)^* C(AB^*)(I_K \otimes \overline{\alpha}_H).$$

∎

Recall that for a group G, and a Hilbert space H, the set $End(H)^G$ denotes the set of G-equivariant maps on H.

Proposition 1.2.32. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G. A linear map $\Phi : End(H) \longrightarrow End(K)$ is G-equivariant if and only if $C(\Phi) \in End(K \otimes \overline{H})^G$.*

Proof:

By injectivity of the Choi-Jamiolkowski map, Φ is G-equivariant if and only if

$$C(Ad_{\pi_K(g)} \circ \Phi) = C(\Phi \circ Ad_{\pi_H(g)}) \qquad \forall g \in G$$

By Lemma 1.2.31, this holds if and only if

$$(\pi_{K(g)} \otimes I_{\overline{H}(g)})C(\Phi)(\pi_{K(g)} \otimes I_{\overline{H}(g)})^* = (I_{K(g)} \otimes \overline{\pi}_{H(g)})^* C(\Phi)(I_{K(g)} \otimes \overline{\pi}_{H(g)}) \qquad \forall g \in G$$

$$\iff (\pi_{K(g)} \otimes \overline{\pi}_{H(g)})C(\Phi) = C(\Phi)(\pi_{K(g)} \otimes \overline{\pi}_{H(g)}) \qquad \forall g \in G$$

$$\iff C(\Phi) \in End(K \otimes \overline{H})^G.$$

∎

Chapter 2

Representations of $SU(2)$

According to the Clebsch-Gordan Decomposition [3, p.87], if H and K are two $SU(2)$-irreducible subspaces, then the $SU(2)$-space $K \otimes E$ is isomorphic to $\bigoplus_i H_i$ where H_i is $SU(2)$-irreducible subspace with multiplicity one. For each i, the inclusion map $\alpha_i : H_i \longrightarrow K \otimes E$ is $SU(2)$-equivariant. Our main goal in this chapter is to find an explicit formula for the map α_i. In the first section, we review the irreducible representations of $SU(2)$, and for an $SU(2)$-irreducible space H, we find an $SU(2)$-equivariant unitary map from H onto $\overline{H}$. In Section 2.2, we state the Clebsch-Gordan expansion theorem. We get our main result of this chapter in Section 2.3, by constructing an $SU(2)$-equivariant isometry defined on the representation space of the $SU(2)$-irreducible representation. We end this chapter with an application of our results, in Section 2.4. The proofs of some Lemmas and corollaries in this chapter are purely technical calculations, and are deferred to Appendix **B**.

The main results of this chapter:

- Constructing an $SU(2)$-equivariant unitary map between any $SU(2)$-irreducible space, and its corresponding conjugate space (Proposition 2.1.6).

- Constructing an $SU(2)$-equivariant isometry defined on the representation space of the $SU(2)$-irreducible representation (Proposition 2.3.3, and Proposition 2.3.5).

- For an $SU(2)$-irreducible subspace H, we give explicit formulae for the projections of $End(H)$ into its $SU(2)$-irreducible invariant subspaces (Proposition 2.4.2).

2.1 The irreducible representations of $SU(2)$

For $m \in \mathbb{N}$, let P_m denote the space of homogeneous polynomials, with complex coefficients, of degree m in the two variables x_1, x_2. It is a complex vector space of dimension $m+1$ with a basis $\left\{x_1^i x_2^{m-i} : 0 \leq i \leq m\right\}$. By convention, we denote by P_{-1} the zero vector space. Recall that

$$SU(2) = \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} : a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1 \right\}$$

Definition 2.1.1. *For $m \in \mathbb{N}$, define $\rho_m : SU(2) \longrightarrow End(P_m)$ by*

$$\left(\rho_m(g) f\right)(x_1, x_2) = f((x_1, x_2)g) = f(ax_1 - \bar{b}x_2, bx_1 + \bar{a}x_2)$$

for $f \in P_m$ and $g \in SU(2)$.

The next proposition summarizes results in [3, p. 85-86], [38, p.181], and [39, p.276-279].

Proposition 2.1.2.

1. *For $m \in \mathbb{N}$, ρ_m is a unitary representation of $SU(2)$ with respect to the inner product on P_m given by*

$$\left\langle x_1^l x_2^{m-l}, \, x_1^k x_2^{m-k} \right\rangle_{P_m} = l! \, (m-l)! \, \delta_{lk}$$

2. *The set* $\{\rho_m : m \in \mathbb{N}\}$ *constitutes the full list of the irreducible representations of* $SU(2)$.

To facilitate the computations, we choose the orthonormal basis for P_m given by the polynomials $\left\{f_l^m = a_m^l x_1^l x_2^{m-l} : 0 \leq l \leq m\right\}$ where $a_m^l = \frac{1}{\sqrt{l!(m-l)!}}$; this basis is called *canonical* [39, p.280]. Throughout this thesis, we utilize the following definition and notation:

Definition 2.1.3. *For* $m \in \mathbb{N}$, *the set* $\{f_l^m : 0 \leq l \leq m\}$ *is called the* standard basis *for the* $SU(2)$*-irreducible space* P_m. *The corresponding standard basis for* $End(P_m)$ *is* $\{E_{lk} = f_{l-1}^m f_{k-1}^{m^*} : 1 \leq l, k \leq m+1\}$.

Remarks 2.1.4. Let $g = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \in SU(2)$. For $m \in \mathbb{N}$, we have

1. The map $\rho_{m(g)}$ is given on the standard basis for P_m by

$$\rho_{m(g)}(f_l^m) = a_m^l (ax_1 - \bar{b}x_2)^l (bx_1 + \bar{a}x_2)^{m-l}$$

   In particular, for $g_0 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in SU(2)$, we have

$$\rho_{m(g_0)}\left(f_l^m\right) = (-1)^{\,l} f_{m-l}^m$$

   and

$$\rho_m(g_0^*)\left(f_l^m\right) = (-1)^{\,m-l} f_{m-l}^m$$

2. The map $\rho_{m(g)}$ belongs to both $End(P_m)$ and $End(\overline{P}_m)$. For if $g \in SU(2)$ then $\overline{g} \in SU(2)$, and $\rho_{m(\overline{g})}$ is a unitary map on P_m. Thus $\rho_{m(g)} = \overline{\rho_{m(\overline{g})}}$ is a unitary map on $\overline{P}_m$, where $\overline{P}_m$ is the conjugate space for P_m.

The element $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ plays a special role in constructing an $SU(2)$-equivariant unitary map from P_m onto $\overline{P}_m$; we will denote this element by g_0.

Definition 2.1.5. *For $m \in \mathbb{N}$, define the endomorphisms*

1. $\Theta_m : P_m \longrightarrow \overline{P}_m$ *by* $\Theta_m\left(\sum_{l=0}^{m}\lambda_l f_l^m\right) = \sum_{l=0}^{m}\lambda_l \cdot f_l^m$, *where* $\cdot$ *is the multiplication in* $\overline{P}_m$.

2. $J_m : P_m \longrightarrow \overline{P}_m$ *by* $J_m = \Theta_m \rho_{m(g_0)}$.

Proposition 2.1.6. *For $m \in \mathbb{N}$,*

1. Θ_m *is a unitary map that satisfies* $\overline{\rho_{m(g)}}\Theta_m = \Theta_m\rho_{m(\overline{g})}$ *for any* $g \in SU(2)$.

2. J_m *is an* $SU(2)$*-equivariant unitary map from* P_m *onto* $\overline{P}_m$.

Proof:

The map Θ_m takes the orthonormal basis $\{f_l^m : 0 \leq l \leq m\}$ for P_m to itself; as it is a basis for $\overline{P}_m$, hence Θ_m is a unitary map. Let $g \in SU(2)$, by Remark 2.1.4,

$$\begin{aligned}
\Theta_m \circ \rho_{m(\overline{g})}(f_l^m) &= \Theta_m\left(a_m^l(\overline{a}x_1 - bx_2)^l(\overline{b}x_1 + ax_2)^{m-l}\right) \\
&= a_m^l(\overline{a}\cdot x_1 - b.x_2)^l(\overline{b}.x_1 + a.x_2)^{m-l} \\
&= \rho_{m(\overline{g})}\left(\Theta_m(f_l^m)\right) = \overline{\rho_{m(g)}} \circ \Theta_m(f_l^m).
\end{aligned}$$

For the second statement, as J_m is a composition of two unitary maps, it is unitary. Since

$$g_0 g = \bar{g} g_0 \qquad \forall g \in SU(2)$$

we have,

$$\begin{aligned}
J_m\rho_{m(g)} &= \Theta_m\rho_{m(g_0)}\rho_{m(g)} = \Theta_m\rho_{m(\overline{g})}\rho_{m(g_0)} \\
&= \overline{\rho_{m(g)}}\Theta_m\rho_{m(g_0)} = \overline{\rho_{m(g)}}J_m.
\end{aligned}$$

∎

Remark 2.1.7. For $m \in \mathbb{N}$ and $0 \leq l \leq m$, we have:

$$J_m(f_l^m) = (-1)^l f_{m-l}^m, \quad J_m^*(f_l^m) = (-1)^{m-l} f_{m-l}^m$$

where f_l^m is the basis element for P_m.

For $m, n \in \mathbb{N}$, we fixed our choice for a basis for $P_m \otimes P_n$ to be

$$\{f_l^m \otimes f_j^n : 0 \leq l \leq m, \, 0 \leq j \leq n\}$$

where writing the basis in this form means that we choose the order to be in the form

$$\{f_0^m \otimes f_0^n, f_1^m \otimes f_0^n, ... f_m^m \otimes f_0^n, f_0^m \otimes f_1^n, f_1^m \otimes f_1^n, ... f_m^m \otimes f_1^n, ..., f_0^m \otimes f_n^n, f_1^m \otimes f_n^n, ... f_m^m \otimes f_n^n\}$$

In this thesis, we call this basis the standard basis for $P_m \otimes P_n$. Recall the $flip$ map in Definition 1.2.22. By direct computations on the elements of the standard basis for $P_m \otimes P_n$, we obtain

Proposition 2.1.8. *For $m, n \in \mathbb{N}$, the map*

$$flip_{P_n}^{\overline{P}_m}(J_m \otimes I_{P_n}) : P_m \otimes P_n \longrightarrow P_n \otimes \overline{P}_m$$

is an $SU(2)$-equivariant isomorphism, that satisfies

$$flip_{P_n}^{\overline{P}_m}(J_m \otimes I_{P_n}) = (I_{P_n} \otimes J_m) flip_{P_n}^{P_m}$$

2.2 Clebsch-Gordan expansion

For $m, n \in \mathbb{N}$, let ρ_m and ρ_n be the irreducible representations of $SU(2)$ with corresponding $SU(2)$-spaces P_m and P_n. One can construct a new representation of $SU(2)$ by taking the tensor product of the two representations, which is not necessarily irreducible. In this section, we build polynomial operators on the $SU(2)$-space $P_m \otimes P_n$. To obtain a concrete representation of $P_m \otimes P_n$, let $x = (x_1, x_2)$, $y = (y_1, y_2)$, $P_m := P_m(x)$, and $P_n := P_n(y)$. We embed the tensor product $P_m(x) \otimes P_n(y)$ into $\mathbb{C}[x, y]$ as follows:

Define the map $: P_m(x) \times P_n(y) \longrightarrow \mathbb{C}[x,y]$ by $(f(x), g(y)) \longmapsto f(x)g(y)$. It is a bilinear map, hence extends to a linear $T : P_m(x) \otimes P_n(y) \longrightarrow \mathbb{C}[x,y]$ taking $f(x) \otimes g(y)$ to $f(x)g(y)$. Let $P_{m,n}$ denote the vector space of polynomials in x and y of bi-degree (m,n) (homogeneous polynomials of degree m in $x = (x_1, x_2)$ and of degree n in $y = (y_1, y_2)$). The space $P_{m,n}$ has a basis consisting of

$$\{x_1^s x_2^{m-s} y_1^t y_2^{n-t} = \frac{1}{a_s^m a_t^n} T(f_s^m \otimes f_t^n) : 0 \leq s \leq m, 0 \leq t \leq n\}$$

Since the map T takes a basis for $P_m \otimes P_n$ to a basis in $P_{m,n}$, it is an isomorphism. Henceforth, we will use $P_{m,n}$ as a concrete representation of $P_m \otimes P_n$.

Remark 2.2.1. Using the identification between $P_m \otimes P_n$ and $P_{m,n}$ above, and Remark 2.1.4, we have

$$\rho_{m(g)} \otimes \rho_{n(g)} f(x,y) = f(ax_1 - \bar{b}x_2, bx_1 + \bar{a}x_2, ay_1 - \bar{b}y_2, by_1 + \bar{a}y_2)$$

where $f(x,y) := f(x_1, x_2, y_1, y_2) \in P_m \otimes P_n$, and $g \in SU(2)$.

Recall that $\mathbb{C}[x_1, x_2, y_1, y_2, \frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \frac{\partial}{\partial y_1}, \frac{\partial}{\partial y_2}]$ is a non-commutative algebra of polynomial differential operators which acts on $\mathbb{C}[x_1, x_2, y_1, y_2]$. The multiplication is the composition of operators.

Definition 2.2.2. *For $m, n \in \mathbb{N}$, define the following maps on $P_m \otimes P_n$*

$$\begin{aligned} \Delta_{xy} : P_m \otimes P_n &\longrightarrow P_{m+1} \otimes P_{n-1} \\ f(x,y) &\longmapsto \left(x_1 \frac{\partial}{\partial y_1} + x_2 \frac{\partial}{\partial y_2}\right) f(x,y) \end{aligned}$$

$$\begin{aligned} \Delta_{yx} : P_m \otimes P_n &\longrightarrow P_{m-1} \otimes P_{n+1} \\ f(x,y) &\longmapsto \left(y_1 \frac{\partial}{\partial x_1} + y_2 \frac{\partial}{\partial x_2}\right) f(x,y) \end{aligned}$$

$$\Gamma_{xy} : P_m \otimes P_n \longrightarrow P_{m+1} \otimes P_{n+1}$$
$$f(x,y) \longmapsto (x_1 y_2 - y_1 x_2)\, f(x,y)$$

$$\Omega_{xy} : P_m \otimes P_n \longrightarrow P_{m-1} \otimes P_{n-1}$$
$$f(x,y) \longmapsto \left(\frac{\partial}{\partial x_1}\frac{\partial}{\partial y_2} - \frac{\partial}{\partial x_2}\frac{\partial}{\partial y_1}\right) f(x,y)$$

for $f(x,y) \in P_m \otimes P_n$.

The statement of the next lemma is mentioned in [29, p.47]. The proof is purely computational, and is provided in Appendix **B**.

Lemma 2.2.3. *The operators* Δ_{xy}, Δ_{yx}, Γ_{xy}, *and* Ω_{xy} *are* $SU(2)$*-equivariant, and satisfy*

$$\Delta^*_{xy} = \Delta_{yx}, \qquad \Gamma^*_{xy} = \Omega_{xy}$$

Theorem 2.2.4. (Clebsch-Gordan expansion)[29, p.46]**.** Let $m, n \in \mathbb{N}$. For a polynomial $f(x,y) \in P_m \otimes P_n$, we have

$$f(x,y) = \sum_{h=0}^{\min\{m,n\}} c_{m,n,h}\, \Gamma^h_{xy} \Delta^{n-h}_{yx} \Delta^{n-h}_{xy} \Omega^h_{xy}(f(x,y))$$

where the coefficients $c_{m,n,h}$ are determined by induction as follows: $c_{m,0,0} = 1$. For $n \geq 1$ and $0 \leq h \leq \min\{m,n\}$.

$$c_{m,n,h} = \begin{cases} \frac{1}{(m+1)n}\; c_{m+1,n-1,h} & h=0 \\ \frac{1}{(m+1)n}\; [c_{m-1,n-1,h-1} + \; c_{m+1,n-1,h}] & 0<h<n \\ \frac{1}{(m+1)n}\; c_{m-1,n-1,h-1} & h=n \end{cases}$$

2.3 An $SU(2)$-equivariant isometry on the representation space of $SU(2)$

In this section, we use Lemma 2.2.3 and Theorem 2.2.4 to define an $SU(2)$-equivariant isometry $\alpha_{m,n,h}$ on the $SU(2)$-irreducible space P_{m+n-2h}, where $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$. We also give the matrix coefficients of $\alpha_{m,n,h}$ with respect to the standard basis for P_{m+n-2h}.

2.3.1 The isometry $\alpha_{m,n,h}$

The proof of the next proposition is in [3, p.87].

Proposition 2.3.1. ***(Clebsch-Gordan decomposition)*** *For $m, n \in \mathbb{N}$, let ρ_m and ρ_n be the irreducible representations of $SU(2)$ with corresponding $SU(2)$-spaces P_m and P_n. Then*

$$\rho_m \otimes \rho_n = \bigoplus_{h=0}^{\min\{m,n\}} \rho_{m+n-2h}$$

Consequently, the $SU(2)$-space $P_m \otimes P_n$ is isomorphic to $\bigoplus_{h=0}^{\min\{m,n\}} P_{m+n-2h}$.

Definition 2.3.2. *For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, let*

$$\alpha_{m,n,h} : P_{m+n-2h} \longrightarrow P_m \otimes P_n$$

be the linear map defined by

$$\alpha_{m,n,h}(f(x_1, x_2)) = \sqrt{c_{m,n,h}}\; \Gamma_{xy}^{h} \Delta_{yx}^{n-h}(f(x_1, x_2))$$

where $f(x_1, x_2)$ is homogeneous polynomial in x_1, x_2 of degree $m + n - 2h$.

By Lemma 2.2.3, and the fact that a composition of two G-equivariant maps is G-equivariant, we have:

Proposition 2.3.3. *For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, the map $\alpha_{m,n,h}$ is an $SU(2)$-equivariant map.*

As a result of Theorem 2.2.4, and Lemma 2.2.3, we get

Lemma 2.3.4. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$.*

1. *The conjugate map of $\alpha_{m,n,h}$ is given by*

$$\alpha^*_{m,n,h} : P_m \otimes P_n \longrightarrow P_{m+n-2h}$$

$$\alpha^*_{m,n,h}\,(g(x_1,\, x_2,\, y_1,\, y_2)) = \sqrt{c_{m,n,h}}\ \Delta^{n-h}_{xy}\Omega^h_{xy}(g(x_1,\, x_2,\, y_1,\, y_2))$$

   where $g(x_1, x_2, y_1, y_2)$ is a homogeneous polynomial of degree m in x_1, x_2, and homogeneous of degree n in y_1, y_2.

2. $\sum\limits_{h=0}^{\min\{m,n\}} \alpha_{m,n,h}\alpha^*_{m,n,h} = I_{P_m \otimes P_n}$.

Proposition 2.3.5. *For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, the map $\alpha_{m,n,h}$ is an isometry.*

Proof:

For $0 \leq h, s \leq \min\{m, n\}$, the map $\alpha^*_{m,n,h}\alpha_{m,n,s} : P_{m+n-2s} \longrightarrow P_{m+n-2h}$ is an $SU(2)$-equivariant map. By Schur's Lemma 1.2.12, we have

$$\alpha^*_{m,n,h}\alpha_{m,n,s} = \begin{cases} 0 & if \quad h \neq s \\ \lambda I_{P_{m+n-2h}} & if \quad h = s \end{cases} \tag{2.3.1}$$

for some non-negative integer λ. It remains to show that $\lambda = 1$. By Lemma 2.3.4, the map $\sum\limits_{s=0}^{\min\{m,n\}} \alpha_{m,n,s}\alpha^*_{m,n,s}$ is the identity map on the space $P_m \otimes P_n$. Thus, for any $0 \leq h \leq \min\{m, n\}$, we have

$$\alpha^*_{m,n,h} = \alpha^*_{m,n,h}\, I_{P_m \otimes P_n} = \alpha^*_{m,n,h} \sum_{s=0}^{\min\{m,n\}} \alpha_{m,n,s}\alpha^*_{m,n,s} = \sum_{s=0}^{\min\{m,n\}} \alpha^*_{m,n,h}\alpha_{m,n,s}\alpha^*_{m,n,s}$$

By Equation (2.3.1) above, we get

$$\alpha^*_{m,n,h} = \alpha^*_{m,n,h}\alpha_{m,n,h}\alpha^*_{m,n,h} = \lambda\alpha^*_{m,n,h}$$

Since $\alpha_{m,n,h} \neq 0$ ($\alpha_{m,n,h}(x_1^{m+n-2h}) \neq 0$), and $\left\|\alpha^*_{m,n,h}\right\| = \|\alpha_{m,n,h}\|$, then $\alpha^*_{m,n,h} \neq 0$ which gives $\lambda = 1$. ∎

Corollary 2.3.6. *Let $m, n \in \mathbb{N}$. The $SU(2)$-space*

$$P_m \otimes P_n = \bigoplus_{h=0}^{\min\{m,n\}} W_{m+n-2h}$$

where $\{W_{m+n-2h} \simeq P_{m+n-2h}, 0 \leq h \leq \min\{m,n\}\}$ are mutually orthogonal $SU(2)$-subspaces, such that W_{m+n-2h} is the range of the orthogonal projection $\alpha_{m,n,h}\alpha^*_{m,n,h}$. This decomposition into $SU(2)$-irreducible subspaces is unique up to permutation.

Proof:

Let $0 \leq h \leq \min\{m,n\}$. By Proposition 2.3.5, the map $\alpha_{m,n,h}\alpha^*_{m,n,h}$ is an orthogonal projection. Let $W_{m+n-2h} = \alpha_{m,n,h}\alpha^*_{m,n,h}(P_m \otimes P_n)$. By surjectivity of $\alpha^*_{m,n,h}$, the equivariance of $\alpha_{m,n,h}$, and the irreducibility of P_{m+n-2h}, the subspace $W_{m+n-2h} = \alpha_{m,n,h}(P_{m+n-2h})$ is an $SU(2)$-irreducible subspace of $P_m \otimes P_n$ that is isomorphic to P_{m+n-2h}. The mutual orthogonality of the subspaces W_{m+n-2h} follows by Corollary 1.2.13. Hence

$$\bigoplus_{h=0}^{\min\{m,n\}} W_{m+n-2h} \subseteq P_m \otimes P_n$$

By comparing the dimensions, we get the equality $P_m \otimes P_n = \bigoplus_{h=0}^{\min\{m,n\}} W_{m+n-2h}$. The uniqueness follows by Corollary 1.2.16. ∎

A similar result can be stated for the space $P_m \otimes \overline{P}_n$. We need the following lemma, whose proof is straightforward using Proposition 2.1.6. Recall that $\overline{P}_n$ is an $SU(2)$-irreducible space under the contragredient representation $\check{\rho}_n$.

Lemma 2.3.7. *Let $m, n \in \mathbb{N}$.*

1. *The map $I_{P_m} \otimes J_n : P_m \otimes P_n \longrightarrow P_m \otimes \overline{P}_n$ is an $SU(2)$-equivariant unitary isomorphism whose inverse is $I_{P_m} \otimes J_n^*$.*

2. *The map $\eta_{m,n,h} = (I_{P_m} \otimes J_n)\,\alpha_{m,n,h}$ is an $SU(2)$-equivariant isometry from P_{m+n-2h} into $P_m \otimes \overline{P}_n$.*

Corollary 2.3.8. *Let $m, n \in \mathbb{N}$. The $SU(2)$-space*

$$P_m \otimes \overline{P}_n = \bigoplus_{h=0}^{\min\{m,n\}} V_{m+n-2h}$$

where $\{V_{m+n-2h} \simeq P_{m+n-2h}, 0 \leq h \leq \min\{m,n\}\}$ are mutually orthogonal $SU(2)$-subspaces, such that V_{m+n-2h} is the range of the orthogonal projection $\eta_{m,n,h}\eta^*_{m,n,h}$. This decomposition into $SU(2)$-irreducible subspaces is unique up to permutation.

2.3.2 The matrix coefficients of $\alpha_{m,n,h}$

In this section, we give the matrix coefficients of the isometry $\alpha_{m,n,h}$ with respect to the standard basis for P_{m+n-2h}. The proof of Lemma 2.3.11 below is a direct computation, and is deferred to Appendix **B**. To simplify our notation, we state the following definition.

Definition 2.3.9. *For a subset A of a space X, the indicator function $\chi_A : X \longrightarrow \{0,1\}$ is defined by*

$$\chi_A(x) = \begin{cases} 1 & if \quad x \in A \\ 0 & if \quad x \notin A \end{cases}$$

For the rest of the thesis, we will systematically use the following notation without further mention. For quick reference, Appendix **C** contains the list of notation and equation that are used in the thesis.

Notation 2.3.10. For $m, n, h, i, j \in \mathbb{N}$ with $0 \leq h \leq \min\{m,n\}$, $0 \leq i \leq m+n-2h$, and $0 \leq j \leq n$, we define

- $B(i) := \{j : \max\{0, -m+i+h\} \leq j \leq \min\{i+h,\, n\}\}$.

- $l_{ij} := i - j + h$.

Lemma 2.3.11. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, and $r = m + n - 2h$. Then*

1. $\alpha_{m,n,h}\left(f_i^r\right) = \sum_{s=0}^{h} \sum_{j=\max\{s,-m+i+h+s\}}^{\min\{i+s,\, n-h+s\}} \beta_{i,s,j}^{m,n,h}\, f_{l_{ij}}^m \otimes f_j^n$

2. $\alpha^*_{m,n,h}\left(f_l^m \otimes f_j^n\right) = \left(\sum_{s=\max\{0,h-l,h+j-n\}}^{\min\{h,j,m-l\}} \beta_{l+j-h,s,j}^{m,n,h}\right) f_{l+j-h}^r \cdot \chi_{[0,r]}(l+j-h)$

   where
$$\beta_{i,s,j}^{m,n,h} = (-1)^s \frac{\binom{h}{s}\binom{n-h}{j-s}\binom{m-h}{i-j+s}}{(m-h)!} \sqrt{\frac{c_{m,n,h}r!\ m!\ n!}{\binom{r}{i}\binom{m}{i-j+h}\binom{n}{j}}}$$

and $\{f_t^k : 0 \leq t \leq k\}$ is the standard basis for P_k, where $k \in \{m, n, r\}$.

Remark 2.3.12. The vectors $f_{l_{ij}}^m$ and f_{l+j-h}^r, in Lemma 2.3.11, are indeed elements of the basis for P_m, and P_r respectively. This follows since

$$\max\{s, -m+i+h+s\} \leq j \leq \min\{i+s,\, n-h+s\}$$

implies
$$0 \leq \max\{0, i-n+h\} \leq l_{ij} \leq \min\{i+h, m\} \leq m$$
and the sum $\sum_{s=\max\{0,h-l,h+j-n\}}^{\min\{h,j,m-l\}} \beta_{l+j-h,s,j}^{m,n,h}$ is nonempty if and only if

$$\max\{0, h-l, h+j-n\} \leq \min\{h, j, m-l\}$$

which implies $0 \leq l + j - h \leq r$.

The following corollary gives more compact forms of the formulae in Lemma 2.3.11.

Corollary 2.3.13. *For $m, n, h \in \mathbb{N}$ with $0 \le h \le \min\{m, n\}$, let $r = m + n - 2h$. The values of the maps $\alpha_{m,n,h}$ and $\alpha^*_{m,n,h}$ on the elements of the standard bases for P_r and $P_m \otimes P_n$ are given by*

$$\alpha_{m,n,h}\left(f^r_i\right) = \sum_{j \in B(i)} \varepsilon^j_{i\,(m,n,h)}\, f^m_{l_{ij}} \otimes f^n_j$$

and

$$\alpha^*_{m,n,h}\left(f^m_l \otimes f^n_j\right) = \varepsilon^j_{l+j-h\,(m,n,h)} f^r_{l+j-h} \cdot \chi_{[0,r]}(l+j-h)$$

where $\varepsilon^j_{t\,(m,n,h)} = \displaystyle\sum_{s=\max\{0,j-t,j+h-n\}}^{\min\{h,j,j+m-t-h\}} \beta^{m,n,h}_{t,s,j}.$

Proof:

For the first equality, let

$A = \{(s, j) : 0 \le s \le h,\ \max\{s, -m + i + h + s\} \le j \le \min\{i + s,\ n - h + s\}\}$, and $A_j = \{s : (s, j) \in A\}$ then

$$A = \bigcup_j \{(s, j) : s \in A_j\}$$

where the index j ranges from $\max\{0, -m + i + h\}$ at $s = 0$ to $\min\{i + h,\ n\}$ at $s = h$.

i.e

$$A_j = \{s : (s, j) \in A\} = \{s : 0 \le s \le h, j - \min\{i,\ n - h\} \le s \le j - \max\{0, -m + i + h\}\}$$

$$= \{s : \max\{0, j - \min\{i,\ n - h\}\} \le s \le \min\{h, j - \max\{0, -m + i + h\}\}\}$$

$$= \{s : \max\{0, j - i, j + h - n\} \le s \le \min\{h, j, j + m - i - h\}$$

By Lemma 2.3.11, we have

$$\alpha_{m,n,h}(f^r_i) = \sum_{(s,j)\in A} \beta^{m,n,h}_{i,s,j} f^m_{l_{ij}} \otimes f^n_j = \sum_{j=\max\{0,-m+i+h\}}^{\min\{i+h,\, n\}} \sum_{s \in A_j} \beta^{m,n,h}_{i,s,j} f^m_{l_{ij}} \otimes f^n_j$$

$$= \sum_{j=\max\{0,-m+i+h\}}^{\min\{i+h,\, n\}} \sum_{s=\max\{0,j-i,j+h-n\}}^{\min\{h,j,j+m-i-h\}} \beta^{m,n,h}_{i,s,j} f^m_{l_{ij}} \otimes f^n_j = \sum_{j\in B(i)} \varepsilon^j_{i\,(m,n,h)}\, f^m_{l_{ij}} \otimes f^n_j.$$

The second equality follows by Lemma 2.3.11. ∎

For the rest of the thesis, when m, n, h are clear from context, we will abbreviate $\varepsilon_{i\,(m,n,h)}^{j}$ to ε_i^j.

Remarks 2.3.14. Let $m, n, h \in \mathbb{N}$, with $0 \leq h \leq \min\{m, n\}$, and $r = m + n - 2h$.

1. For $0 \leq i \leq r$, we have
   (a) The set $B(i)$ is non-empty, as $\max\{0, -m + i + h\} \leq \min\{i + h, n\}$.
   (b) $B(r - i) = n - B(i)$.
2. If $B^{m,n,h}(i)$ denotes the set $B(i)$ associated to $\alpha_{m,n,h}$, and $B^{n,m,h}(i)$ denotes the set $B(i)$ associated to $\alpha_{n,m,h}$, then
$$j \in B^{m,n,h}(i) \quad \text{if and only if} \quad l_{ij} \in B^{n,m,h}(i)$$
3. The map $\alpha_{m,n,h}$ can be written as
$$\alpha_{m,n,h} = \sum_{i=0}^{r} \sum_{j \in B(i)} \varepsilon_i^j \left(f_{l_{ij}}^m \otimes f_j^n \right) f_i^{r^*}$$
4. The map $\eta_{m,n,h}$ in Lemma 2.3.7 is given on the basis elements for P_r by
$$\eta_{m,n,h}\left(f_i^r\right) = \sum_{j \in B(i)} (-1)^j \varepsilon_{i\,(m,n,h)}^{j}\, f_{l_{ij}}^m \otimes f_{n-j}^n$$

The following corollary, whose proof is in Appendix **B**, contains basic relations for the coefficients ε_i^j.

Corollary 2.3.15. *For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, let $r = m + n - 2h$. The matrix coefficients $\varepsilon_i^j := \varepsilon_{i\,(m,n,h)}^{j}$ of the isometry $\alpha_{m,n,h}$ satisfy*

1. $\varepsilon_i^j = (-1)^h \varepsilon_{r-i}^{n-j}$ *for* $0 \leq i \leq r$ *and* $j \in B(i)$.

2. $\varepsilon_i^{i+h} = \beta_{i,h,h+i}^{m,n,h}$ *for* $i \leq n-h$.

3. $\varepsilon_i^{n} = \beta_{i,h,n}^{m,n,h} = (-1)^h \left|\beta_{i,h,n}^{m,n,h}\right| \neq 0$ *for* $n-h \leq i \leq r$.

4. $\varepsilon_0^{j} = \beta_{0,j,j}^{m,n,h} = (-1)^j \left|\beta_{0,j,j}^{m,n,h}\right| \neq 0$ *for* $j \in B(0)$.

5. $\varepsilon_i^{0} = \beta_{i,0,0}^{m,n,h} \neq 0$ *for* $0 \leq i \leq m-h$.

6. $\varepsilon_i^{j}{}_{(m,n,n)} = \beta_{i,j,j}^{m,n,n}$, *and* $\varepsilon_i^{j}{}_{(m,n,0)} = \beta_{i,0,j}^{m,n,0}$.

Corollary 2.3.16. *Let* $m,n,h \in \mathbb{N}$ *with* $0 \leq h \leq \min\{m,n\}$, *and* $r = m+n-2h$.

1. *The coefficient* $c_{m,n,h}$ *in the Clebsch-Gordan expansion (Theorem 2.2.4), is given by*

$$c_{m,n,h} = \frac{((m-h)!)^2}{r!\ m!\ n! \left(\sum_{k=0}^{h} \frac{\binom{h}{k}^2}{\binom{m}{h-k}\binom{n}{k}} \right)}$$

Consequently,

$$\beta_{i,s,j}^{m,n,h} = \frac{(-1)^s \binom{h}{s}\binom{n-h}{j-s}\binom{m-h}{i-j+s}}{\sqrt{\binom{r}{i}\binom{m}{i-j+h}\binom{n}{j}\left(\sum_{k=0}^{h} \frac{\binom{h}{k}^2}{\binom{m}{h-k}\binom{n}{k}} \right)}}$$

2. *For* $0 \leq i \leq r$, *and* $j \in B(i)$, *we have*

$$\varepsilon_i^{j}{}_{(m,n,h)} = (-1)^h \varepsilon_i^{l_{ij}}{}_{(n,m,h)}$$

Proof:

By Corollary 2.3.13, we have $\alpha_{m,n,h}(f_0^r) = \sum_{j=0}^{h} \beta_{0,j,j}^{m,n,h} f_{l_{0j}}^m \otimes f_j^n$. Since $\left\{ f_{l_{0j}}^m \otimes f_j^n \right\}$ are orthonormal set, and $\alpha_{m,n,h}$ is isometry, then $1 = \sum_{j=0}^{h} \left(\beta_{0,j,j}^{m,n,h}\right)^2$. As

$$\beta_{0,j,j}^{m,n,h} = (-1)^j \sqrt{c_{m,n,h}}\ \frac{\binom{h}{j}}{(m-h)!} \sqrt{\frac{r!\ m!\ n!}{\binom{m}{h-j}\binom{n}{j}}},$$

the first statement follows. For the second one, by using the formula for ε_i^j in Corollary 2.3.13, we have

$$\varepsilon_i^{l_{ij}}(n,m,h) = \sum_{t=\max\{0,l_{ij}-i,l_{ij}+h-m\}}^{\min\{h,l_{ij},l_{ij}-i-h+n\}} \beta_{i,t,l_{ij}}^{n,m,h} = \sum_{t=\max\{0,h-j,i+2h-j-m\}}^{\min\{h,i-j+h,n-j\}} \beta_{i,t,l_{ij}}^{n,m,h}$$

By Remarks 2.3.14 (2), and since $\beta_{i,h-s,l_{ij}}^{n,m,h} = (-1)^h \beta_{i,s,j}^{m,n,h}$ for any $0 \leq s \leq h$, we have

$$\begin{aligned}\varepsilon_i^{l_{ij}}(n,m,h) &= \sum_{t=\max\{0,h-j,i+2h-j-m\}}^{\min\{h,i-j+h,n-j\}} \beta_{i,t,l_{ij}}^{n,m,h} = \sum_{s=\max\{0,j-i,j+h-n\}}^{\min\{h,j,j-i+m-h\}} \beta_{i,h-s,l_{ij}}^{n,m,h} \\ &= \sum_{s=\max\{0,j-i,j+h-n\}}^{\min\{h,j,j-i+m-h\}} (-1)^h \beta_{i,s,j}^{m,n,h} = (-1)^h \varepsilon_i^j(m,n,h).\end{aligned}$$

∎

2.4 An application: The algebra $End(P_m)$ as a direct sum of orthogonal $SU(2)$-subspaces

In this section, following [29, p.580], we express the algebra $End(P_m)$ as a direct sum of mutually orthogonal $SU(2)$-subspaces, and find explicit formulae for the projections on these subspaces. We also give a general method to decompose a matrix $A \in End(P_m)$ into an orthogonal direct sum of matrices, and compute the first two matrices in this decomposition.

The following proposition is a direct result of Corollary 1.2.16, Lemma 1.2.25, and Corollary 2.3.8.

Proposition 2.4.1. *Let $m \in \mathbb{N}$. The algebra $End(P_m)$ can be written uniquely as an orthogonal direct sum of $SU(2)$-irreducible subspaces. i.e.*

$$End(P_m) = \bigoplus_{t=0}^{m} U_{2t}$$

where $\{U_{2t} : 0 \leq t \leq m\}$ *is a set of* $SU(2)$*-irreducible subspaces each of them is isomorphic to* P_{2t} *for some* $0 \leq t \leq m$.

The next proposition gives formulae for the projections of $End(P_m)$ onto the subspaces $\{U_{2t} : 0 \leq t \leq m\}$. Recall that by Corollary 2.3.8, the map $\eta_{m,m,m-t}\eta^*_{m,m,m-t}$ is the projection of $P_m \otimes \overline{P}_m$ onto the $SU(2)$-invariant subspace that is isomorphic to P_{2t}.

Proposition 2.4.2. *Let* $m \in \mathbb{N}$, *and* $\bigoplus_{t=0}^{m} U_{2t}$ *be the decomposition of* $End(P_m)$ *into a direct sum of* $SU(2)$*-irreducible subspaces. For each* $0 \leq t \leq m$, *the map*

$$\mathrm{Vec}^*\eta_{m,m,m-t}\eta^*_{m,m,m-t}\mathrm{Vec}$$

is the $SU(2)$*-equivariant orthogonal projection of* $End(P_m)$ onto U_{2t}.

Proof:

By Lemma 1.2.25, and Lemma 2.3.7, the map

$$\mathrm{Vec}^*\eta_{m,m,m-t}\eta^*_{m,m,m-t}\mathrm{Vec} : End(P_m) \longrightarrow P_m \otimes \overline{P}_m \longrightarrow End(P_m)$$

is an $SU(2)$-equivariant orthogonal projection. Since the map Vec is unitary $SU(2)$-equivariant, and the space

$$P_m \otimes \overline{P}_m = \bigoplus_{t=0}^{m} V_{2t}$$

with $V_{2t} = \eta_{m,m,m-t}\eta^*_{m,m,m-t}(P_m \otimes \overline{P}_m) \simeq P_{2t}$ (Corollary 2.3.8), then $\mathrm{Vec}^*\eta_{m,m,m-t}\eta^*_{m,m,m-t}\mathrm{Vec}$ is a projection onto a subspace isomorphic to P_{2t}. The result follows by the uniqueness of the decomposition of $End(P_m)$. ∎

Corollary 2.4.3. *Let* $m \in \mathbb{N}$, *and* $A \in End(P_m)$. *The matrix of* A *can be decomposed into a direct sum of mutually orthogonal matrices* $(A_0, A_2, ...A_{2m})$, *where*

$$A_{2t} = \mathrm{Vec}^*\eta_{m,m,m-t}\eta^*_{m,m,m-t}\mathrm{Vec}(A).$$

Namely,
$A = \sum_{t=0}^{m} A_{2t}$ *where* $A_{2t} \in U_{2t}$, *and* $End(P_m) = \bigoplus_{t=0}^{m} U_{2t}$.

In the rest of this section, we find a general formula to compute the decomposition of a matrix $A \in End(P_m)$ into a direct sum of mutually orthogonal matrices $\{A_{2t}, 0 \leq t \leq m\}$. By Corollary 2.4.3, A_{2t} is obtained by applying the two following steps :

1. Computing the vectors $v_{2t} = \eta^*_{m,m,m-t}\text{Vec}(A) \in P_{2t}$ for each $0 \leq t \leq m$.
2. Computing the mutually orthogonal matrices $A_{2t} := A_{v_{2t}} = \text{Vec}^*\eta_{m,m,m-t}(v_{2t})$.

For a better explanation of this idea, we find the decomposition for a general matrix $A \in End(P_1)$. Recall that $\eta_{m,m,m-t} = (I_{P_m} \otimes J_m)\,\alpha_{m,m,m-t}$, and that by Remark 2.1.7, we have $J_m(f_l^m) = (-1)^l f_{m-l}^m$, $J_m^*(f_l^m) = (-1)^{m-l} f_{m-l}^m$

Example 2.4.4. Let $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in End(P_1)$. The matrix A is decomposed into (A_0, A_2) where

$$A_0 = \begin{pmatrix} \frac{a_{11}+a_{22}}{2} & 0 \\ 0 & \frac{a_{11}+a_{22}}{2} \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} \frac{a_{11}-a_{22}}{2} & a_{12} \\ a_{21} & \frac{a_{22}-a_{11}}{2} \end{pmatrix}$$

Since

$$\langle A_0 \,|A_2 \rangle_{End(P_1)} = tr(A_0^* A_2) = 0$$

then A_0 and A_2 are mutually orthogonal.

Proof:

Fix the basis for $End(P_1)$ in the following order $\{f_0^1 f_0^{1^*}, f_1^1 f_0^{1^*}, f_0^1 f_1^{1^*}, f_1^1 f_1^{1^*}\}$. Let $A = \sum_{i,j=0}^{1} a_{(i+1)(j+1)}(f_i^1 f_j^{1^*})$. By Corollary 2.4.3, for any $t \in \{0,1\}$, we have

$$A_{2t} = \sum_{i,j=0}^{1} a_{(i+1)(j+1)} \mathrm{Vec}^* \eta_{1,1,1-t} \eta_{1,1,1-t}^* \mathrm{Vec}(f_i^1 f_j^{1^*}).$$

- Case $t = 0$:

  Let $\varepsilon_i^j := \varepsilon_{i\,(1,1,1)}^j$. Using Corollary 2.3.13, and Remark 2.1.7, we have:

$$\begin{aligned}\eta_{1,1,1}^* \mathrm{Vec}(f_i^1 f_j^{1^*}) &= \eta_{1,1,1}^*(f_i^1 \otimes f_j^1) = \alpha_{1,1,1}^*(I_{P_1} \otimes J_1^*)(f_i^1 \otimes f_j^1) \\ &= \alpha_{1,1,1}^*(f_i^1 \otimes (-1)^{1-j} f_{1-j}^1) = (-1)^{1-j} \varepsilon_{i-j}^{1-j} f_{i-j}^0 \delta_{ij} \\ &= (-1)^{1-j} \varepsilon_1^{1-j} \delta_{ij} f_0^0\end{aligned}$$

  but

$$\begin{aligned}\mathrm{Vec}^* \eta_{1,1,1}(f_0^0) &= \mathrm{Vec}^*(I_{P_1} \otimes J_1)\alpha_{1,1,1}(f_0^0) \\ &= \mathrm{Vec}^*(I_{P_1} \otimes J_1)(\sum_{s=0}^{1} \varepsilon_0^s f_{1-s}^1 \otimes f_s^1) \\ &= \mathrm{Vec}^*(\sum_{s=0}^{1} (-1)^s \varepsilon_0^s f_{1-s}^1 \otimes f_{1-s}^1) \\ &= \sum_{s=0}^{1} (-1)^s \varepsilon_0^s f_{1-s}^1 f_{1-s}^{1*} = \varepsilon_0^0 f_1^1 f_1^{1^*} - \varepsilon_0^1 f_0^1 f_0^{1^*};\end{aligned}$$

  then,

$$\begin{aligned}\mathrm{Vec}^* \eta_{1,1,1} \eta_{1,1,1}^* \mathrm{Vec}(f_i^1 f_j^{1^*}) &= (-1)^{1-j} \varepsilon_1^{1-j} \delta_{ij} \mathrm{Vec}^* \eta_{1,1,1}(f_0^0) \\ &= (-1)^{1-j} \varepsilon_1^{1-j} \delta_{ij} (\varepsilon_0^0 f_1^1 f_1^{1^*} - \varepsilon_0^1 f_0^1 f_0^{1^*}) \\ &= (-1)^{1-j} \varepsilon_1^{1-j} \delta_{ij} (\tfrac{1}{\sqrt{2}} f_1^1 f_1^{1^*} + \tfrac{1}{\sqrt{2}} f_0^1 f_0^{1^*}).\end{aligned}$$

Hence,

$$A_0 = \mathrm{Vec}^* \eta_{1,1,1}\eta^*_{1,1,1}\mathrm{Vec}(A) = (\tfrac{1}{\sqrt{2}} f^1_1 f^{1^*}_1 + \tfrac{1}{\sqrt{2}} f^1_0 f^{1^*}_0)\sum_{i,j=0}^{1} a_{(i+1)(j+1)}(-1)^{1-j}\varepsilon^{1-j}_1 \delta_{ij}$$
$$= (\tfrac{1}{\sqrt{2}} f^1_1 f^{1^*}_1 + \tfrac{1}{\sqrt{2}} f^1_0 f^{1^*}_0)(-\varepsilon^1_0 a_{11} + \varepsilon^0_0 a_{22})$$
$$= (\tfrac{1}{\sqrt{2}} f^1_1 f^{1^*}_1 + \tfrac{1}{\sqrt{2}} f^1_0 f^{1^*}_0)(\tfrac{1}{\sqrt{2}} a_{11} + \tfrac{1}{\sqrt{2}} a_{22})$$
$$= \tfrac{a_{11}+a_{22}}{2} I_2.$$

- <u>Case $t = 1$</u> :

Let $\varepsilon^j_i := \varepsilon^j_{i\,(1,1,0)}$, using Corollary 2.3.13, and Remark 2.1.7, we have

$$\eta^*_{1,1,0}\mathrm{Vec}(f^1_i f^{1^*}_j) = \eta^*_{1,1,0}(f^1_i \otimes f^1_j) = \alpha^*_{1,1,0}(I_{P_1} \otimes J^*_1)(f^1_i \otimes f^1_j)$$
$$= \alpha^*_{1,1,0}(f^1_i \otimes (-1)^{1-j} f^1_{1-j})$$
$$= (-1)^{1-j}\varepsilon^{1-j}_{i-j+1} f^2_{i-j+1} \cdot \chi_{[-1,1]}(i-j+1)$$

so

$$\eta^*_{1,1,0}\mathrm{Vec}(f^1_0 f^{1^*}_0) = -\varepsilon^1_1 f^2_1, \qquad \eta^*_{1,1,0}\mathrm{Vec}(f^1_0 f^{1^*}_1) = \varepsilon^0_0 f^2_0$$

and

$$\eta^*_{1,1,0}\mathrm{Vec}(f^1_1 f^{1^*}_0) = -\varepsilon^1_2 f^2_2, \qquad \eta^*_{1,1,0}\mathrm{Vec}(f^1_1 f^{1^*}_1) = \varepsilon^0_1 f^2_1.$$

As for $0 \le l \le 2$,

$$\mathrm{Vec}^*\eta_{1,1,0}(f^2_l) = \mathrm{Vec}^*(I_{P_1} \otimes J_1)\alpha_{1,1,0}(f^2_l) = \mathrm{Vec}^*(I_{P_1} \otimes J_1)(\sum_{s=\max\{0,l-1\}}^{\min\{l,1\}} \varepsilon^s_l f^1_{l-s} \otimes f^1_s)$$
$$= \mathrm{Vec}^*(\sum_{s=\max\{0,l-1\}}^{\min\{l,1\}} (-1)^s \varepsilon^s_l f^1_{l-s} \otimes f^1_{1-s}) = \sum_{s=\max\{0,l-1\}}^{\min\{l,1\}} (-1)^s \varepsilon^s_l f^1_{l-s} f^{1^*}_{1-s}$$

and

$$\varepsilon^0_0 = 1 = \varepsilon^1_2, \quad \text{and} \qquad \varepsilon^0_1 = \tfrac{1}{\sqrt{2}} = \varepsilon^1_1,$$

we have:

1. $\mathrm{Vec}^*\eta_{1,1,0}\eta^*_{1,1,0}\mathrm{Vec}(f^1_0 f^{1^*}_0) = (\varepsilon^1_1)^2 f^1_0 f^{1^*}_0 - \varepsilon^0_1\varepsilon^1_1 f^1_1 f^{1^*}_1 = \frac{1}{2} f^1_0 f^{1^*}_0 - \frac{1}{2} f^1_1 f^{1^*}_1$.
2. $\mathrm{Vec}^*\eta_{1,1,0}\eta^*_{1,1,0}\mathrm{Vec}(f^1_0 f^{1^*}_1) = (\varepsilon^0_0)^2 f^1_0 f^{1^*}_1 = f^1_0 f^{1^*}_1$.
3. $\mathrm{Vec}^*\eta_{1,1,0}\eta^*_{1,1,0}\mathrm{Vec}(f^1_1 f^{1^*}_0) = (\varepsilon^1_2)^2 f^1_1 f^{1^*}_0 = f^1_1 f^{1^*}_0$.
4. $\mathrm{Vec}^*\eta_{1,1,0}\eta^*_{1,1,0}\mathrm{Vec}(f^1_1 f^{1^*}_1) = (\varepsilon^0_1)^2 f^1_1 f^{1^*}_1 - \varepsilon^0_1\varepsilon^1_1 f^1_0 f^{1^*}_0 = \frac{1}{2} f^1_1 f^{1^*}_1 - \frac{1}{2} f^1_0 f^{1^*}_0$.

Thus

$$\begin{aligned} A_2 &= a_{11}\left(\tfrac{1}{2} f^1_0 f^{1^*}_0 - \tfrac{1}{2} f^1_1 f^{1^*}_1\right) + a_{21} f^1_1 f^{1^*}_0 + a_{12} f^1_0 f^{1^*}_1 + a_{22}\left(\tfrac{1}{2} f^1_1 f^{1^*}_1 - \tfrac{1}{2} f^1_0 f^{1^*}_0\right) \\ &= \begin{pmatrix} \frac{a_{11}-a_{22}}{2} & a_{12} \\ a_{21} & \frac{a_{22}-a_{11}}{2} \end{pmatrix}. \end{aligned}$$

∎

The same idea in the example above is used to find the decomposition of any matrix A in $End(P_m)$ for $m \in \mathbb{N}$. By linearity, it is enough to compute the decomposition of $f^m_{i_1} f^{m^*}_{i_2}$, the basis element for $End(P_m)$. This decomposition is given in Corollary 2.4.8 below. We begin with the following lemmas which generalize the steps in the example above.

Lemma 2.4.5. *Let $m \in \mathbb{N}$, and $f^m_{i_1} f^{m^*}_{i_2}$ be an element of the standard basis of $End(P_m)$. Then*

$$f^m_{i_1} f^{m^*}_{i_2} = (\varphi_t(v_{2t}))_{0\le t\le m}$$

where

- $\varphi_t : P_{2t} \longrightarrow U_{2t}$, *given by* $\varphi_t = Vec^*\eta_{m,m,m-t}$, *and*
- $v_{2t} = (-1)^{m-i_2}\varepsilon^{m-i_2}_{i_1-i_2+t(m,m,m-t)} f^{2t}_{i_1-i_2+t} \cdot \chi_{[-t,t]}(i_1-i_2)$

Proof:

By Corollary 2.4.3,

$$f_{i_1}^m f_{i_2}^{m^*} = \left(Vec^* \eta_{m,m,m-t} \eta_{m,m,m-t}^* Vec(f_{i_1}^m f_{i_2}^{m^*})\right)_{0 \le t \le m}$$

Let $v_{2t} = \eta_{m,m,m-t}^* \mathrm{Vec}(f_{i_1}^m f_{i_2}^{m^*}) \in P_{2t}$. Since $\eta_{m,m,m-t}^* = \alpha_{m,m,m-t}^* (I_{P_m} \otimes J_m^*)$, then by Corollary 2.3.13, and Remark 2.1.7, we have

$$v_{2t} = (-1)^{m-i_2} \varepsilon_{i_1-i_2+t}^{m-i_2}{}_{(m,m,m-t)} f_{i_1-i_2+t}^{2t} \cdot \chi_{[-t,t]}(i_1-i_2)$$

The result now follows. ∎

Lemma 2.4.6. *Let $m \in \mathbb{N}$ and $0 \le t \le m$. Let $\psi_t : P_{2t} \longrightarrow U_{2t}$ be the map $\psi_t = Vec^* \eta_{m,m,m-t}$. For each i such that $0 \le i \le 2t$, we have*

$$\psi_t(f_i^{2t}) = \sum_{j=\max\{0,i-t\}}^{\min\{i+m-t,m\}} (-1)^j \varepsilon_i^j{}_{(m,m,m-t)} f_{i+(m-j)-t}^m f_{m-j}^{m^*}$$

Proof:

By Remarks 2.3.14 (4),

$$\eta_{m,m,m-t}(f_i^{2t}) = \sum_{j=\max\{0,i-t\}}^{\min\{i+m-t,m\}} (-1)^j \varepsilon_i^j{}_{(m,m,m-t)} f_{i+(m-j)-t}^m \otimes f_{m-j}^m$$

so

$$\psi_t(f_i^{2t}) = Vec^* \eta_{m,m,m-t}(f_i^{2t}) = \sum_{j=\max\{0,i-t\}}^{\min\{i+m-t,m\}} (-1)^j \varepsilon_i^j{}_{(m,m,m-t)} f_{i+(m-j)-t}^m f_{m-j}^{m^*}$$

∎

Remark 2.4.7. If in the last lemma $i = t$, then the matrix $\psi_t(f_t^{2t})$ will be a diagonal matrix given by

$$\sum_{j=0}^{m} (-1)^j \varepsilon_t^j{}_{(m,m,m-t)} f_{m-j}^m f_{m-j}^{m^*}$$

Corollary 2.4.8. *Let $m \in \mathbb{N}$. For $0 \leq i_1, i_2 \leq m$, we have*

$$f_{i_1}^m f_{i_2}^{m^*} = \big(C_{2t}(f_{i_1}^m f_{i_2}^{m^*})\big)_{0 \leq t \leq m}$$

where $\big\{C_{2t}(f_{i_1}^m f_{i_2}^{m^*}), 0 \leq t \leq m\big\}$ is a set of mutually orthogonal matrices given by

$$\left[\sum_{j=\max\{0, i_1-i_2\}}^{\min\{m+i_1-i_2, m\}} (-1)^{m-i_2+j} \varepsilon^{m-i_2}_{i_1-i_2+t\,(m,m,m-t)} \varepsilon^{j}_{i_1-i_2+t\,(m,m,m-t)} f^m_{i_1-i_2+(m-j)} f^{m^*}_{m-j}\right] \cdot \chi_{[-t,t]}(i_1-i_2)$$

In particular,

$$f_i^m f_i^{m^*} = \left(\sum_{j=0}^{m} (-1)^{m-i+j} \varepsilon^{m-i}_{t\,(m,m,m-t)} \varepsilon^{j}_{t\,(m,m,m-t)} f^m_{m-j} f^{m^*}_{m-j}\right)_{0 \leq t \leq m}$$

Proof:

For any s, let $\varepsilon^s_{i_1-i_2+t} := \varepsilon^s_{i_1-i_2+t\,(m,m,m-t)}$. By Lemma 2.4.5, and Lemma 2.4.6, we have

$$f_{i_1}^m f_{i_2}^{m^*} = \big(C_{2t}(f_{i_1}^m f_{i_2}^{m^*})\big)_{0 \leq t \leq m}$$

where $C_{2t}(f_{i_1}^m f_{i_2}^{m^*}) = Vec^* \eta_{m,m,m-t}(v_{2t})$ is a matrix corresponds to a unique vector

$$v_{2t} = (-1)^{m-i_2} \varepsilon^{m-i_2}_{i_1-i_2+t} f^{2t}_{i_1-i_2+t} \cdot \chi_{[-t,t]}(i_1-i_2)$$

Applying the formula in Remark 2.3.14 (4), we get

$$C_{2t}(f_{i_1}^m f_{i_2}^{m^*}) = \left[(-1)^{m-i_2} \varepsilon^{m-i_2}_{i_1-i_2+t} Vec^* \eta_{m,m,m-t}(f^{2t}_{i_1-i_2+t})\right] \cdot \chi_{[-t,t]}(i_1-i_2)$$

$$= \left[\sum_{j=\max\{0, i_1-i_2\}}^{\min\{m+i_1-i_2, m\}} (-1)^{m-i_2+j} \varepsilon^{m-i_2}_{i_1-i_2+t} \varepsilon^{j}_{i_1-i_2+t} f^m_{i_1-i_2+(m-j)} f^{m^*}_{m-j}\right] \cdot \chi_{[-t,t]}(i_1-i_2)$$

∎

Example 2.4.9. Let $m \in \mathbb{N}$, and $A \in End(P_m)$. If $(A_{2t})_{0\leq t\leq m}$ is the decomposition of A into mutually orthogonal matrices, then

$$A_0 = \tfrac{tr(A)}{m+1}\, I_{P_m}$$

Proof:

Let $A = \sum\limits_{i_1,i_2=0}^{m} a_{(i_1+1)(i_2+1)} f_{i_1}^m f_{i_2}^{m^*}$. Using Corollary 2.4.3, we have

$$\begin{aligned} A_0 = \mathrm{Vec}^*\eta_{m,m,m}\eta^*_{m,m,m}\mathrm{Vec}(A) &= \sum_{i_1,i_2=0}^{m} a_{(i_1+1)(i_2+1)}\mathrm{Vec}^*\eta_{m,m,m}\eta^*_{m,m,m}\mathrm{Vec}(f_{i_1}^m f_{i_2}^{m^*}) \\ &= \sum_{i_1,i_2=0}^{m} a_{(i_1+1)(i_2+1)} C_0(f_{i_1}^m f_{i_2}^{m^*}) \end{aligned}$$

By Corollary 2.4.8, for $0 \leq i_1, i_2 \leq m$, we have

$$C_0(f_{i_1}^m f_{i_2}^{m^*}) = \left[\sum_{j=0}^{m} (-1)^{m-i_2+j}\varepsilon_0^{m-i_2}{}_{(m,m,m)}\varepsilon_0^{j}{}_{(m,m,m)} f_{m-j}^m f_{m-j}^{m^*}\right]\cdot \delta_{i_1 i_2}$$

thus

$$A_0 = \sum_{i=0}^{m} a_{(i+1)(i+1)}\left(\sum_{j=0}^{m}(-1)^{m-i+j}\varepsilon_0^{m-i}{}_{(m,m,m)}\varepsilon_0^{j}{}_{(m,m,m)} f_{m-j}^m f_{m-j}^{m^*}\right)$$

as

$\varepsilon_0^{m-i}{}_{(m,m,m)} = (-1)^{m-i}\frac{1}{\sqrt{m+1}}$, and $\varepsilon_0^{j}{}_{(m,m,m)} = (-1)^{j}\frac{1}{\sqrt{m+1}}$, we have

$$A_0 = \sum_{i=0}^{m} a_{(i+1)(i+1)}\left(\sum_{j=0}^{m}\frac{1}{m+1} f_{m-j}^m f_{m-j}^{m^*}\right) = \frac{1}{m+1} tr(A) I_{P_m}.$$

∎

Corollary 2.4.10. *Let $m \in \mathbb{N}$, $A \in End(P_m)$, and $(A_{2t})_{0\leq t\leq m}$ is the decomposition of A into mutually orthogonal matrices. If $tr(A) \neq 0$, then for each $1 \leq t \leq m$*

$$tr(A_{2t}) = 0$$

To continue in finding formulae for $\{A_{2t}, 0 < t \leq m\}$, we apply the same algorithm in the example above. Due to the complicated computations that are needed to find $C_{2t}(f^m_{i_1} f^{m^*}_{i_2})$ for general t, we only compute the matrix A_2 (at $t = 1$) in the decomposition of A. Before doing so, we need a computational lemma whose proof is in Appendix **B**.

Lemma 2.4.11. *Let $m \in \mathbb{N} \setminus \{0\}$, and $\varepsilon^j_i := \varepsilon^j_{i\,(m,m,m-1)}$. The following identities hold*

1. $\varepsilon^j_0 = (-1)^j \sqrt{\frac{6(j+1)(m-j)}{m(m+1)(m+2)}}$ *for* $0 \leq j \leq m-1$.

2. $\varepsilon^j_1 = (-1)^j \sqrt{\frac{3}{m(m+1)(m+2)}}\,(m-2j)$ *for* $0 \leq j \leq m$.

3. $\varepsilon^j_2 = (-1)^{j-1} \sqrt{\frac{6j(m-j+1)}{m(m+1)(m+2)}}$ *for* $1 \leq j \leq m$.

The following proposition is a direct result of Corollary 2.4.8, and Lemma 2.4.11. Note that if $f^m_{i_1} f^{m^*}_{i_2} \notin \{f^m_i f^{m^*}_i, f^m_i f^{m^*}_{i+1}, f^m_{i+1} f^{m^*}_i\}$, then $|i_1 - i_2| > 1$ and $C_2(f^m_{i_1} f^{m^*}_{i_2})$ will be a zero matrix.

Proposition 2.4.12. *Let $m \in \mathbb{N}$. Then*

1. $C_2(f^m_i f^{m^*}_i) = \frac{-3(m-2i)}{m(m+1)(m+2)} \sum_{j=0}^{m} (m-2j) f^m_{m-j} f^{m^*}_{m-j},$ *for* $0 \leq i \leq m$.
2. $C_2(f^m_i f^{m^*}_{i+1}) = \frac{6\sqrt{(i+1)(m-i)}}{m(m+1)(m+2)} \sum_{j=0}^{m-1} \sqrt{(j+1)(m-j)}\, f^m_{m-j-1} f^{m^*}_{m-j},$ *for* $0 \leq i \leq m-1$.
3. $C_2(f^m_{i+1} f^{m^*}_i) = \frac{6\sqrt{(i+1)(m-i)}}{m(m+1)(m+2)} \sum_{j=1}^{m} \sqrt{j(m-j+1)}\, f^m_{m-j+1} f^{m^*}_{m-j},$ *for* $0 \leq i \leq m-1$.
4. *$C_2(f^m_{i_1} f^{m^*}_{i_2})$ is a zero matrix for any $f^m_{i_1} f^{m^*}_{i_2} \notin \{f^m_i f^{m^*}_i, f^m_i f^{m^*}_{i+1}, f^m_{i+1} f^{m^*}_i\}$.*

Example 2.4.13. Let $m \in \mathbb{N}$ and, $A = \sum_{i_1,i_2=0}^{m} a_{(i_1+1)(i_2+1)} f_{i_1}^m f_{i_2}^{m^*} \in End(P_m)$. Let $(A_{2t})_{0 \le t \le m}$ be the decomposition of A into mutually orthogonal matrices as in Corollary 2.4.3. Then

$$A_2 = (b_{kj})_{1 \le k,l \le m+1}$$

where

- $b_{jj} = \frac{3(m-2j+2)}{m(m+2)(m+1)} \sum_{i=1}^{m+1} a_{ii}(m-2i+2), \qquad \text{for } 1 \le j \le m+1.$
- $b_{j,j+1} = \frac{6\sqrt{j(m-j+1)}}{m(m+1)(m+2)} \sum_{i=1}^{m+1} a_{i,i+1}\sqrt{i(m-i+1)}$, and

  $b_{j+1,j} = \frac{6\sqrt{j(m-j+1)}}{m(m+1)(m+2)} \sum_{i=1}^{m+1} a_{i+1,i}\sqrt{i(m-i+1)} \qquad \text{for } 1 \le j \le m.$
- $b_{kj} = 0$ elsewhere.

i.e. A_2 has the form

$$\begin{bmatrix} b_{11} & b_{12} & 0 & 0 & 0 & \ddots & 0 \\ b_{12} & b_{22} & b_{23} & 0 & 0 & \ddots & 0 \\ 0 & b_{32} & b_{33} & b_{34} & 0 & \ddots & 0 \\ 0 & 0 & b_{43} & b_{44} & b_{45} & \ddots & 0 \\ 0 & 0 & 0 & b_{54} & b_{55} & \ddots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & b_{m,m+1} \\ 0 & 0 & 0 & 0 & 0 & b_{m+1,m} & b_{m+1,m+1} \end{bmatrix}$$

where $b_{jj}, b_{j,j+1}, b_{j+1,j}$ are given above.

Proof:

By Corollary 2.4.3, the matrix

$$A_2 = \sum_{i_1,i_2=0}^{m} a_{(i_1+1)(i_2+1)} \text{Vec}^* \eta_{m,m,m-1} \eta_{m,m,m-1}^* \text{Vec}(f_{i_1}^m f_{i_2}^{m^*}) = \sum_{i_1,i_2=0}^{m} a_{(i_1+1)(i_2+1)} C_2(f_{i_1}^m f_{i_2}^{m^*})$$

As in Proposition 2.4.12 (4),

$C_2(f_{i_1}^m f_{i_2}^{m^*}) = 0$ for $f_{i_1}^m f_{i_2}^{m^*} \notin \{f_i^m f_i^{m^*}, f_i^m f_{i+1}^{m^*}, f_{i+1}^m f_i^{m^*}\}$,

we have

$$A_2 = \sum_{i=0}^{m} a_{i+1,i+1} C_2(f_i^m f_i^{m^*}) + \sum_{i=0}^{m-1} a_{i+1,i+2} C_2(f_i^m f_{i+1}^{m^*}) + \sum_{i=0}^{m-1} a_{i+2,i+1} C_2(f_{i+1}^m f_i^{m^*})$$

Using Proposition 2.4.12 (1,2,3), we get:

$$A_2 = \sum_{j=1}^{m+1} \left(\sum_{i=1}^{m+1} a_{ii} \frac{3(m-2j+2)(m-2i+2)}{m(m+1)(m+2)} \right) f_{j-1}^m f_{j-1}^{m^*} + \sum_{j=1}^{m} \left(\sum_{i=1}^{m} a_{i,i+1} \frac{6\sqrt{i(m-i+1)}\sqrt{j(m-j+1)}}{m(m+1)(m+2)} \right) f_{j-1}^m f_j^{m^*}$$
$$+ \sum_{j=1}^{m} \left(\sum_{i=1}^{m} a_{i+1,i} \frac{6\sqrt{i(m-i+1)}\sqrt{j(m-j+1)}}{m(m+1)(m+2)} \right) f_j^m f_{j-1}^{m^*}.$$

∎

Remark 2.4.14. Since $\sum_{j=1}^{m+1} (m-2j+2) = 0$, then

$$tr(A_2) = \sum_{j=1}^{m+1} \left(\sum_{i=1}^{m+1} a_{ii} \frac{3(m-2j+2)(m-2i+2)}{m(m+1)(m+2)} \right) = \sum_{i=1}^{m+1} a_{ii} \frac{(m-2i+2)}{m(m+1)(m+2)} \sum_{j=1}^{m+1} (m-2j+2) = 0$$

which is compatible with Corollary 2.4.10.

Chapter 3

Introduction to Quantum Channels

This chapter contains the required definitions and propositions from both operator algebra and the quantum information theory needed to model our examples of quantum channels. Most of this preliminary information is taken from [16], [27], and [41].

3.1 Positive and completely positive maps

Definition 3.1.1. *Let H and K be Hilbert spaces. A linear map $\Phi : End(H) \longrightarrow End(K)$ is said to be*

- *positive if $\Phi(A) \geq 0$ for any positive matrix $A \in End(H)$.*
- *n-positive if $\Phi \otimes I_n$ is positive, where*

$$\Phi \otimes I_n : End(H) \otimes \mathbb{M}_n(\mathbb{C}) \longrightarrow End(K) \otimes \mathbb{M}_n(\mathbb{C})$$

  is the linear map, such that

$$\Phi \otimes I_n (A \otimes B) = \Phi(A) \otimes B$$

  for $A \in End(H)$ and $B \in \mathbb{M}_n(\mathbb{C})$.

- *completely positive if it is n-positive for all $n \geq 1$.*

It follows from the definition that any completely positive map is positive; however the converse is not true. The following contains an example of a positive map that is not completely positive.

Examples 3.1.2.

1. Let H be a Hilbert space. The identity map $I_{End(H)} : End(H) \longrightarrow End(H)$ is completely positive.

2. Any $*-$homomorphism is completely positive.

3. The transpose map $T : \mathbb{M}_n(\mathbb{C}) \longrightarrow \mathbb{M}_n(\mathbb{C})$ defined by taking $A \longmapsto A^t$,

   is an example of a positive map that is not completely positive [28, p.5].

For the proof of the following proposition, see Proposition A.2.3 in Appendix **A**.

Proposition 3.1.3. *Let H and K be Hilbert spaces, and let $\Phi : End(H) \longrightarrow End(K)$ be a linear map. If Φ is n-positive, then it is k-positive for all $1 \leq k \leq n$.*

Theorem 3.1.4. [28, p.35]. Let K be a Hilbert space, and $n \in \mathbb{N}$. A linear map $\Phi : \mathbb{M}_n(\mathbb{C}) \longrightarrow End(K)$ is completely positive if and only if it is n-positive.

The next theorem, known as the Choi theorem [5, 28, p.35], shows that the complete positivity of Φ is reflected in its Choi matrix (Lemma 1.2.30).

Theorem 3.1.5. Let H and K be Hilbert spaces. A linear map $\Phi : End(H) \longrightarrow End(K)$ is completely positive if and only if $C(\Phi)$ is a positive element in $End(K \otimes \overline{H})$.

Definition 3.1.6. *Let H and K be Hilbert spaces. A linear map $\Phi : End(H) \longrightarrow End(K)$ is said to be trace-preserving if $tr(\Phi(A)) = tr(A)$ for any $A \in End(H)$, where tr denotes the unnormalized trace on $End(H)$.*

3.2 Quantum channels

3.2.1 Quantum systems and quantum states

A quantum system is pair consisting of the arena, where the operations take place and where the data can be stored, and a state describing this arena known as a *quantum state* [27, p.80]. Such a quantum system is represented mathematically by a complex Hilbert space known as the state space, and a density operator on H known as the state of H. A formal definition of state is the following:

Definition 3.2.1. *Let H be a Hilbert space.*

1. *A* state *of H is a density operator $\varrho \in End(H)$, i.e, a positive operator in $End(H)$ that has trace one.*

2. *A state that is a rank one projection is called a* pure state*. An impure state is called a* mixed state*.*

3. *The maximally mixed state of H is the state $\frac{1}{d_H} I_H$.*

The set of all states of H is denoted by $D(H)$, and $\mathcal{P}(H)$ denotes the subset of all pure states of H.

Remark 3.2.2. In operator algebras, the state has a different definition corresponding to the one above, see [10, Ch.6 (6.3 and 6.7)],

Example 3.2.3. The simplest quantum system has a two-dimensional state space. It is called the qubit, and represented mathematically by $\mathbb{C}^2$. The state $e_1 e_1^* = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is an example of a pure state of $\mathbb{C}^2$. An impure state of $\mathbb{C}^2$ is $\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Remarks 3.2.4.

1. The state $\varrho \in D(H)$ is pure if and only if ϱ can be written in the form ww^* for some unit vector w in H. The fact that w is a unit vector corresponds to the condition $tr(\varrho) = 1$ $(1 = tr(ww^*) = \|w\|^2)$.

2. As proved in Section 3.1.2 in [41, p.29], the set of quantum states of a finite-dimensional Hilbert space H is a compact convex set whose extreme points are the pure states.

A quantum system that is made up of two or more other quantum systems is called a *composite system*. The state space of a composite system is the tensor product of the state spaces of the components, and the *joint state of the total system* is the tensor product of the states of the component [27, p.102]. That is, if $\varrho_i \in D(H_i)$ for each $1 \leq i \leq m$, then $\varrho_1 \otimes \varrho_2 \otimes .... \otimes \varrho_m \in D(H_1 \otimes H_2 \otimes ... \otimes H_m)$. The state $\varrho_1 \otimes \varrho_2 \otimes .... \otimes \varrho_m$ represents the case where the quantum systems H_i are mutually independent. If the state of $H_1 \otimes H_2 \otimes ... \otimes H_m$ can not be expressed as a product state, then $\{H_i\}$ are called *correlated*.

Definition 3.2.5. *Let H_i, $1 \leq i \leq m$ be Hilbert spaces, and $\varrho_i \in D(H_i)$.*

1. *The state $\varrho_1 \otimes \varrho_2 \otimes .... \otimes \varrho_m$ is called a* product state *of the composite system $H_1 \otimes H_2 \otimes ... \otimes H_m$.*

2. *A separable state is a convex combination of product states of $H_1 \otimes H_2 \otimes ... \otimes H_m$.*

3. *A non-separable state is called an entangled state. A composite system that has an entangled state is called an entangled system.*

Definition 3.2.6. *A bipartite quantum system is a composite system that consists of two quantum systems. A state on bipartite system is called a bipartite state. If ϱ is a state of $H_1 \otimes H_2$, then $\varrho^{H_1} = Tr_{H_2}(\varrho)$ and $\varrho^{H_2} = Tr_{H_1}(\varrho)$ are states of the subsystems H_1 and H_2 respectively. The states ϱ^{H_1} and ϱ^{H_2} are called the reduced density operators of ϱ.*

Example 3.2.7.

The state $\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = ww^*$ where $w = \frac{1}{\sqrt{2}}(e_1 \otimes e_1 + e_2 \otimes e_2)$ is an example of a pure entangled state on the composite system $\mathbb{C}^2 \otimes \mathbb{C}^2$. This is called a Bell state.

Definition 3.2.8. *Let* (H, π_H) *be a representation of a group* G. *A* G*-equivariant state of* H *is a state of* H *which is a* G*-equivariant map.*

If $D(H)^G$ denotes the G-equivariant states of H, then

$$D(H)^G = End(H)^G \cap D(H)$$

Example 3.2.9. [40] Let H be Hilbert space of dimension n. Let $G = \{U \otimes U : U \in U(n)\}$ where $U(n)$ is the set of all unitary operators on H. A *Werner state* is an $n \times n$-dimensional bipartite quantum state that is G-equivariant.

3.2.2 Quantum channels, definition and examples

Sending information from one quantum system to another requires transformations of the states. In quantum mechanics, a *quantum channel* (*a channel*) is defined to be any method that is used to transfer states between two quantum systems. A mathematical definition of the quantum channel is the following:

Definition 3.2.10. *Let* H *and* K *be Hilbert spaces. A* quantum channel $\Phi : End(H) \longrightarrow End(K)$ *is a linear completely positive trace-preserving map.*

We denote the set of all quantum channels from $End(H)$ to $End(K)$ by $QC(H, K)$. The requirement that Φ is completely positive is justified in the introduction of [19].

Examples 3.2.11. Let H be a Hilbert space.

1. For a unitary operator U on H, the map $\Phi : End(H) \longrightarrow End(H)$ defined by $\Phi(A) = UAU^*$ for any $A \in End(H)$ is a quantum channel. Such a channel is called a *unitary conjugation channel* or briefly a *unitary channel*. A convex combination of unitary channels on H is called a *random unitary channel*. It is in the form $\Phi(A) = \sum_{i=1}^{d} p_i U_i A U_i^*$ where $\{p_i : 1 \leq i \leq d\}$ is a probability distribution, and U_i is a unitary operator on H for each i. The identity map on $End(H)$ is a special case of the unitary channel.

2. A *depolarizing channel* is defined for $0 \leq \lambda \leq 1$ by

$$\Phi_\lambda : End(H) \longrightarrow End(H)$$

$$A \longmapsto \lambda \frac{tr(A)}{d_H} I_H + (1-\lambda)A$$

where d_H is the dimension of H, and I_H is the identity map on H.

   - For $\lambda = 1$, the map Φ_λ is called *the completely depolarizing channel*.
   - If K is a Hilbert space, *the generalized completely depolarizing channel* is the linear map $\Phi : End(H) \longrightarrow End(K)$ defined by $\Phi(A) = \frac{tr(A)}{d_K} I_K$ for any $A \in End(H)$, where I_K is the identity matrix on K, and d_k is the dimension of the space K.

3. For $\frac{-1}{d_H - 1} \leq \lambda \leq \frac{1}{d_H + 1}$, let

$$\Phi_\lambda : End(H) \rightarrow End(H)$$

$$\Phi_\lambda(A) = \lambda \frac{tr(A)}{d_H} I_H + (1-\lambda)A^t$$

where A^t denotes the transpose matrix of A. The map Φ_λ is a quantum channel. This channel is called the transpose depolarizing channel.

4. The partial trace, in Definition 1.2.20, is a quantum channel.

We refer the reader to [12, p.123-129], for the proofs that the examples given above are channels. The following proposition is straightforward.

Proposition 3.2.12. *The tensor product of quantum channels, the composition of composable quantum channels, and convex linear combinations of quantum channels are quantum channels.*

Proposition 3.2.13. *Let H and K be Hilbert spaces. For any $\alpha \in End(H,K)$, the map Ad_α is a linear completely positive map; it is a channel if and only if α is an isometry.*

Proof:

For $A \in End(H)$ such that $A \geq 0$, there exist $B \in End(H)$ such that $A = BB^*$. As

$$Ad_\alpha(A) = \alpha A \alpha^* = \alpha B B^* \alpha^* = \alpha B \left(\alpha B\right)^* \geq 0$$

the map Ad_α is positive. Let $n \in \mathbb{N}$, as $End(H) \otimes \mathbb{M}_n\left(\mathbb{C}\right) \simeq End(H \otimes \mathbb{C}^n)$, and

$$Ad_\alpha \otimes I_n = Ad_{(\alpha \otimes I_n)}$$

it follows that $Ad_\alpha \otimes I_n$ is positive. If α is an isometry, then

$$tr(Ad_\alpha(A)) = tr(\alpha A \alpha^*) = tr(A)$$

so Ad_α is trace preserving. ∎

Definition 3.2.14. *[12, p.125].(Unital channel) Let H and K be Hilbert spaces. A quantum channel $\Phi : End(H) \longrightarrow End(K)$ is said to be unital if*

$$\Phi(\tfrac{1}{d_H} I_H) = \tfrac{1}{d_K} I_K$$

Example 3.2.15. The random unitary channel, and the depolarizing channel are unital channels.

3.2.3 Characterization of quantum channels

In this section, we give many equivalent representations of the quantum channel.

Definition 3.2.16. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel. A Stinespring representation (dilation) of Φ is a pair (E, α) consisting of a Hilbert space E (an environment space), and an isometry $\alpha : H \longrightarrow K \otimes E$ such that $\Phi(A) = Tr_E(\alpha A \alpha^*)$ for any $A \in End(H)$. The map Tr_E denotes the partial trace over E.*

Remark 3.2.17. In operator algebra, a Stinespring representation exists for any completely positive map, see [28, p.43]. In the case of quantum channels, the partial trace appears as a consequence of being a trace-preserving map. The author in [16, p.107-109] explains the link between the two representations in both operator algebra and quantum information theory.

Definition 3.2.18. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a completely positive map. A Kraus representation of Φ is a set of operators*

$$\{T_j : 1 \leq j \leq k\} \subset End(H, K)$$

that satisfies

$$\Phi(A) = \sum_{j=1}^{k} T_j A T_j^*$$

The operators $\{T_j : 1 \leq j \leq k\}$ are called Kraus operators. If Φ is a quantum channel, then a Kraus representation $\{T_j : 1 \leq j \leq k\}$ of Φ is required to satisfy the additional condition

$$\sum_{j=1}^{k} T_j^* T_j = I_H.$$

The next proposition gives relationships among the different representations of a quantum channel and its Choi matrix.

Proposition 3.2.19. *Let H and K be Hilbert spaces, and let $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel.*

1. *If (E, α) is a Stinespring representation of Φ, and $\{e_j : 1 \leq j \leq d_E\}$ is an orthonormal basis for E, then the maps $\{T_j : H \longrightarrow K, 1 \leq j \leq d_E\}$ defined by*

$$T_j = (I_K \otimes e_j^*)\alpha$$

yield a Kraus representation of Φ.

2. *If $\{T_j : 1 \leq j \leq k\}$ is a family of Kraus operators of Φ, then*

   (a) *The space $E = \mathbb{C}^k$, and the map $\alpha = \sum_{j=1}^{k} T_j \otimes e_j$, where $\{e_j : 1 \leq j \leq k\}$ is an orthonormal basis element for $\mathbb{C}^k$, form a Stinespring representation of Φ.*

   (b) *The Choi matrix of Φ is given by $C(\Phi) = \sum_{j=1}^{k} \mathrm{Vec}(T_j)\mathrm{Vec}(T_j)^*$.*

Proof:

Let $T_j = (I_K \otimes e_j^*)\alpha$, and $A \in End(H)$. Since $\sum_{j=1}^{d_E}(I_K \otimes e_j^*)B(I_K \otimes e_j) = (I_K \otimes tr)(B)$ for any $B \in End(K \otimes E)$, then

$$\begin{aligned}\sum_{j=1}^{d_E} T_j A T_j^* &= \sum_{j=1}^{d_E}(I_K \otimes e_j^*)\alpha A \alpha^*(I_K \otimes e_j) \\ &= (I_K \otimes tr)(\alpha A \alpha^*) = Tr_E(\alpha A \alpha^*) = \Phi(A)\end{aligned}$$

and

$$\begin{aligned}\sum_{j=1}^{d_E} T_j^* T_j &= \sum_{j=1}^{d_E} \alpha^*(I_K^* \otimes e_j)(I_K \otimes e_j^*)\alpha \\ &= \alpha^*(I_K \otimes \sum_{j=1}^{d_E} e_j e_j^*)\alpha = \alpha^*(I_K \otimes I_E)\alpha = I_H.\end{aligned}$$

For the proof of the second statement, see [41, p.51-p.54]. ∎

The following theorem summarizes the results in [41, p.51-54].

Theorem 3.2.20. Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a linear map. The following are equivalent:

1. Φ is a quantum channel.

2. The Choi matrix $C(\Phi)$ is a positive element in $End(K \otimes \overline{H})$ that satisfies $Tr_K(C(\Phi)) = I_{\overline{H}}$.

3. Φ has a Stinespring representation (E, α).

4. Φ has a Stinespring representation (E, α) such that $dim(E) = rank(C(\Phi))$.

5. Φ has a Kraus representation.

6. Φ has a Kraus representation $\{T_1, T_2, ...T_k\}$ of Φ where $k = rank(C(\Phi))$.

As a corollary to the equivalence between (1) and (2) in the theorem above, we have:

Corollary 3.2.21. *Let H and K be Hilbert spaces. The set of all quantum channel $\Phi : End(H) \longrightarrow End(K)$ can be identified with a proper subset of all the states of $K \otimes \overline{H}$. Namely, the set $\{\varrho \in D(K \otimes \overline{H}) : Tr_K(\varrho) = \frac{1}{d_H} I_{\overline{H}}\}$. This identification is given by $\frac{1}{d_H}C$, where C is the Choi-Jamiolkowski map.*

Remark 3.2.22. For any quantum channel a Stinespring representation is never unique. In [15], Holevo shows that if (E, α) and (E', α') are two Stinespring representations of $\Phi : End(H) \longrightarrow End(K)$, then there exists a partial isometry $J : E \longrightarrow E'$ such that $\alpha' = (I_K \otimes J)\alpha$ and $\alpha = (I_K \otimes J^*)\alpha'$. Stinespring representations with minimal dimensionality of the space E are called *minimal dilations*. The next corollary shows that the Stinespring representation with an environment space satisfies $dim(E) = rank(C(\Phi))$ is a minimal dilation.

By Proposition 3.2.19, and Theorem 3.2.20, we have:

Corollary 3.2.23. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel. The rank of the Choi matrix of Φ gives an achievable lower bound for both the number of any Kraus operators of Φ, and of the dimension of any environment space.*

Proof:

Let $\{T_1, T_2, ...T_k\}$ be Kraus operators of Φ. By Proposition 3.2.19, we have:

$$rank(C(\Phi)) = rank\left(\sum_{j=1}^{k} vec(T_j)vec(T_j)^*\right) \leq \sum_{j=1}^{k} rank\left(vec(T_j)vec(T_j)^*\right) = k$$

By Theorem 3.2.20 (6), this bound is achievable. Let (α, E) be a Stinespring representation of Φ. By Proposition 3.2.19 (1), there exist a set of Kraus operators which has d_E elements. Thus, $rank(C(\Phi)) \leq d_E$. By Theorem 3.2.20 (4), this bound is achievable. ∎

3.3 G-covariant quantum channels

In this section, we restrict our study to a class of quantum channels that are also G-equivariant maps with respect to a given group G.

Definition 3.3.1. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G. A quantum channel $\Phi : End(H) \longrightarrow End(K)$ is G-covariant if*

$$\Phi(\pi_{H(g)} A \pi^*_{H(g)}) = \pi_{K(g)} \Phi(A) \pi^*_{K(g)}$$

for each $A \in End(H)$ and $g \in G$. If both π_H and π_K are irreducible representations, then Φ is called G-irreducibly covariant.

We denote the set of all G-covariant channels from $End(H)$ to $End(K)$ by $QC(H, K)^G$.

Examples 3.3.2. Let (H, π_H) and (K, π_K) be two unitary representations of a group G.

1. The partial trace over H (Definition 1.2.20), is an example of a G-covariant channel from $End(H \otimes K)$ to $End(K)$. It is a quantum channel [12, p.124], with a Stinespring representation $(H, I_{H\otimes K})$, and Kraus operators $\{T_j = I_K \otimes e_j^* : 1 \leq j \leq d_H\}$, where $\{e_j : 1 \leq j \leq d_H\}$ is an orthonormal basis for H. By Lemma 1.2.21, it is a G-equivariant map.

2. The map $\Phi : End(H \otimes K) \longrightarrow End(K \otimes H)$ defined by $\Phi(A) = flip_K^H A\, (flip_K^H)^*$ is a unitary conjugation, G-covariant quantum channel. Recall that by Lemma 1.2.23, the map $flip_K^H$ is a G-equivariant map.

3. The generalized completely depolarizing channel (defined in Example 3.2.11) is a G-covariant channel.

Proposition 3.3.3. *Let G be a group. The tensor product of G-covariant channels, and the composition of G-covariant channels are again G-covariant channels.*

By the convexity of both the set of quantum channels [41, p.49], and the space of G-equivariant maps, we have :

Proposition 3.3.4. *Let (H, π_H) and (K, π_K) be two representations of a group G. The set $QC(H, K)^G$ of G-covariant channels is a convex set.*

As by Example 3.3.2, and Proposition 1.2.7, the partial trace, and the conjugation map are G-equivariant, the proof of the following proposition is straightforward.

Proposition 3.3.5. *Let (H, π_H), (K, π_K), and (E, π_E) be representations of a group G. Let $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel given by a Stinespring representation (E, α). If $\alpha : H \longrightarrow K \otimes E$ is G-equivariant, then Φ is G-covariant.*

Recall that if H and K are vector spaces, and W is subspace of H, then the restriction of a linear map $\Phi : End(H) \longrightarrow End(K)$ on $End(W)$, denoted by $\Phi\,|W$, is the map $\Phi \circ Ad_{\iota_W} : End(W) \longrightarrow End(K)$, where ι_W is the inclusion map of W in H.

Proposition 3.3.6. *Let (H, π_H) and (K, π_K) be representations of a group G. Let W be a G-invariant subspace of H, and $\Phi : End(H) \longrightarrow End(K)$ be G-covariant channel. The restriction of Φ on $End(W)$ is a G-covariant channel.*

Proof:

Let ι_W be the inclusion map of W. By Lemma 1.2.10, and Proposition 1.2.7 (3), the map $Ad_{\iota_W} : End(W) \longrightarrow End(H)$ is G-equivariant. By Proposition 3.2.13, it is a channel. As the composition of two G-covariant channels is G-covariant, the result follows. ∎

Remark 3.3.7. If (E, α) is a Stinespring representation of Φ, then $(E, \alpha \circ \iota_W)$ is a Stinespring representation of $\Phi\,|W$. Hence, the proof of the proposition above can be done using Proposition 3.3.5.

Proposition 3.3.8. *Let (H, π_H) be a representation of a group G such that $H = \bigoplus_{i=1}^{m} W_i$, where W_i are G-invariant subspaces of H. Let $\{q_i : 1 \leq i \leq m\}$ be the orthogonal projections of H on W_i. The map*

$$\Phi : End(H) \longrightarrow \bigoplus_{i=1}^{m} End(W_i)$$

$$A \longmapsto \sum_{i=1}^{m} q_i A q_i^*$$

is a unital G-covariant channel.

Proof:

By Lemma 1.2.10, $\{q_i : 1 \leq i \leq m\}$ is a set of G-equivariant maps, so by Proposition 1.2.7 and Proposition 3.2.13, the conjugation map

$$Ad_{q_i} : End(H) \longrightarrow End(W_i)$$

$$A \longmapsto q_i A q_i^*$$

is a G-equivariant completely positive map; thus so is Φ. As $(q_i^* q_i)_{i=1}^m$ is a partition of I_H, and $(q_i q_i^*)_{i=1}^m$ is a partition of $I_{\bigoplus_{i=1}^m W_i}$, the map Φ is trace-preserving and unital. ∎

The next proposition is taken from [7, p.6]; we provide a proof for completeness.

Proposition 3.3.9. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G, and $\Phi : End(H) \longrightarrow End(K)$ be a linear map. Then*

1. *Φ is a G-covariant channel if and only if*
$$\frac{1}{d_H} C(\Phi) \in End(K \otimes \overline{H})^G \cap \left\{ \varrho \in D(K \otimes \overline{H}) : Tr_K(\varrho) = \frac{1}{d_H} I_{\overline{H}} \right\}$$
2. *If π_H is irreducible, then Φ is a G-covariant channel if and only if*
$$\frac{1}{d_H} C(\Phi) \in D(K \otimes \overline{H})^G.$$

Proof:

By Corollary 1.2.29, the map $\frac{1}{d_H} C$ is a bijective map. Hence

$$\tfrac{1}{d_H} C\left(A \cap B\right) = \tfrac{1}{d_H}\left(C\left(A\right) \cap C\left(B\right)\right)$$

for any $A, B \subseteq End(End(H), End(K))$. The first statement follows from this, Proposition 1.2.32, and Corollary 3.2.21. For the second statement, assume π_H is an irreducible representation of G. By (1), it is enough to show that

$$End(K \otimes \overline{H})^G \cap \left\{ \varrho \in D(K \otimes \overline{H}) : Tr_K(\varrho) = \tfrac{1}{d_H} I_{\overline{H}} \right\} = D(K \otimes \overline{H})^G$$

Since

$$End(K \otimes \overline{H})^G \cap \left\{ \varrho \in D(K \otimes \overline{H}) : Tr_K(\varrho) = \tfrac{1}{d_H} I_{\overline{H}} \right\} \subseteq D(K \otimes \overline{H})^G$$

always holds, then we only have to prove the other inclusion.
Let $\varrho \in D(K \otimes \overline{H})^G$. For $g \in G$, we have

$$\varrho = \left(\pi_{K(g)} \otimes \check{\pi}_{H(g)}\right) \varrho \left(\pi_{K(g)} \otimes \check{\pi}_{H(g)}\right)^*$$

As the partial trace is G-equivariant, we get

$$Tr_K(\varrho) = Tr_K\left(\left(\pi_{K(g)} \otimes \check{\pi}_{H(g)}\right) \varrho \left(\pi_{K(g)} \otimes \check{\pi}_{H(g)}\right)^*\right) = \check{\pi}_{H(g)}\, Tr_K\left(\varrho\right) \check{\pi}_{H(g)}{}^*$$

So, $Tr_K(\varrho)$ is intertwining the irreducible representation $\check{\pi}_H$. By Schur's Lemma 1.2.12, $Tr_K \varrho = \lambda I_H$ for some scalar λ. Taking the trace of both sides, we have $\lambda = \frac{1}{d_H}$. Thus

$$\varrho \in End(K \otimes \overline{H})^G \cap \left\{ \varrho \in D(K \otimes \overline{H}) : Tr_K(\varrho) = \tfrac{1}{d_H} I_{\overline{H}} \right\}$$

∎

Lemma 3.3.10. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G, and $\Phi : End(H) \longrightarrow End(K)$ be a G-covariant channel. If $\{T_j : 1 \leq j \leq n\}$ are Kraus operators of Φ, then for each $g \in G$, $\{\pi_{K(g)} T_j \pi_{H(g)}{}^* : 1 \leq j \leq n\}$ are Kraus operators of Φ.*

Proof:

Let $g \in G$. As π_H and π_K are unitary representations, then

$$\sum_{j=1}^{n} \left(\pi_{K(g)} T_j \pi_{H(g)}{}^*\right)^* \pi_{K(g)} T_j \pi_{H(g)}{}^* = \pi_{H(g)} \left(\sum_{j=1}^{n} T_j^* T_j\right) \pi_{H(g)}{}^* = I_H$$

For $A \in End(H)$, we have

$$\sum_{j=1}^{n} \pi_{K(g)} T_j \pi_{H(g)}{}^* A \left(\pi_{K(g)} T_j \pi_{H(g)}{}^*\right)^* = \sum_{j=1}^{n} \pi_{K(g)} T_j \pi_{H(g)}{}^* A \pi_{H(g)} T_j^* \pi_{K(g)}{}^*$$

$$= \pi_{K(g)} \left(\sum_{j=1}^{n} T_j \pi_{H(g)}{}^* A \pi_{H(g)} T_j^* \right) \pi_{K(g)}{}^*$$
$$= \pi_{K(g)} \Phi(\pi_{H(g)}{}^* A \pi_{H(g)}) \pi_{K(g)}{}^*$$
$$= \pi_{K(g)} \pi_{K(g)}{}^* \Phi(A) \pi_{K(g)} \pi_{K(g)}{}^* = \Phi(A)$$

the result follows by Definition 3.2.18. ∎

Chapter 4

EPOSIC Channels

The present chapter introduces EPOSIC channels, examples of $SU(2)$-covariant channels. We define these channels in the first section using Stinespring representation, and study them in the rest of this chapter. In Section 4.2, we obtain Kraus representation of the EPOSIC channel, and compute its Choi matrix in Section 4.3. In the next two sections, we compute a complementary channel, and the dual map of the EPOSIC channel. We end this chapter with an application to operator algebra by getting an example of a positive map that is not completely positive.

The main results of this chapter:

- Constructing EPOSIC channels (Proposition 4.1.1).
- Obtaining a Kraus representation, and the Choi matrix of the EPOSIC channel (Definition 4.2.1, and Proposition 4.3.5).
- Computing a complementary channel, and the dual map of the EPOSIC channel (Proposition 4.4.4, and Proposition 4.5.6).

- Obtaining an example of a positive, non-completely positive map (Proposition 4.6.3, and Proposition 4.6.5).

4.1 EPOSIC channels

Recall the $SU(2)$-equivariant isometry $\alpha_{m,n,h} : P_{m+n-2h} \longrightarrow P_m \otimes P_n$ that was given in Proposition 2.3.5. According to Definition 3.2.16, and Proposition 3.3.5, this isometry induces an $SU(2)$-covariant quantum channel $\Phi_{m,n,h} : End(P_{m+n-2h}) \longrightarrow End(P_m)$, that has a Stinespring representation $(P_n, \alpha_{m,n,h})$.

Proposition 4.1.1. *For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, let $r = m + n - 2h$ and $\alpha_{m,n,h}$ be as in Definition 2.3.2. The map $\Phi_{m,n,h} : End(P_r) \longrightarrow End(P_m)$ defined for $A \in End(P_r)$ by*

$$\Phi_{m,n,h}(A) = Tr_{P_n}(\alpha_{m,n,h} A \alpha^*_{m,n,h})$$

is an $SU(2)$-irreducibly covariant channel.

Definition 4.1.2. *Let $r, m \in \mathbb{N}$, and*

$$\mathcal{E}(r, m) = \{(n, h) \in \mathbb{N}^2 : r = m + n - 2h,\ 0 \leq h \leq \min\{m, n\}\}$$

For $(n, h) \in \mathcal{E}(r, m)$, we call the quantum channel $\Phi_{m,n,h} : End(P_r) \longrightarrow End(P_m)$, defined in Proposition 4.1.1, an EPOSIC channel.

For $r, m \in \mathbb{N}$, we denote by $EC(r, m)$ the set of all EPOSIC channels from $End(P_r)$ into $End(P_m)$, and abbreviate $EC(m, m)$ to $EC(m)$. As we show in Section 5.1, the set $EC(r, m)$ constitutes the set of extreme points of all $SU(2)$-irreducibly covariant channels from $End(P_r)$ into $End(P_m)$, justifying the nomenclature EPOSIC.

Lemma 4.1.3. *Let $r, m \in \mathbb{N}$. Then*

$$\mathcal{E}(r, m) = \{(r + m - 2l, m - l) \in \mathbb{N}^2 :\ 0 \leq l \leq \min\{r, m\}\}$$

Proof:

Let $\mathcal{B} = \{(r+m-2l, m-l) \in \mathbb{N}^2 : 0 \leq l \leq \min\{r,m\}\}$. Suppose that $(r+m-2l, m-l) \in \mathcal{B}$ for some $0 \leq l \leq \min\{r,m\}$. Set $n_0 = r+m-2l$ and $h_0 = m-l$. The pair (n_0, h_0) satisfies $r = n_0 + m - 2h_0$ and $0 \leq h_0 \leq \min\{m, n_0\}$ (note that $h_0 \leq h_0 + (r-l) = m-l+r-l = m+r-2l = n_0$). According to Definition 4.1.2, $(r+m-2l, m-l) = (n_0, h_0) \in \mathcal{E}(r,m)$.
Conversely, assume $(n,h) \in \mathcal{E}(r,m)$. Set $l_0 = m-h$, then $0 \leq l_0 \leq m$, $n = r-m+2h = r+m-2l_0$, and $l_0 \leq l_0 + (n-h) = (m-h)+(n-h) = m+n-2h = r$. Hence, $0 \leq l_0 \leq \min\{r,m\}$, and $(n,h) = (r+m-2l_0, m-l_0) \in \mathcal{B}$. ∎

Consequently, we have:

Proposition 4.1.4. *Let $r, m \in \mathbb{N}$. The set of all EPOSIC channels from $End(P_r)$ to $End(P_m)$ is*

$$EC(r,m) = \{\Phi_{m,r+m-2l,m-l} : 0 \leq l \leq \min\{r,m\}\}$$

Remark 4.1.5. In [14, p.42], using Schur's Lemma, it is shown that any G-irreducibly covariant channel is unital, see Definition 3.2.14. It follows that the EPOSIC channels are unital.

4.2 Kraus representations of EPOSIC channels

In this section, we obtain a Kraus representation for the EPOSIC channel $\Phi_{m,n,h}$. We exhibit some of their properties, and show that the obtained Kraus operators has a symmetric relation.

Definition 4.2.1. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m,n\}$, and $\alpha_{m,n,h}$ be the isometry given in Definition 2.3.2. For $0 \leq j \leq n$, let $T_j : P_{m+n-2h} \longrightarrow P_m$ be the* *map defined by*

$$T_j = (I_{P_m} \otimes f_j^{n^*})\alpha_{m,n,h}$$

where $\{f_j^n : 0 \leq j \leq n\}$ *denotes the standard basis for* P_n.

In the definition above, we identify the two spaces $P_m \otimes \mathbb{C}$ and P_m through the unitary map $u \otimes \lambda \longmapsto \lambda u$. By Proposition 3.2.19, the set $\{T_j : 0 \leq j \leq n\}$ is a Kraus representation of $\Phi_{m,n,h}$. We call these Kraus operators, the EPOSIC Kraus operators.

By direct computations using Corollary 2.3.13 and the definition above, one can obtain the matrix coefficients of the EPOSIC Kraus operator as follows.

Proposition 4.2.2. *Let* $m, n, h \in \mathbb{N}$ *with* $0 \leq h \leq \min\{m, n\}$, *and* $r = m+n-2h$. *If* $\{T_j : 0 \leq j \leq n\}$ *are the EPOSIC Kraus operators of* $\Phi_{m,n,h}$, *then for each* $0 \leq j \leq n$,

$$T_j(f_i^r) = \begin{cases} \varepsilon_i^j f_{l_{ij}}^m & if \quad j \in B(i) \\ 0 & otherwise \end{cases}$$

where ε_i^j and $B(i)$ are given in Notation 2.3.10, and $\{f_s^k : 0 \leq s \leq k\}$ *is the standard basis for* P_k for $k \in \{m, r\}$.

Remarks 4.2.3. With the notation of 2.3.10, we have

$$j \in B(i) \iff \max\{0, j-h\} \leq i \leq \min\{r, m-h+j\}$$

$$\iff \max\{0, h-j\} \leq l_{ij} \leq \min\{r-j+h, m\}$$

Hence,

1. According to the definition of T_j above, we have

$$rank(T_j) = dim(Col(T_j)) \leq |\{i : j \in B(i)\}| = \min\{m,\, m+j-h,\, r,\, r-j+h\}$$

2. The Kraus operator T_j can be written as

$$T_j = \sum_{i=\max\{0,j-h\}}^{\min\{r,m+j-h\}} \varepsilon_i^j \, f_{l_{ij}}^m f_i^{r^*}$$

3. The Kraus operator T_j can also be written as

$$T_j = \sum_{l=\max\{0,h-j\}}^{\min\{r-j+h,m\}} \varepsilon_{l+j-h}^j \, f_l^m f_{l+j-h}^{r^*}$$

4. The adjoint map of T_j is given by

$$T_j^* = \sum_{l=\max\{0,h-j\}}^{\min\{r-j+h,m\}} \varepsilon_{l+j-h}^j f_{l+j-h}^r f_l^{m*}$$

5. Every T_j has a vector representation in $P_m \otimes \overline{P}_r$ given by

$$Vec(T_j) = \sum_{i=\max\{0,j-h\}}^{\min\{r,m-h+j\}} \varepsilon_i^j \, f_{l_{ij}}^m \otimes f_i^r$$

   Equivalently,

$$Vec(T_j) = \sum_{l=\max\{0,h-j\}}^{\min\{r-j+h,m\}} \varepsilon_{l+j-h}^j \, f_l^m \otimes f_{l+j-h}^r$$

The next proposition follows directly from Corollary 1.2.19.

Proposition 4.2.4. *Let $m, n, h \in \mathbb{N}$ with $0 \le h \le \min\{m, n\}$, and $r = m + n - 2h$. If $\{T_j : 0 \le j \le n\}$ are the EPOSIC Kraus operators of $\Phi_{m,n,h}$, then*

$$\langle T_{j_1} | T_{j_2} \rangle_{End(H,K)} = \tfrac{r+1}{n+1} \delta_{j_1 j_2}$$

for each $0 \le j_1, j_2 \le n$.

Recall by Remark 2.1.4 (1) that for $g_0 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in SU(2)$, we have

$$\rho_m(g_0)\left(f_l^m\right) = (-1)^{\,l} f_{m-l}^m$$

Proposition 4.2.5. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, $r = m + n - 2h$, and $\{T_j : 0 \leq j \leq n\}$ be the EPOSIC Kraus operators of $\Phi_{m,n,h}$. For each $0 \leq j \leq n$, we have*

$$\rho_m(g_0) T_j \rho_r^*(g_0) = (-1)^j \, T_{n-j}$$

Proof:

Fix $j \in \mathbb{N}$, such that $0 \leq j \leq n$. For each $0 \leq i \leq r$, we have one of the following cases:

- If $j \in B(i)$, since $m - l_{ij} = l_{(r-i)(n-j)}$ then by Corollary 2.3.15 (1), we have:

$$\begin{aligned} \rho_m(g_0) T_j(f_i^r) &= (-1)^{l_{ij}} \, \varepsilon_i^j f_{m-l_{ij}}^m = (-1)^{l_{ij}+h} \, \varepsilon_{r-i}^{n-j} f_{l_{(r-i)(n-j)}}^m \\ &= (-1)^{l_{ij}+h} \, T_{n-j}(f_{r-i}^r) = (-1)^j T_{n-j} \rho_r(g_0)(f_i^r) \end{aligned}$$

- If $j \notin B(i)$, then $n - j \notin n - B(i) = B(r - i)$. So, both $T_j(f_i^r)$ and $T_{n-j}(f_{r-i}^r)$ are zero. This implies that the identity also holds in this case.

∎

It is worth noticing that even though Φ is a G-covariant channel, Kraus operators of Φ are not necessarily G-equivariant. The relation in Proposition 4.2.5 can be translated into a symmetric relation among the vectors representing the operators T_j and T_{n-j} in $P_m \otimes \overline{P}_r$. Recall that by Lemma 1.2.25, the map Vec is $SU(2)$-equivariant; thus applying the map Vec on both side of the equation in Proposition 4.2.5, we have:

$$\text{Vec}(T_{n-j}) = (-1)^j \left(\rho_m(g_0) \otimes \check{\rho}_r(g_0) \right) \text{Vec}(T_j) \tag{4.2.1}$$

Proposition 4.2.6. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, and $r = m + n - 2h$. The EPOSIC Kraus operators $\{T_j : 0 \leq j \leq n\}$, and the maps J_m,J_r (Definition 2.1.5) satisfy*

$$flip_{P_r}^{\overline{P}_m} \left(J_m \otimes J_r^* \right) \left(Vec(T_{n-j}) \right) = (-1)^{m+j} Vec(T_j^*)$$

for each $0 \leq j \leq n$.

Proof:

By Equation 4.2.1, we have

$$\mathrm{Vec}(T_{n-j}) = (-1)^j \left(\rho_m(g_0) \otimes \check{\rho}_r(g_0)\right) \mathrm{Vec}(T_j)$$

Thus,

$$flip_{P_r}^{\overline{P}_m} \left(J_m \otimes J_r^*\right) \left(Vec(T_{n-j})\right) = flip_{P_r}^{\overline{P}_m} \left(J_m \otimes J_r^*\right) \left((-1)^j \left(\rho_m(g_0) \otimes \check{\rho}_r(g_0)\right) \mathrm{Vec}(T_j)\right)$$

$$= (-1)^j flip_{P_r}^{\overline{P}_m} \left(J_m \otimes J_r^*\right) \left(\rho_m(g_0) \otimes \check{\rho}_r(g_0)\right) \left(\sum_{l=\max\{0,h-j\}}^{\min\{r-j+h,m\}} \varepsilon_{l+j-h}^j f_l^m \otimes f_{l+j-h}^r\right)$$

$$= (-1)^j \sum_{l=\max\{0,h-j\}}^{\min\{r-j+h,m\}} (-1)^{j-h} \varepsilon_{l+j-h}^j flip_{P_r}^{\overline{P}_m} \left(\left(J_m \otimes J_r^*\right) \left(f_{m-l}^m \otimes f_{r-(l+j-h)}^r\right)\right)$$

$$= (-1)^j \sum_{l=\max\{0,h-j\}}^{\min\{r-j+h,m\}} (-1)^m \varepsilon_{l+j-h}^j flip_{P_r}^{\overline{P}_m} \left(\left(f_l^m \otimes f_{l+j-h}^r\right)\right)$$

$$= (-1)^{j+m} \sum_{l=\max\{0,h-j\}}^{\min\{r-j+h,m\}} \varepsilon_{l+j-h}^j \left(f_{l+j-h}^r \otimes f_l^m\right) = (-1)^{m+j} Vec(T_j^*).$$

∎

The following corollary to Proposition 4.2.2 gives the matrix coefficients of the EPOSIC channel $\Phi_{m,n,h}$, with respect to the standard basis of P_{m+n-2h}.

Corollary 4.2.7. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, let $r = m + n - 2h$. For $0 \leq i_1, i_2 \leq r$,*

$$\Phi_{m,n,h}(f_{i_1}^r f_{i_2}^{r^*}) = \sum_{j \in B(i_1) \cap B(i_2)} \varepsilon_{i_1}^j \varepsilon_{i_2}^j f_{l_{i_1} j}^m f_{l_{i_2} j}^{m^*}$$

For $m \in \mathbb{N}$, and $0 \leq i \leq m$, the set $B(i)$ associated to the map $\alpha_{m,0,0}$ is equal to $\{0\}$. It follows from this and Corollary 4.2.7, that the channel $\Phi_{m,0,0}$ is the identity map on $End(P_m)$. We also have:

Corollary 4.2.8. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, and $r = m + n - 2h$. If D_k denotes the set of all diagonal operators in $End(P_k)$, then*

$$\Phi_{m,n,h}(D_r) \subseteq D_m$$

Corollary 4.2.9. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, $r = m + n - 2h$, and $0 \leq i \leq r$. The sets of non-zero eigenvalues of $\Phi_{m,n,h}(f^r_{r-i} f^{r^*}_{r-i})$, $\Phi_{m,n,h}(f^r_i f^{r^*}_i)$, and of $\Phi_{n,m,h}(f^r_i f^{r^*}_i)$ coincide. They are all given by $\left\{(\varepsilon^j_i(m,n,h))^2 : j \in B(i)\right\}$.*

Proof:

By Corollary 4.2.7, the set $\{(\varepsilon^j_i(m,n,h))^2 : j \in B(i)\}$ contains all nonzero eigenvalues of $\Phi_{m,n,h}(f^r_i f^{r^*}_i)$. Let $g_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. As

$$\rho_r(g_0)\left(f^r_i\right) = (-1)^i f^r_{r-i}$$

the equivariance of the channel $\Phi_{m,n,h}$ gives

$$\Phi_{m,n,h}(f^r_{r-i} f^{r^*}_{r-i}) = \Phi_{m,n,h}(\rho_r(g_0) f^r_i f^{r^*}_i (\rho_r(g_0))^*) = \rho_m(g_0)\Phi_{m,n,h}(f^r_i f^{r^*}_i)(\rho_m(g_0))^*$$

So, $\Phi_{m,n,h}(f^r_{r-i} f^{r^*}_{r-i})$ and $\Phi_{m,n,h}(f^r_i f^{r^*}_i)$ are unitarily conjugate, and have the same eigenvalues. For the last one, let

- $B^{m,n,h}(i) = \{j : \max\{0, -m + i + h\} \leq j \leq \min\{i + h, n\}\}$, the set $B(i)$ associated with $\alpha_{m,n,h}$, and
- $B^{n,m,h}(i) = \{l : \max\{0, -n + i + h\} \leq l \leq \min\{i + h, m\}\}$, the set $B(i)$ associated with $\alpha_{n,m,h}$.

As $l \in B^{n,m,h}(i)$ if and only if $i - l + h \in B^{m,n,h}(i)$, we have

$$\begin{aligned}
\left\{(\varepsilon^l_i(n,m,h))^2 : l \in B^{n,m,h}(i)\right\} &= \left\{(\varepsilon^l_i(n,m,h))^2 : i-l+h \in B^{m,n,h}(i)\right\} \\
&= \left\{(\varepsilon^{i-j+h}_i(n,m,h))^2 : j \in B^{m,n,h}(i)\right\} \\
&= \left\{(\varepsilon^{l_{ij}}_i(n,m,h))^2 : j \in B^{m,n,h}(i)\right\}
\end{aligned}$$

Corollary 2.3.16 (2) finishes the proof. ∎

4.3 The Choi matrix of the EPOSIC channel

In this section, we show that the Choi matrix of $\Phi_{m,n,h}$ is a multiple of the projection of $P_m \otimes \overline{P}_r$ onto the $SU(2)$-subspace isomorphic to the environment space P_n. The following proposition is a special case of Proposition 1.2.17, where $H = P_m \otimes \overline{P}_r$.

Proposition 4.3.1. *Let ρ_m and ρ_r be the irreducible representations of $SU(2)$ in P_m and P_r respectively. Then $End(P_m \otimes \overline{P}_r)^{SU(2)}$ is an abelian algebra generated by the projections on the $SU(2)$-subspaces of $P_m \otimes \overline{P}_r$.*

Recall by Corollary 2.3.8, that the space $P_m \otimes \overline{P}_r$ decomposes into an orthogonal direct sum of $SU(2)$-irreducible subspaces V_{m+r-2l}, $0 \leq l \leq \min\{m,r\}$. For each $0 \leq l \leq \min\{m,r\}$, the map $\eta_{m,r,l} : P_{m+r-2l} \longrightarrow P_m \otimes \overline{P}_r$ is an isometry whose image is V_{m+r-2l}. The maps $q_{m,r,l} = \eta_{m,r,l}\eta^*_{m,r,l}$ where $0 \leq l \leq \min\{m,r\}$ are the mutually orthogonal projections onto the subspaces V_{m+r-2l}. These projections satisfy $\sum_{l=0}^{\min\{m,r\}} q_{m,r,l} = I_{P_m \otimes \overline{P}_r}$.

Since $\Phi_{m,n,h}$ is an $SU(2)$-covariant channel, by Proposition 4.3.1, and Proposition 1.2.32, we obtain:

Corollary 4.3.2. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m,n\}$, and $r = m+n-2h$. With the notation above, the Choi matrix of $\Phi_{m,n,h}$ is a linear combination of $\{q_{m,r,l} : 0 \leq l \leq \min\{m,r\}\}$.*

Remark 4.3.3. For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m,n\}$, we have:

$$P_m \otimes \overline{P}_{m+n-2h} \simeq \bigoplus_{l=0}^{\min\{m,m+n-2h\}} P_{n+2(m-h-l)}$$

$$= P_{n+2(m-h)} \oplus P_{n+2(m-h-1)} \oplus \ldots\ldots \oplus P_n \oplus \ldots. \oplus P_{n+2(m-h-\min\{m,m+n-2h\})}$$

It follows that if $r = m+n-2h$, then the set $\{q_{m,r,l} : 0 \leq l \leq \min\{m,r\}\}$ contains $q_{m,r,m-h} = \eta_{m,r,m-h}\eta^*_{m,r,m-h}$ which is the projection on a subspace isomorphic to P_n.

The following lemma will be used in the proof of Proposition 4.3.5.

Lemma 4.3.4. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, and $r = m + n - 2h$. The operator $C(\Phi_{m,n,h})\eta_{m,r,m-h}$ is nonzero.*

Proof:

Let $\{f_s^k : 0 \leq s \leq k\}$ be the standard basis for P_k where $k \in \{r, n, m\}$. It is enough to show that $C(\Phi_{m,n,h})\left(\eta_{m,r,m-h}(f_0^n)\right) \neq 0$. By Lemma 1.2.30 and Corollary 4.2.7, we have:

$$C(\Phi_{m,n,h}) = \sum_{i_1,i_2=0}^{r} \Phi_{m,n,h}(f_{i_1}^r f_{i_2}^{r^*}) \otimes f_{i_1}^r f_{i_2}^{r^*} = \sum_{i_1,i_2=0}^{r} \sum_{j \in B(i_1)\cap B(i_2)} \varepsilon_{i_1}^j \varepsilon_{i_2}^j f_{l_{i_1 j}}^m f_{l_{i_2 j}}^{m^*} \otimes f_{i_1}^r f_{i_2}^{r^*}.$$

By Lemma 2.3.7 and Corollary 2.3.13, we have:

$$\eta_{m,r,m-h}(f_0^n) = \left(I_{P_m} \otimes J_r\right) \alpha_{m,r,m-h}(f_0^n) = \left(I_{P_m} \otimes J_r\right) \left(\sum_{t \in B(0)} \varepsilon_{0(m,r,m-h)}^t f_{l_{0t}}^m \otimes f_t^r\right)$$

$$= \sum_{t \in B(0)} (-1)^t \varepsilon_{0(m,r,m-h)}^t f_{l_{0t}}^m \otimes f_{r-t}^r = \sum_{t \in B(0)} \lambda_t f_{m-(t+h)}^m \otimes f_{r-t}^r$$

where $\lambda_t > 0$ (Corollary 2.3.15 (4)).

Hence, we get:

$$C(\Phi_{m,n,h})\left(\eta_{m,r,m-h}(f_0^n)\right) = \sum_{i_1,i_2=0}^{r} \sum_{j \in B(i_1)\cap B(i_2)} \varepsilon_{i_1}^j \varepsilon_{i_2}^j f_{l_{i_1 j}}^m f_{l_{i_2 j}}^{m^*} \otimes f_{i_1}^r f_{i_2}^{r^*} \left(\sum_{t \in B(0)} \lambda_t f_{m-(t+h)}^m \otimes f_{r-t}^r\right)$$

$$= \sum_{i_1,i_2=0}^{r} \sum_{j \in B(i_1)\cap B(i_2)} \sum_{t \in B(0)} \lambda_t \varepsilon_{i_1}^j \varepsilon_{i_2}^j \left(f_{l_{i_1 j}}^m f_{l_{i_2 j}}^{m^*}\right) f_{m-(t+h)}^m \otimes \left(f_{i_1}^r f_{i_2}^{r^*}\right) f_{r-t}^r$$

But for $0 \leq i_1, i_2 \leq r$, $j \in B(i_1) \cap B(i_2)$ and $t \in B(0)$, we have:

$$f_{l_{i_1 j}}^m f_{l_{i_2 j}}^{m^*} f_{m-(t+h)}^m \otimes f_{i_1}^r f_{i_2}^{r^*} f_{r-t}^r = \begin{cases} f_{l_{i_1 n}}^m \otimes f_{i_1}^r & if \quad i_2 = r - t, j = n \\ \\ 0 & otherwise \end{cases}.$$

Since $n \in B(i_1)$ if and only if $n-h \leq i_1 \leq r$, we have

$$C(\Phi_{m,n,h})\,(\eta_{m,r,m-h}(f_0^n)) = \sum_{i_1=n-h}^{r} \sum_{t\in B(0)} \lambda_t \varepsilon_{i_1}^n \varepsilon_{r-t}^n f_{i_1-n+h}^m \otimes f_{i_1}^r$$

Assume that

$$0 = C(\Phi_{m,n,h})\,(\eta_{m,r,m-h}(f_0^n)) = \sum_{i_1=n-h}^{r} \sum_{t\in B(0)} \lambda_t \varepsilon_{i_1}^n \varepsilon_{r-t}^n\, f_{i_1-n+h}^m \otimes f_{i_1}^r$$

By the linear independence of $\{f_l^m \otimes f_i^r : 0 \leq l \leq m, 0 \leq i \leq r\}$, we would have

$$\sum_{t\in B(0)} \lambda_t \varepsilon_{i_1}^n \varepsilon_{r-t}^n = 0 \quad for \quad n-h \leq i_1 \leq r$$

Since by Corollary 2.3.15 (3),

$$\varepsilon_{i_1}^n \neq 0 \quad for \quad n-h \leq i_1 \leq r$$

we would have $\sum_{t\in B(0)} \lambda_t \varepsilon_{r-t}^n = 0$.

But by Corollary 2.3.15 (3), we have

$\varepsilon_{r-t}^n = {\scriptstyle (-1)^h}\theta_t$ with $\theta_t > 0$ for $t \in B(0) = \{t : 0 \leq t \leq m-h\}$.

Therefore,

$$\sum_{t\in B(0)} \lambda_t \varepsilon_{r-t}^n = {\scriptstyle (-1)^h} \sum_{t=0}^{m-h} \lambda_t \theta_t \neq 0$$

which is a contradiction. ∎

Proposition 4.3.5. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, and $r = m + n - 2h$. The Choi matrix of the EPOSIC channel $\Phi_{m,n,h}$ is given by*

$$C(\Phi_{m,n,h}) = \tfrac{r+1}{n+1} q_{m,r,m-h}$$

where $q_{m,r,m-h}$ is the projection of $P_m \otimes \overline{P}_r$ onto the $SU(2)$-subspace of dimension $n+1$.

Proof:

By Corollary 4.3.2, the Choi matrix

$$C(\Phi_{m,n,h}) = \sum_{l=0}^{\min\{m,r\}} \lambda_l q_{m,r,l}$$

where $\left\{q_{m,r,l} = \eta_{m,r,l}\eta^*_{m,r,l}, 0 \leq l \leq \min\{m,r\}\right\}$ are the mutually orthogonal projections onto $\{V_{m+r-2l}, 0 \leq l \leq \min\{m,r\}\}$. Consequently,

$$rank(C(\Phi_{m,n,h})) = \sum_{l=0,\lambda_l \neq 0}^{\min\{m,r\}} rank(q_{m,r,l})$$

By Lemma 4.3.4, we have $\lambda_{m-h} \neq 0$, hence

$$rank(C(\Phi_{m,n,h})) \geq rank(q_{m,r,m-h}) = dim(V_n) = n+1$$

Since by Corollary 3.2.23, $rank(C(\Phi_{m,n,h})) \leq n+1$,we have

$$C(\Phi_{m,n,h}) = \lambda_{m-h} q_{m,r,m-h}$$

Taking the trace of both sides of the equation, we get

$$r+1 = tr(C(\Phi_{m,n,h})) = \lambda_{m-h} tr(q_{m,r,m-h}) = \lambda_{m-h} n + 1$$

i.e. $\lambda_{m-h} = \frac{r+1}{n+1}$. ∎

Remark 4.3.6. The above proposition establishes a one-to-one correspondence between $EC(r, m)$, and the projections on the $SU(2)$-subspaces of $P_m \otimes \overline{P}_r$. This correspondence is given by

$$\Phi_{m,m+r-2l,m-l} \longleftrightarrow \frac{r+1}{m+r-2l+1} q_{m,r,l}$$

Consequently, we have:

Corollary 4.3.7. *For $r, m \in \mathbb{N}$, there are exactly $\min\{r, m\}+1$ elements in $EC(r, m)$.*

4.4 A channel complementary to the EPOSIC channel

Let us first recall the notion of complementary channels given in [15]. Given three Hilbert spaces H,K and E, and a linear isometry $\alpha : H \longrightarrow K \otimes E$, the maps

$$A \longmapsto Tr_E(\alpha A \alpha^*) \qquad \text{and} \qquad A \longmapsto Tr_K(\alpha A \alpha^*) \qquad \text{where } A \in End(H)$$

define two quantum channels

$$\Phi : End(H) \longrightarrow End(K), \text{ and } \Psi : End(H) \longrightarrow End(E)$$

The maps Φ and Ψ are called *mutually complementary.* By Theorem 3.2.20, to any quantum channel, one can associate a complementary channel. However, as the Stinespring representation (dilation) is not unique, there can be many candidates for "the" complementary channel. In [15], Holevo shows that if (E, α) and (E', α') are two Stinespring representations of $\Phi : End(H) \longrightarrow End(K)$, then there exists a partial isometry $J : E \longrightarrow E'$ such that $\alpha' = (I_K \otimes J)\alpha$ and $\alpha = (I_K \otimes J^*)\alpha'$. It follows that if Ψ_E and $\Psi_{E'}$ are complementary channels of Φ, then they are equivalent in the sense that there exist a partial isometry $J : E \longrightarrow E'$ such that $\Psi_E(A) = J^*\Psi_{E'}(A)J$ and $\Psi_{E'}(A) = J\Psi_E(A)J^*$ for any $A \in End(H)$. Moreover, if Ψ is a complementary channel of Φ, then a complementary of Ψ is isometric to Φ [15, p.96].

Definition 4.4.1. *Let H and K be Hilbert spaces, $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel, and (E, α) be a Stinespring representation of Φ. The map $\Psi : End(H) \longrightarrow End(E)$ sending $A \longmapsto Tr_K(\alpha A \alpha^*)$ is called a* complementary channel of Φ.

It follows from [15, p.96], and [16, p.125].

Proposition 4.4.2. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G. If $\Phi : End(H) \longrightarrow End(K)$ is a G-covariant channel, then any channel complementary to Φ is G-covariant.*

The rest of this section is devoted to giving a formula for channel complementary to EPOSIC channel. The next proposition is needed for the main result of this section.

Proposition 4.4.3. *Let $m, n, h \in \mathbb{N}$ with $0 \le h \le \min\{m, n\}$. Then*

$$flip_{P_n}^{P_m} \alpha_{m,n,h} = (-1)^h \alpha_{n,m,h}$$

where $\alpha_{m,n,h}$ is the isometry in Definition 2.3.2.

Proof:

Let $r = m + n - 2h$, and $\{f_s^k : 0 \le s \le k\}$ be the standard basis of P_k, $k \in \{r, m, n\}$. For $0 \le i \le r$, let

$$B^{m,n,h}(i) = \{j : \max\{0, -m + i + h\} \le j \le \min\{i + h,\, n\}\}$$

and

$$B^{n,m,h}(i) = \{j : \max\{0, -n + i + h\} \le j \le \min\{i + h,\, m\}\}$$

Since $j \in B^{m,n,h}(i)$ if and only if $l_{ij} = i - j + h \in B^{n,m,h}(i)$, we have by Corollary 2.3.16 (2),

$$flip_{P_n}^{P_m} \alpha_{m,n,h}(f_i^r) = \sum_{j \in B^{m,n,h}(i)} \varepsilon_i^j{}_{(m,n,h)}\, f_j^n \otimes f_{l_{ij}}^m = (-1)^h \sum_{l_{ij} \in B^{n,m,h}(i)} \varepsilon_i^{l_{ij}}{}_{(n,m,h)}\, f_j^n \otimes f_{l_{ij}}^m$$

Let $l = l_{ij}$, then

$$flip^{P_m}_{P_n}\alpha_{m,n,h}(f^r_i) = (-1)^h \sum_{l\in B^{n,m,h}(i)} \varepsilon^l_{i(n,m,h)}\, f^n_{i-l+h} \otimes f^m_l$$

$$= (-1)^h \sum_{l\in B^{n,m,h}(i))} \varepsilon^l_{i(n,m,h)}\, f^n_{l_{il}} \otimes f^m_l = (-1)^h \alpha_{n,m,h}(f^r_i)$$

∎

Recall that EPOSIC channel $\Phi_{m,n,h}$ has a Stinespring representation given by $(P_n, \alpha_{m,n,h})$ such that $\alpha_{m,n,h} : P_{m+n-2h} \longrightarrow P_m \otimes P_n$.

Proposition 4.4.4. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$. The channel $\Phi_{n,m,h}$ is a channel complementary to $\Phi_{m,n,h}$.*

Proof:

By Proposition 4.4.3, and Lemma 1.2.23, we have:

$$Tr_{P_m}\left(\alpha_{m,n,h} A \alpha^*_{m,n,h}\right) = Tr_{P_m}\left(flip^{P_m}_{P_n}\alpha_{n,m,h} A \alpha^*_{n,m,h}\left(flip^{P_m}_{P_n}\right)^*\right)$$

$$= Tr_{P_m}\left(\alpha_{n,m,h} A \alpha^*_{n,m,h}\right) = \Phi_{n,m,h}(A).$$

∎

Recall that by Proposition 2.1.6, for any $m \in \mathbb{N}$, the map $J_m : P_m \longrightarrow \overline{P}_m$ is unitary. The following corollary to Proposition 4.4.3 will be used in the next section.

Corollary 4.4.5. *For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$,*

$$flip^{\overline{P}_m}_{P_n}(J_m \otimes J^*_n)\eta_{m,n,h} = (-1)^h\, \eta_{n,m,h}$$

Proof:

By Lemma 2.3.7, we have

$$flip_{P_n}^{\overline{P}_m}(J_m \otimes J_n^*)\eta_{m,n,h} = flip_{P_n}^{\overline{P}_m}(J_m \otimes J_n^*)(I_{P_m} \otimes J_n)\alpha_{m,n,h}$$

$$= flip_{P_n}^{\overline{P}_m}(J_m \otimes I_{P_n})\alpha_{m,n,h}$$

By Proposition 2.1.8, and Proposition 4.4.3, we get

$$flip_{P_n}^{\overline{P}_m}(J_m \otimes J_n^*)\eta_{m,n,h} = (I_{P_n} \otimes J_m) flip_{P_n}^{P_m}\alpha_{m,n,h}$$

$$= (-1)^h (I_{P_n} \otimes J_m)\alpha_{n,m,h} = (-1)^h \eta_{n,m,h}.$$

∎

4.5 Duals of EPOSIC channels

In this section, we give a formula for the dual map of $\Phi_{m,n,h}$, and investigate when this map is a channel. We begin by recalling the definition, and some properties of the dual map of a linear map.

Definition 4.5.1. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a linear map. The dual map of Φ is the unique map $\Phi^* : End(K) \longrightarrow End(H)$ satisfying*

$$\langle B \,|\Phi(A)\rangle_{End(K)} = \langle \Phi^*(B)\,|A\rangle_{End(H)}$$

for any $A \in End(H)$ and $B \in End(K)$, where $\langle \cdot\,|\cdot\,\rangle_{End(H)}$ and $\langle \cdot\,|\,\cdot\rangle_{End(K)}$ are the Hilbert-Schmidt inner products on $End(H)$ and $End(K)$, respectively.

The proofs of the following propositions are given in Appendix **A**.

Proposition 4.5.2. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a linear map. Then*

1. *Φ^* is completely positive if and only if Φ is completely positive.*

2. *Φ^* is trace-preserving if and only if $\Phi(I_H) = I_K$.*

Proposition 4.5.3. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G. A linear map $\Phi : End(H) \longrightarrow End(K)$ is G-equivariant if and only if Φ^* is G-equivariant.*

Proposition 4.5.4. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a completely positive map. If $\{T_i : 1 \leq i \leq d\}$ are Kraus operators of Φ, then $\{T_i^* : 1 \leq i \leq d\}$ are Kraus operators of Φ^*.*

The rest of this section is devoted to finding the dual map of the EPOSIC channel. As the Choi-Jamiolkowski map is unitary (Corollary 1.2.29), we obtain a relation between $\Phi_{m,n,h}$ and $\Phi^*_{m,n,h}$ by examining their Choi matrices, $C(\Phi_{m,n,h}) \in End(P_m \otimes \overline{P}_r)$, and $C(\Phi^*_{m,n,h}) \in End(P_r \otimes \overline{P}_m)$.

Proposition 4.5.5. *For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, let $r = m + n - 2h$ and $\mathcal{T}_{m,r} = flip_{P_r}^{\overline{P}_m}(J_m \otimes J_r^*)$. Then*

$$C(\Phi^*_{m,n,h}) = \mathcal{T}_{m,r} C(\Phi_{m,n,h}) \mathcal{T}^*_{m,r}$$

Proof:

Let $\{T_j : 0 \leq j \leq n\}$ be the EPOSIC Kraus operators of $\Phi_{m,n,h}$, then $\{T_j^* : 0 \leq j \leq n\}$ are Kraus operators for $\Phi^*_{m,n,h}$. By Propositions 3.2.19 2(b), and Proposition 4.2.6, we have

$$C(\Phi^*_{m,n,h}) = \sum_{j=0}^{n} Vec(T_j^*) \left(Vec\left(T_j^*\right)\right)^* = \sum_{j=0}^{n} \mathcal{T}_{m,r} Vec(T_{n-j}) \left(\mathcal{T}_{m,r} Vec(T_{n-j})\right)^*$$

$$= \sum_{j=0}^{n} \mathcal{T}_{m,r} Vec(T_{n-j}) \left(Vec(T_{n-j})\right)^* \mathcal{T}^*_{m,r} = \mathcal{T}_{m,r} \left(\sum_{j=0}^{n} Vec(T_{n-j}) \left(Vec(T_{n-j})\right)^* \right) \mathcal{T}^*_{m,r}$$

$$= \mathcal{T}_{m,r}\left(\sum_{j=0}^{n} Vec(T_j)\,(Vec(T_j))^*\right)\mathcal{T}^*_{m,r} = \mathcal{T}_{m,r}C(\Phi_{m,n,h})\mathcal{T}^*_{m,r}.$$

∎

Proposition 4.5.6. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$. Then*

$$\Phi^*_{m,n,h} = \frac{m+n-2h+1}{m+1}\Phi_{m+n-2h,n,n-h}$$

Proof:

Let $r = m + n - 2h$. By Corollary 1.2.29, it suffices to show that

$$C(\Phi^*_{m,n,h}) = \tfrac{r+1}{m+1}C(\Phi_{r,n,n-h})$$

By Proposition 4.5.5, this is equivalent to show

$$\mathcal{T}_{m,r}C(\Phi_{m,n,h})\mathcal{T}^*_{m,r} = \tfrac{r+1}{m+1}C(\Phi_{r,n,n-h})$$

By Proposition 4.3.5, it suffices to show that

$$\mathcal{T}_{m,r}q_{m,r,m-h}\mathcal{T}^*_{m,r} = q_{r,m,m-h}$$

where $q_{m,r,m-h}$, and $q_{r,m,m-h}$ are the projections on the $SU(2)$-irreducible subspaces of $P_m \otimes \overline{P}_r$ and $P_r \otimes \overline{P}_m$ respectively. By Corollary 2.3.8, and Corollary 4.4.5, one has

$$\begin{aligned}\mathcal{T}_{m,r}q_{m,r,m-h}\mathcal{T}^*_{m,r} &= \mathcal{T}_{m,r}\eta_{m,r,m-h}\eta^*_{m,r,m-h}\mathcal{T}^*_{m,r}\\ &= flip^{\overline{P}_m}_{P_r}\left(J_m \otimes J^*_r\right)\eta_{m,r,m-h}\left(flip^{\overline{P}_m}_{P_r}\left(J_m \otimes J^*_r\right)\eta_{m,r,m-h}\right)^*\\ &= \eta_{r,m,m-h}\eta^*_{r,m,m-h} = q_{r,m,m-h}.\end{aligned}$$

∎

By Proposition 4.5.6, we have

Corollary 4.5.7. *The dual map of $\Phi_{m,n,h}$ is a quantum channel if and only if $n = 2h$. In this case $\Phi^*_{m,2h,h}$ is equal to $\Phi_{m,2h,h}$.*

4.6 A positive map that is not completely positive

By Proposition 4.1.4, for $m \in \mathbb{N} \setminus \{0\}$, the set of EPOSIC channels from $End(P_1)$ to $End(P_m)$ is given by

$$EC(1, m) = \{\Phi_{m,m+1,m}, \Phi_{m,m-1,m-1}\}$$

Below $\{f_0^1, f_1^1\}$ is the standard basis for P_1, given by $f_0^1(x_1, x_2) = x_2$ and $f_1^1(x_1, x_2) = x_1$.

Lemma 4.6.1. *Let $h \in P_1$ with $\|h\| = 1$. Then*

1. *There exists $g_h \in SU(2)$ such that $\rho_{1(g_h)}(f_0^1) = h$.*
2. *If $\Phi : End(P_1) \longrightarrow End(P_m)$ is an $SU(2)$-equivariant map, then the matrices $\Phi(hh^*)$ and $\Phi(f_0^1 f_0^{1^*})$ have the same eigenvalues.*

Proof:

Assume that h is a unit element in P_1; then h can be written as $u_0 f_0^1 + u_1 f_1^1$ for some $u_0, u_1 \in \mathbb{C}$ that satisfy $|u_0|^2 + |u_1|^2 = 1$. Let $g_h = \begin{bmatrix} \overline{u}_0 & u_1 \\ -\overline{u}_1 & u_0 \end{bmatrix} \in SU(2)$. By Remark 2.1.4 (1), we have

$$\begin{aligned}(\rho_{1(g_h)} f_0^1)_{(x_1,x_2)} &= f_0^1(\overline{u}_0 x_1 - \overline{u}_1 x_2, u_1 x_1 + u_0 x_2) \\ &= u_1 x_1 + u_0 x_2 = u_0 f_0^1{}_{(x_1,x_2)} + u_1 f_1^1{}_{(x_1,x_2)} \\ &= h_{(x_1,x_2)}.\end{aligned}$$

For the second statement, by (1), we have

$$hh^* = \rho_{1(g_h)} f_0^1 f_0^{1^*} \rho^*_{1(g_h)}$$

So, by the equivariance property of Φ, we have

$$\Phi(hh^*) = \Phi(\rho_{1(g_h)} f_0^1 f_0^{1^*} \rho^*_{1(g_h)}) = \rho_{1(g_h)} \Phi(f_0^1 f_0^{1^*}) \rho^*_{1(g_h)}$$

which gives the result.

∎

By direct computations using the formula for ε_i^j in Corollary 2.3.13, and by Corollary 4.2.7, one can show:

Lemma 4.6.2. *Let $m \in \mathbb{N} \smallsetminus \{0\}$. Then*

1. $\Phi_{m,m+1,m}(f_0^1 f_0^{1^*}) = \sum_{j=0}^{m} \frac{2(m-j+1)}{(m+1)(m+2)} f_{m-j}^m f_{m-j}^{m^*}$.

2. $\Phi_{m,m-1,m-1}(f_0^1 f_0^{1^*}) = \sum_{j=0}^{m-1} \frac{2(j+1)}{m(m+1)} f_{m-j-1}^m f_{m-j-1}^{m^*}$.

Proposition 4.6.3. *For $m \in \mathbb{N} \smallsetminus \{0\}$ and $\alpha \in \mathbb{R}$, the linear map*

$$\Phi_{m,m+1,m} - \alpha\, \Phi_{m,m-1,m-1} : End(P_1) \longrightarrow End(P_m)$$

is positive if and only if $\alpha \leq \frac{1}{m+2}$.

Proof:

Let A be a positive matrix in $End(P_1)$. By the spectral theorem, there exist an orthonormal basis $\{e_1, e_2\}$ for P_1, and non-negative numbers λ_1, λ_2 such that

$$A = \sum_{i=1}^{2} \lambda_i e_i e_i^*.$$

To show that $\Phi := \Phi_{m,m+1,m} - \alpha \Phi_{m.m-1,m-1}$ is positive, it suffices to show the positivity of $\Phi(e_i e_i^*)$. By Lemma 4.6.1, this is equivalent to the positivity of $\Phi(f_0^1 f_0^{1^*})$.
By Lemma 4.6.2, we have that

$$\Phi(f_0^1 f_0^{1^*}) = \Phi_{m,m+1,m}(f_0^1 f_0^{1^*}) - \alpha\, \Phi_{m,m-1,m-1}(f_0^1 f_0^{1^*}) \geq 0$$

if and only if

$$\sum_{j=0}^{m} \frac{2(m-j+1)}{(m+1)(m+2)} f_{m-j}^m f_{m-j}^{m^*} - \alpha \sum_{j=0}^{m-1} \frac{2(j+1)}{m(m+1)} f_{m-j-1}^m f_{m-j-1}^{m^*} \geq 0$$

if and only if

$$\frac{2}{m+2} f_m^m f_m^{m^*} + \sum_{j=0}^{m-1} \left[\frac{2(m-j)}{(m+1)(m+2)} - \alpha \frac{2(j+1)}{m(m+1)} \right] f_{m-j-1}^m f_{m-j-1}^{m^*} \geq 0.$$

Thus

$$\Phi(f_0^1 f_0^{1^*}) \geq 0 \Longleftrightarrow \alpha \leq \min\{\tfrac{m(m-j)}{(m+2)\,(j+1)} : 0 \leq j \leq m-1\}.$$

Since the map $f(t) = \frac{(m-t)}{t+1}$ is decreasing for $0 \leq t \leq m-1$, then

$$\min\{\tfrac{m(m-j)}{(m+2)\,(j+1)} : 0 \leq j \leq m-1\} = \tfrac{1}{m+2}$$

Consequently, $\Phi(f_0^1 f_0^{1^*}) \geq 0$ if and only if $\alpha \leq \frac{1}{m+2}$. ∎

The following lemma follows by direct computation, using the formula for ε_i^j in Corollary 2.3.13.

Lemma 4.6.4. *For $m \in \mathbb{N} \setminus \{0\}$, we have*

$$\varepsilon^0_{1(m,1,0)} = \sqrt{\tfrac{m}{m+1}}, \qquad \varepsilon^1_{1(m,1,0)} = \sqrt{\tfrac{1}{m+1}}$$

and

$$\varepsilon^0_{0(m,1,1)} = \sqrt{\tfrac{1}{m+1}}, \qquad \varepsilon^1_{0(m,1,1)} = -\sqrt{\tfrac{m}{m+1}}$$

Proposition 4.6.5. *Let $m \in \mathbb{N} \setminus \{0\}$. For $\alpha > 0$, the map*

$$\Phi_{m,m+1,m} - \alpha\, \Phi_{m,m-1,m-1}$$

is not completely positive.

Proof:

Let $\Phi := \Phi_{m,m+1,m} - \alpha \Phi_{m,m-1,m-1}$. By Theorem 3.1.5, it is enough to show that $-\frac{2\alpha}{m}$ is an eigenvalue of $C(\Phi)$.

By Proposition 4.3.5,

$$C(\Phi_{m,m+1,m}) = \tfrac{2}{m+2} \eta_{m,1,0} \eta^*_{m,1,0}$$

and

$$C(\Phi_{m,m-1,m-1}) = \tfrac{2}{m}\eta_{m,1,1}\eta^*_{m,1,1}$$

Let $v = \sqrt{m}(f_0^m \otimes f_0^1) + f_1^m \otimes f_1^1$, then

$$\begin{aligned}
C(\Phi_{m,m+1,m})\,(v) &= \tfrac{2}{m+2}\eta_{m,1,0}\eta^*_{m,1,0}\,(\sqrt{m}(f_0^m \otimes f_0^1) + f_1^m \otimes f_1^1) \\
&= \tfrac{2}{m+2}\eta_{m,1,0}\,[(-\sqrt{m}\varepsilon^1_{1(m,1,0)} + \varepsilon^0_{1(m,1,0)})f_1^{m+1}] \\
&= \tfrac{2}{m+2}\eta_{m,1,0}\left[(-\sqrt{\tfrac{m}{m+1}} + \sqrt{\tfrac{m}{m+1}})f_1^{m+1}\right] \text{ (Lemma 4.6.4)} \\
&= \tfrac{2}{m+2}\eta_{m,1,0}\,[0 \times f_1^{m+1}] = 0.
\end{aligned}$$

Similarly,

$$\begin{aligned}
C(\Phi_{m,m-1,m-1})\,(v) &= \tfrac{2}{m}\eta_{m,1,1}\eta^*_{m,1,1}\,(\sqrt{m}(f_0^m \otimes f_0^1) + f_1^m \otimes f_1^1) \\
&= \tfrac{2}{m+2}\eta_{m,1,1}\,[(-\sqrt{m}\varepsilon^1_{0(m,1,1)} + \varepsilon^0_{0(m,1,1)})f_0^{m-1}] \\
&= \tfrac{2}{m}(\tfrac{m+1}{\sqrt{m+1}})\eta_{m,1,1}(f_0^{m-1}) \text{ (Lemma 4.6.4)} \\
&= \tfrac{2\sqrt{m+1}}{m}\left[\sum_{j=0}^{1}(-1)^j\varepsilon_0^j f_{1-j}^m \otimes f_{1-j}^1\right] \\
&= \tfrac{2\sqrt{m+1}}{m}(\tfrac{1}{\sqrt{m+1}}f_1^m \otimes f_1^1 + \sqrt{\tfrac{m}{m+1}}f_0^m \otimes f_0^1) \\
&= \tfrac{2}{m}(f_1^m \otimes f_1^1 + \sqrt{m}f_0^m \otimes f_0^1) = \tfrac{2}{m}v.
\end{aligned}$$

So, we have

$$C(\Phi)(v) = C(\Phi_{m,m+1,m})(v) - \alpha C(\Phi_{m,m-1,m-1})(v) = -\tfrac{2\alpha}{m}v$$

Hence, $-\frac{2\alpha}{m}$ is a negative eigenvalue of $C(\Phi)$ for any $\alpha > 0$. ∎

Combining the result of Proposition 3.1.3, and 4.6.3 and Theorem 3.1.4, we obtain:

Theorem 4.6.6. Let $m \in \mathbb{N} \setminus \{0\}$. For $\alpha > 0$, the map

$$\Phi_{m,m+1,m} - \alpha\,\Phi_{m,m-1,m-1}$$

is not n-positive for any $n > 1$.

Chapter 5

$SU(2)$-Irreducibly Covariant Channels

Here, we study $SU(2)$-irreducibly covariant channels. In the first section, we use results from Section 4.3 to show that the EPOSIC channels $EC(r,m)$ form a spanning set of the set of all $SU(2)$-irreducibly equivariant maps $End(End(P_r), End(P_m))^{SU(2)}$. We also show that they are the extreme points of the set of all $SU(2)$-irreducibly covariant channels $QC(P_r, P_m)^{SU(2)}$. In Section 5.2, we decompose $SU(2)$-irreducibly covariant channels as orthogonal direct sums of operators between isomorphic $SU(2)$-irreducible subspaces of $End(P_r)$ and $End(P_m)$ respectively.

The main results of this chapter:

- The EPOSIC channels $EC(r,m)$ constitute the extreme points of the $SU(2)$-irreducibly covariant channels $QC(P_r, P_m)^{SU(2)}$ (Corollary 5.1.5).
- Any completely positive $SU(2)$-irreducibly equivariant map is a multiple of an $SU(2)$-covariant channel (Corollary 5.1.6).

- Any $SU(2)$-irreducibly covariant channel is an orthogonal direct sum of operators (Corollary 5.2.4).

5.1 Extreme points of $SU(2)$-irreducibly covariant channels

Recall that for $r, m \in \mathbb{N}$, the set $EC(r,m)$ is $\{\Phi_{m,r+m-2l,m-l},\ 0 \le l \le \min\{r,m\}\}$, and $QC(P_r, P_m)^{SU(2)}$ is the set of $SU(2)$-irreducibly covariant channels from $End(P_r)$ to $End(P_m)$. In this section, we show that $EC(r,m)$ consist of all the extreme points of $QC(P_r, P_m)^{SU(2)}$.

Recall also that $End(End(P_r), End(P_m))^{SU(2)}$ denotes the vector space of the $SU(2)$-equivariant maps from $End(P_r)$ to $End(P_m)$.

Proposition 5.1.1. *Let $r, m \in \mathbb{N}$. The set $EC(r,m)$ is a spanning set of*

$$End(End(P_r), End(P_m))^{SU(2)}$$

.

Proof:

By Proposition 4.3.1, and Proposition 4.3.5, we have

$$\begin{aligned} End(P_m \otimes \overline{P}_r)^{SU(2)} &= \left\{ \sum_{l=0}^{\min\{r,m\}} \lambda_l q_{m,r,l} : \lambda_l \in \mathbb{C} \right\} \\ &= \left\{ \sum_{l=0}^{\min\{r,m\}} \mu_l C(\Phi_{m,m+r-2l,m-l}) : \mu_l \in \mathbb{C} \right\} \\ &= Span\left\{ C\left(\Phi\right) : \Phi \in EC(r,m) \right\} \end{aligned}$$

The result now follows from Corollary 1.2.29 and Proposition 1.2.32. ∎

Proposition 5.1.2. *Let $r, m \in \mathbb{N}$. The set $QC(P_r, P_m)^{SU(2)}$ is the convex hull of $EC(r, m)$.*

Proof:

Let $\Phi \in QC(P_r, P_m)^{SU(2)}$. Since Φ is an $SU(2)$-equivariant map, then by Proposition 5.1.1, we have

$$\Phi = \sum_{l=0}^{\min\{r,m\}} \lambda_l \Phi_{m,m+r-2l,m-l} \qquad \lambda_l \in \mathbb{C}$$

It remains to show that $0 \leq \lambda_l$ and $\sum_{l=0}^{\min\{r,m\}} \lambda_l = 1$. By Remark 4.3.6, we have

$$C(\Phi) = \sum_{l=0}^{\min\{r,m\}} \tfrac{r+1}{m+r-2l+1} \lambda_l q_{m,r,l}$$

where $\{q_{m,r,l}\,, 0 \leq l \leq \min\{r, m\}\}$ are mutually orthogonal projections of $P_m \otimes \overline{P}_r$. By the orthogonality of the projections $\{q_{m,r,l}\,, 0 \leq l \leq \min\{r, m\}\}$, and the positivity of $C(\Phi)$, we have $\lambda_l \geq 0$ for $0 \leq l \leq \min\{m, r\}$.
As Φ and $\Phi_{m,m+r-2l,m-l}$ are trace preserving, by choosing any state $\varrho \in D(P_r)$, we have

$$1 = tr(\varrho) = tr(\Phi(\varrho)) = \sum_{l=0}^{\min\{r,m\}} \lambda_l tr(\Phi_{m,m+r-2l,m-l}(\varrho)) = \sum_{l=0}^{\min\{r,m\}} \lambda_l$$

Since $EC(r, m) \subseteq QC(P_r, P_m)^{SU(2)}$ the result follows. ∎

Proposition 5.1.3. *Let $r, m \in \mathbb{N}$. Any element in $QC(P_r, P_m)^{SU(2)}$ is uniquely written as a convex combination of elements of $EC(r, m)$.*

Proof:

By Proposition 5.1.2, we need only to prove the uniqueness. Let $\Psi \in QC(P_r, P_m)^{SU(2)}$ such that

$$\sum_{l=0}^{\min\{r,m\}} \lambda_l \Phi_l = \Psi = \sum_{l=0}^{\min\{r,m\}} \mu_l \Phi_l$$

where $\Phi_l = \Phi_{m,m+r-2l,m-l}$. By Proposition 4.3.5, and the orthogonality of

$$\{q_{m,r,l}, 0 \leq l \leq \min\{m, r\}\}$$

we have

$$\frac{r+1}{m+r-2l+1}\lambda_l q_{m,r,l} = q_{m,r,l} C(\Psi) = \frac{r+1}{m+r-2l+1}\mu_l q_{m,r,l}$$

Thus, $\lambda_l = \mu_l$. ∎

The following definition is a special case of the definition of the extreme sets given in [31, p.70].

Definition 5.1.4. *Let K be a subset of a vector space X, and $x \in K$. we say that x is an extreme point of K if x is not an internal point of a line interval whose end points are in K. Analytically, the condition can be expressed as follows:*
if $y \in K$, $z \in K$, $0 < t < 1$, and $x = ty + (1-t)z$, then $x = y = z$.
i.e. x can not be written as a proper convex combination of elements of K other than itself.

Corollary 5.1.5. *Let $r, m \in \mathbb{N}$. The set $EC(r, m)$ forms all the extreme points of $QC(P_r, P_m)^{SU(2)}$.*

Proof:

As $EC(r, m) \subset QC(P_r, P_m)^{SU(2)}$, by Proposition 5.1.3, we have $EC(r, m)$ are extreme points of $QC(P_r, P_m)^{SU(2)}$. On the other direction, if Φ is an extreme point of $QC(P_r, P_m)^{SU(2)}$, then it can not be written as a linear combination of elements of $QC(P_r, P_m)^{SU(2)}$ other than itself. Hence, Φ must be in $EC(r, m)$. ∎

As $EC(r, m)$ is a spanning set of both $End(End(P_r), End(P_m))^{SU(2)}$, and $QC(P_r, P_m)^{SU(2)}$, we have the following corollary:

Corollary 5.1.6. *Let $r, m \in \mathbb{N}$. Any completely positive $SU(2)$-equivariant linear map $\Phi : End(P_r) \longrightarrow End(P_m)$ is a multiple of an $SU(2)$-irreducibly covariant channel.*

Proof:

By Proposition 5.1.1, we have

$$\Phi = \sum_{l=0}^{\min\{r,m\}} \lambda_l \Phi_{m,r+m-2l,m-l}$$

for some $\lambda_l \in \mathbb{C}$. Since Φ is completely positive, the coefficients λ_l are non-negative (otherwise, $C(\Phi) = \sum_{l=0}^{\min\{r,m\}} \frac{r+1}{m+r-2l+1} \lambda_l q_{m,r,l}$ will have a negative eigenvalue).
Let $\lambda = \sum_{l=0}^{\min\{r,m\}} \lambda_l$.

If $\lambda = 0$ then $\lambda_l = 0$ for all $0 \leq l \leq \min\{r, m\}$, and $\Phi = 0$ is a multiple of any $SU(2)$-irreducibly covariant channel. If $\lambda \neq 0$, then

$$\Psi = \sum_{l=0}^{\min\{m,r\}} \frac{\lambda_l}{\lambda} \Phi_{m,m+r-2l,m-l}$$

is a convex combination of EPOSIC channels. Thus, by Proposition 5.1.2, Ψ is an $SU(2)$-irreducibly covariant channel, and $\Phi = \lambda\Psi$. ∎

Remark 5.1.7. For $\Phi \in QC(P_r, P_m)^{SU(2)}$, the dual map of Φ can be computed using Proposition 5.1.2, and Proposition 4.5.6. It also follows (by Corollary 4.5.7) that the map Φ^* is a quantum channel if and only if $\Phi \in QC(P_m)^{SU(2)}$.

Recall that $QC(P_m)^{SU(2)}$, the set of all $SU(2)$-covariant channels from $End(P_m) \longrightarrow End(P_m)$, is the convex hull of $EC(m) = \{\Phi_{m,2h,h} : 0 \leq h \leq m\}$. Let $\circ$ denote the composition of two channels, then

Proposition 5.1.8. *The set $\left(QC(P_m)^{SU(2)}, \circ\right)$ is an abelian monoid. It is closed under involution, in fact every element is self-adjoint.*

Proof:

As the composition of two G-covariant channels is again G-covariant, the composition of linear maps is an associative binary operation on $QC(P_m)^{SU(2)}$, with the identity map being the identity element. By Proposition 4.3.1, it is abelian. Since the dual map of $\Phi_{m,2h,h}$ is $\Phi_{m,2h,h}$ (Corollary 4.5.7), then by Proposition 5.1.3 every element is self adjoint, so $QC(P_m)^{SU(2)}$ is closed under involution. ∎

We complete this section with two examples of $SU(2)$-irreducibly covariant channels written as convex combinations of EPOSIC channels.

Example I: The generalized completely depolarizing channel

Recall that the generalized completely depolarizing channel is defined for Hilbert spaces H and K by

$$\Phi : End(H) \longrightarrow End(K)$$

$$A \longrightarrow \tfrac{tr(A)}{d_K} I_K$$

where I_K is the identity matrix on K, and d_k is the dimension of the space K. Recall also that it is a G-covariant channel, see Example 3.3.2. For $r, m \in \mathbb{N}$, we denote the generalized completely depolarizing channel from $End(P_r)$ to $End(P_m)$ by $\Psi_{r,m}$.

Proposition 5.1.9. *Let $r, m \in \mathbb{N}$. Then*

$$\Psi_{r,m}(A) = \sum_{l=0}^{\min\{r,m\}} \tfrac{r+m-2l+1}{(r+1)(m+1)}\, \Phi_{m,r+m-2l,m-l}(A).$$

for any $A \in End(P_r)$.

Proof:

By Corollary 5.1.2, there exist $\{\lambda_l : 0 \leq l \leq \min\{r,m\}\}$ such that $0 \leq \lambda_l \leq 1$, $\sum_{l=0}^{\min\{r,m\}} \lambda_l = 1$, and

$$\Psi_{r,m} = \sum_{l=0}^{\min\{r,m\}} \lambda_l \, \Phi_{m,r+m-2l,m-l}$$

Applying the Choi-Jamiolkowski map on both sides, by Proposition 4.3.5, we get

$$C(\Psi_{r,m}) = \sum_{l=0}^{\min\{r,m\}} \lambda_l \, \tfrac{r+1}{r+m-2l+1} q_{m,r,l}.$$

On the other hand, by Lemma 1.2.30,

$$\begin{aligned} C(\Psi_{r,m}) &= \sum_{i_1,i_2} \tfrac{tr(E_{i_1 i_2})}{m+1} \, I_{P_m} \otimes E_{i_1 i_2} = \sum_{i_1,i_2} \tfrac{1}{m+1} \delta_{i_1 i_2} \, I_{P_m} \otimes E_{i_1 i_2} \\ &= \sum_{i_1} \tfrac{1}{m+1} \, I_{P_m} \otimes E_{i_1 i_1} = \tfrac{1}{m+1} \, I_{P_m} \otimes \sum_{i_1} E_{i_1 i_1} = \tfrac{1}{m+1} \, I_{P_m} \otimes I_{P_r} \end{aligned}$$

Thus

$$\sum_{l=0}^{\min\{r,m\}} \lambda_l \, \tfrac{(r+1)(m+1)}{r+m-2l+1} q_{m,r,l} = I_{P_m} \otimes I_{P_r}$$

By the orthogonality of $\{q_{m,r,l} : 0 \leq l \leq \min\{r,m\}\}$, we have

$$\lambda_s \, \tfrac{(r+1)(m+1)}{r+m-2s+1} q_{m,r,s} = q_{m,r,s} \, (I_{P_m} \otimes I_{P_r}) = q_{m,r,s}$$

for $0 \leq s \leq \min\{r,m\}$. Taking the trace of both sides, we get $\lambda_s = \frac{r+m-2s+1}{(r+1)(m+1)}$. ∎

Example II: The maps $\Phi_{1,m-1,0} \circ \Phi_{m,m-1,m-1}$ and $\Phi_{1,m-1,0} \circ \Phi_{m,m+1,m}$

Recall (by Proposition 4.1.4) that for $m \in \mathbb{N} \setminus \{0\}$,

$$EC(1,m) = \{\Phi_{m,m+1,m}, \Phi_{m,m-1,m-1}\}, \text{ and } EC(m,1) = \{\Phi_{1,m+1,1}, \Phi_{1,m-1,0}\}$$

Lemma 5.1.10. *For $m \in \mathbb{N} \setminus \{0\}$, and $0 \leq i \leq m$, we have*

$$\Phi_{1,m-1,0}(f_i^m f_i^{m^*}) = \tfrac{m-i}{m} f_0^1 f_0^{1^*} + \tfrac{i}{m} f_1^1 f_1^{1^*}$$

where $\{f_i^m : 0 \leq i \leq m\}$ is the standard basis for P_m.

Proof:

To simplify the notation, let $\varepsilon_i^j := \varepsilon_{i\,(1,m-1,0)}^j$ for any $j \in B(i)$. For $1 \leq i \leq m-1$, by direct computation, we have

$$\varepsilon_i^{i-1} = \sqrt{\tfrac{i}{m}}, \quad \varepsilon_i^i = \sqrt{\tfrac{m-i}{m}}$$

We also have $\varepsilon_0^0 = 1$, and $\varepsilon_m^{m-1} = 1$.

Thus, by Corollary 4.2.7,

$$\Phi_{1,m-1,0}(f_i^m f_i^{m^*}) = \sum_{j \in B(i)} (\varepsilon_i^j)^2 f_{l_{ij}}^m f_{l_{ij}}^{m^*} = \begin{cases} (\varepsilon_0^0)^2 f_0^1 f_0^{1^*} & i = 0 \\ (\varepsilon_i^{i-1})^2 f_1^1 f_1^{1^*} + (\varepsilon_i^i)^2 f_0^1 f_0^{1^*} & 1 \leq i \leq m-1 \\ (\varepsilon_m^{m-1})^2 f_1^1 f_1^{1^*} & i = m \end{cases}$$

$$= \begin{cases} f_0^1 f_0^{1^*} & i = 0 \\ \frac{i}{m} f_1^1 f_1^{1^*} + \frac{m-i}{m} f_0^1 f_0^{1^*} & 1 \leq i \leq m-1 \\ f_1^1 f_1^{1^*} & i = m \end{cases}$$

$$= \tfrac{i}{m} f_1^1 f_1^{1^*} + \tfrac{m-i}{m} f_0^1 f_0^{1^*}.$$

∎

Proposition 5.1.11. *For $m \in \mathbb{N} \setminus \{0\}$, we have*

$$\Phi_{1,m-1,0} \circ \Phi_{m,m+1,m} = \Phi_{1,2,1}$$

and

$$\Phi_{1,m-1,0} \circ \Phi_{m,m-1,m-1} = \tfrac{m-1}{2m}\Phi_{1,2,1} + \tfrac{m+1}{2m}\Phi_{1,0,0}$$

Proof:

By Proposition 5.1.2, both maps $\Phi_{1,m-1,0} \circ \Phi_{m,m+1,m}$, and $\Phi_{1,m-1,0} \circ \Phi_{m,m-1,m-1}$ are convex combination of elements in $EC(1,1) = \{\Phi_{1,2,1}, \Phi_{1,0,0}\}$. So, there exist $0 \le p_1, p_2 \le 1$ such that

$$\Phi_{1,m-1,0} \circ \Phi_{m,m+1,m} = p_1\Phi_{1,2,1} + (1-p_1)\Phi_{1,0,0}$$

and

$$\Phi_{1,m-1,0} \circ \Phi_{m,m-1,m-1} = p_2\Phi_{1,2,1} + (1-p_2)\Phi_{1,0,0}$$

To find p_1 and p_2, we evaluate the expressions above at $f_0^1 f_0^{1^*}$. By Lemma 4.6.2, and Lemma 5.1.10, we have

$$\begin{aligned}
\Phi_{1,m-1,0}\circ\Phi_{m,m+1,m}(f_0^1 f_0^{1^*}) &= \Phi_{1,m-1,0}\left(\sum_{j=0}^{m} \tfrac{2(m-j+1)}{(m+1)(m+2)} f_{m-j}^m f_{m-j}^{m^*}\right) \\
&= \Phi_{1,m-1,0}\left(\sum_{i=0}^{m} \tfrac{2(i+1)}{(m+1)(m+2)} f_i^m f_i^{m^*}\right) \\
&= \sum_{i=0}^{m} \tfrac{2(i+1)}{(m+1)(m+2)} \Phi_{1,m-1,0}\left(f_i^m f_i^{m^*}\right) \\
&= \sum_{i=0}^{m} \tfrac{2(i+1)}{(m+1)(m+2)} \left[\tfrac{m-i}{m} f_0^1 f_0^{1^*} + \tfrac{i}{m} f_1^1 f_1^{1^*}\right] \\
&= \tfrac{2}{m(m+1)(m+2)}\left[\sum_{i=0}^{m}(i+1)(m-i) f_0^1 f_0^{1^*} + \sum_{i=0}^{m} i(i+1) f_1^1 f_1^{1^*}\right] \\
&= \tfrac{2}{m(m+1)(m+2)}\left[\tfrac{m(m+1)(m+2)}{6} f_0^1 f_0^{1^*} + \tfrac{m(m+1)(m+2)}{3} f_1^1 f_1^{1^*}\right] \\
&= \tfrac{1}{3} f_0^1 f_0^{1^*} + \tfrac{2}{3} f_1^1 f_1^{1^*}
\end{aligned}$$

On the other hand, direct computations using Corollary 4.2.7, gives

$$p_1\Phi_{1,2,1}(f_0^1 f_0^{1^*}) + (1-p_1)\Phi_{1,0,0}(f_0^1 f_0^{1^*}) = \tfrac{p_1}{3} f_0^1 f_0^{1^*} + \tfrac{2p_1}{3} f_1^1 f_1^{1^*} + (1-p_1) f_0^1 f_0^{1^*}$$

Thus $p_1 = 1$. In similar way, by Lemma 4.6.2, we have

$$\begin{aligned}
\Phi_{1,m-1,0}\circ\Phi_{m,m-1,m-1}(f_0^1 f_0^{1^*}) &= \Phi_{1,m-1,0}\left(\sum_{j=0}^{m-1}\tfrac{2(j+1)}{m(m+1)} f_{m-j-1}^m f_{m-j-1}^{m^*}\right)\\
&= \Phi_{1,m-1,0}\left(\sum_{i=0}^{m-1}\tfrac{2(m-i)}{m(m+1)} f_i^m f_i^{m^*}\right)\\
&= \sum_{i=0}^{m-1}\tfrac{2(m-i)}{m(m+1)}\Phi_{1,m-1,0}\left(f_i^m f_i^{m^*}\right)\\
&= \sum_{i=0}^{m-1}\tfrac{2(m-i)}{m(m+1)}\left[\tfrac{(m-i)}{m} f_0^1 f_0^{1^*} + \tfrac{i}{m} f_1^1 f_1^{1^*}\right]\\
&= \tfrac{2}{m^2(m+1)}\left[\sum_{i=0}^{m-1}(m-i)^2 f_0^1 f_0^{1^*} + \sum_{i=0}^{m-1} i(m-i) f_1^1 f_1^{1^*}\right]\\
&= \tfrac{2}{m^2(m+1)}\left[\tfrac{m(m+1)(2m+1)}{6} f_0^1 f_0^{1^*} + \tfrac{m(m+1)(m-1)}{6} f_1^1 f_1^{1^*}\right]\\
&= \tfrac{2m+1}{3m} f_0^1 f_0^{1^*} + \tfrac{m-1}{3m} f_1^1 f_1^{1^*}
\end{aligned}$$

On the other hand

$$p_2\Phi_{1,2,1}(f_0^1 f_0^{1^*}) + (1-p_2)\Phi_{1,0,0}(f_0^1 f_0^{1^*}) = \tfrac{p_2}{3} f_0^1 f_0^{1^*} + \tfrac{2p_2}{3} f_1^1 f_1^{1^*} + (1-p_2) f_0^1 f_0^{1^*}$$

which implies that $p_2 = \frac{m-1}{2m}$. ∎

5.2 $SU(2)$-irreducibly covariant channel as direct sum of operators

In this section, we use the decomposition of $End(P_r)$ and $End(P_m)$ in Proposition 2.4.1, to write any $SU(2)$-irreducibly covariant channel as an orthogonal direct sum of operators. Recall that if $H_1, H_2, ...H_n$ is a family of complex Hilbert spaces, then their orthogonal direct sum, denoted by $\bigoplus_{i=1}^{n} H_i$ is $\{(h_1, h_2, ..., h_n) : h_i \in H_i\}$.

Definition 5.2.1. *Let* $H = \bigoplus_{i=1}^{n} W_i$ *(resp.* $K = \bigoplus_{i=1}^{n} V_i$*) be the orthogonal direct sum of Hilbert spaces* H_i *(resp.* K_i *) for* $1 \leq i \leq n$*, and* $\{\phi_i : W_i \longrightarrow V_i, 1 \leq i \leq n\}$ *be a collection of linear maps. The orthogonal direct sum of* $\{\phi_i : W_i \longrightarrow V_i, 1 \leq i \leq n\}$*, denoted by* $\bigoplus_{i=1}^{n} \phi_i$ *is the map* $\Phi : H \longrightarrow K$ *defined by*

$$\Phi((h_1, h_2, ..., h_n)) = (\phi_1(h_1), \phi_2(h_2), ..., \phi_n(h_n))$$

The proof of the next theorem is provided in the Appendix **B**.

Theorem 5.2.2. Let G be a group and $H = \bigoplus_{t=1}^{r} W_t$ (resp. $K = \bigoplus_{s=1}^{m} V_s$), where $\{W_t : 1 \leq t \leq r\}$ (resp. $\{V_s : 1 \leq s \leq m\}$) are nonequivalent G-irreducible spaces. Suppose there exists $k \in \mathbb{N}$ such that

1. For each $1 \leq t \leq k$, $W_t \simeq V_t$ via a G-equivariant isomorphism

$$\psi_t : W_t \longrightarrow V_t$$

2. For each $t > k$ the subspace W_t is not equivalent to any of the V_s, for any $1 \leq s \leq m$.

Then, for any G-equivariant map $\Phi : H \longrightarrow K$, there exist $\lambda_1, \lambda_2, ..., \lambda_k$ such that Φ is the orthogonal direct sum of the operators $\{\lambda_t \psi_t : 1 \leq t \leq k\}$

i.e.,

$$\Phi = \bigoplus_{t=1}^{k} \lambda_t \psi_t$$

Reminder:

Recall by Proposition 2.4.1 and Proposition 2.4.2, that for $m \in \mathbb{N}$, the algebra $End(P_m)$ decomposes into mutually orthogonal subspaces $\{U_{2t} : 0 \leq t \leq m\}$ where

$$U_{2t} = \mathrm{Vec}_m^* \eta_{m,m,m-t} \eta_{m,m,m-t}^* \mathrm{Vec}_m(End(P_m)) = \mathrm{Vec}_m^* \eta_{m,m,m-t}(P_{2t})$$

and where each matrix A_{2t} in U_{2t} corresponds to a unique vector v_{2t} in P_{2t}.

Lemma 5.2.3. *Let $r, m \in \mathbb{N}$. Let $End(P_r) = \bigoplus_{t=0}^{r} U_{2t}$ (resp. $End(P_m) = \bigoplus_{s=0}^{m} U'_{2s}$) be the decomposition of $End(P_r)$ (resp. $End(P_m)$) into $SU(2)$-irreducible invariant subspaces. For any $0 \leq t \leq \min\{m, r\}$, the map*

$$\mathrm{Vec}_{\mathrm{m}}^{*} \eta_{m,m,m-t} \eta_{r,r,r-t}^{*} \mathrm{Vec}_{\mathrm{r}}$$

defines an $SU(2)$-isomorphism $\psi_{2t} : U_{2t} \longrightarrow U'_{2t}$. Moreover, both matrices $A_{2t} \in U_{2t}$, and $\psi_{2t}(A_{2t}) \in U'_{2t}$ correspond to the same vector in P_{2t}.

Proof:

Let $0 \leq t \leq r$ and $0 \leq s \leq m$, by Proposition 2.4.2, the $SU(2)$-irreducible subspaces U_{2t} and U'_{2s} are given via the equations $U_{2t} = \mathrm{Vec}_{\mathrm{r}}^{*} \eta_{r,r,r-t}(P_{2t})$, and $U'_{2s} = \mathrm{Vec}_{\mathrm{m}}^{*} \eta_{m,m,m-s}(P_{2s})$ respectively. For each $0 \leq t \leq \min\{m, r\}$, the map

$$\psi_{2t} = \mathrm{Vec}_{\mathrm{m}}^{*} \eta_{m,m,m-t} \eta_{r,r,r-t}^{*} \mathrm{Vec}_{\mathrm{r}} : U_{2t} \longrightarrow U'_{2t}$$

is a nonzero $SU(2)$-equivariant map (note that $\eta_{m,m,m-t}^{*} \eta_{m,m,m-t} = I_{P_{2t}} = \eta_{r,r,r-t}^{*} \eta_{r,r,r-t}$, so $\eta_{r,r,r-t}^{*}$ is onto and $\eta_{m,m,m-t} \neq 0$. Hence, the map $\eta_{m,m,m-t} \eta_{r,r,r-t}^{*}$ is nonzero). By Schur's Lemma 1.2.12, the map ψ_{2t} is isomorphism. To show the second statement, pick $A_{2t} \in U_{2t}$ then $v_{2t} = \eta_{r,r,r-t}^{*} \mathrm{Vec}_{\mathrm{r}}(A_{2t})$ is the vector in P_{2t} corresponding to A_{2t}, and

$$\psi_{2t}(A_{2t}) = \mathrm{Vec}_{\mathrm{m}}^{*} \eta_{m,m,m-t} \eta_{r,r,r-t}^{*} \mathrm{Vec}_{\mathrm{r}}(A_{2t}) = \mathrm{Vec}_{\mathrm{m}}^{*} \eta_{m,m,m-t}(v_{2t})$$

is the matrix in $U'_{2t} \subseteq End(P_m)$ corresponding to v_{2t}. ∎

Recall by Corollary 2.4.3 that any $A \in End(P_r)$ can be decomposed into an orthogonal direct sum of matrices. Namely $A = (A_0, A_2, \ldots .A_{2r})$ where $A_{2t} \in U_{2t}$. By Theorem 5.2.2 and Lemma 5.2.3, we have

Corollary 5.2.4. *Let $r, m \in \mathbb{N}$. Let $\Phi : End(P_r) \longrightarrow End(P_m)$ be an $SU(2)$-equivariant map. The map Φ can be written as an orthogonal direct sum of operators. More precisely, there exist $\{\lambda_{2t} : 0 \leq t \leq \min\{m, r\}\}$, and operators*

$\left\{\psi_{2t} = \mathrm{Vec}^*_{m}\eta_{m,m,m-t}\eta^*_{r,r,r-t}\mathrm{Vec}_{r} : \ 0 \leq t \leq \min\{m,r\}\right\}$ *such that*

$$\Phi\left(A_0 + A_2 + ... + A_{2r}\right) = \sum_{t=0}^{\min\{m,r\}} \lambda_{2t}\psi_{2t}(A_{2t})$$

for $A_0 + A_2 + ... + A_{2r} \in End(P_r)$.

Remark 5.2.5. By Lemma 5.2.3, the matrix $\psi_{2t}(A_{2t})$ in Corollary 5.2.4 is computed using the map $\mathrm{Vec_m}^*\eta_{m,m,m-t}\eta^*_{r,r,r-t}\mathrm{Vec_r}$ independently from the definition of the map Φ, and depends only on m,r. i.e. all the information about the map Φ will be encoded in the set of the numbers $\{\lambda_{2t} : 0 \leq t \leq \min\{r,m\}\}$.

The rest of this section is devoted to computing the numbers $\{\lambda_{2t} : \ 0 \leq t \leq \min\{r,m\}\}$ in Corollary 5.2.4 for the EPOSIC channel $\Phi_{m,n,h}$. As $\Phi_{m,n,h}(A_{2t}) = \lambda_{2t}\psi_{2t}(A_{2t})$ for any $0 \leq t \leq \min\{r,m\}$, we can find λ_{2t} by evaluating both sides of $\Phi_{m,n,h}(A_{2t}) = \lambda_{2t}\psi_{2t}(A_{2t})$ at some basic element of P_m. The big challenge is making a good choice for the matrix A_{2t}, the one that minimizes the computations. By Remark 2.4.7, the matrix A_{2t} that corresponds to the vector f^{2t}_t is a diagonal matrix. Hoping for a good choice, we choose this matrix to compute λ_{2t}. This matrix is given by the formula $A_{2t} = \sum\limits_{j=0}^{r}(-1)^j\varepsilon^j_{t\,(r,r,r-t)}f^r_{r-j}f^{r^*}_{r-j}$.

Proposition 5.2.6. *Let* $m,n,h \in \mathbb{N}$ *with* $0 \leq h \leq \min\{m,n\}$. *Let* $\Phi_{m,n,h}$ *be the associated EPOSIC channel, and* $r = m+n-2h$. *For* $0 \leq t \leq \min\{m,r\}$, *the coefficient* λ_{2t} *is given by*

$$\lambda_{2t} = \frac{\sum\limits_{j=m-h}^{r}(-1)^j\varepsilon^j_{t\,(r,r,r-t)}\left(\varepsilon^{r-j+h}_{r-j\,(m,n,h)}\right)^2}{(-1)^m\varepsilon^m_{t\,(m,m,m-t)}}$$

Proof:

Pick $f^{2t}_t \in P_{2t}$. By Remark 2.4.7, the matrix in $End(P_r)$ that corresponds to f^{2t}_t is

$$A_{2t} = \sum_{j=0}^{r}(-1)^j\varepsilon^j_{t\,(r,r,r-t)}f^r_{r-j}f^{r^*}_{r-j}$$

By Corollary 4.2.7,

$$\Phi_{m,n,h}(f^r_{r-j}f^{r^*}_{r-j})(f^m_0) = \begin{cases} \left(\varepsilon^{r-j+h}_{r-j}{}_{(m,n,h)}\right)^2 f^m_0 & if \quad r-j+h \in B(r-j) \\ 0 & else \end{cases}$$

$$= \begin{cases} \left(\varepsilon^{r-j+h}_{r-j}{}_{(m,n,h)}\right)^2 f^m_0 & if \quad j \geq m-h \\ 0 & else \end{cases}$$

Thus

$$\Phi_{m,n,h}(A_{2t})(f^m_0) = \sum_{j=0}^{r} (-1)^j \varepsilon^j_t{}_{(r,r,r-t)} \Phi_{m,n,h}(f^r_{r-j}f^{r^*}_{r-j})(f^m_0)$$

$$= \sum_{j=m-h}^{r} (-1)^j \varepsilon^j_t{}_{(r,r,r-t)} \left(\varepsilon^{r-j+h}_{r-j}{}_{(m,n,h)}\right)^2 f^m_0$$

By Remark 2.4.7, and Lemma 5.2.3, the matrix

$$\psi_{2t}(A_{2t}) = \sum_{j=0}^{m} (-1)^j \varepsilon^j_t{}_{(m,m,m-t)} f^m_{m-j} f^{m^*}_{m-j}$$

As by Corollary 5.2.4,

$$\Phi_{m,n,h}(A_{2t}) = \lambda_{2t}\psi_{2t}(A_{2t})$$

we get

$$\lambda_{2t} = \frac{\sum_{j=m-h}^{r} (-1)^j \varepsilon^j_t{}_{(r,r,r-t)} \left(\varepsilon^{r-j+h}_{r-j}{}_{(m,n,h)}\right)^2}{(-1)^m \varepsilon^m_t{}_{(m,m,m-t)}}$$

∎

For $m \in \mathbb{N}$, and $0 \leq t \leq m$, we have

$$\varepsilon^m_t{}_{(m,m,m-t)} = (-1)^{m-t} m! \sqrt{c_{m,m,m-t}}$$

Thus, the formula above for λ_{2t} can simplified:

Corollary 5.2.7. *Assuming the same hypothesis as in Proposition 5.2.6, the coefficient λ_{2t}, is given by*

$$\lambda_{2t} = \frac{\sum\limits_{j=m-h}^{r} (-1)^{t+j} \varepsilon_t^j{}_{(r,r,r-t)} \left(\varepsilon_{r-j}^{r-j+h}{}_{(m,n,h)}\right)^2}{m! \sqrt{c_{m,m,m-t}}}$$

Next we compute the coefficients λ_{2t} for some EPOSIC channels of small dimensions such as $EC(0, m)$, $EC(m, 0)$, $EC(1, m)$, and $EC(m, 1)$. Before doing so, some computational lemmas are needed, and can be proved easily using the equations in Corollary 2.3.16 and the identity $\sum\limits_{k=1}^{m} k = \frac{m(m+1)}{2}$.

Lemma 5.2.8. *Let $c_{m,n,h}$ be as defined in Theorem 2.2.4. For $m \in \mathbb{N}$, we have*

$$c_{m,m,m} = \frac{1}{m!(m+1)!} \qquad c_{0,m,0} = \frac{1}{(m!)^2} \qquad c_{m,m+1,m} = \frac{2}{m!(m+2)!}$$
$$c_{m,m-1,m-1} = \frac{2}{(m-1)!(m+1)!} \qquad c_{1,m-1,0} = \frac{1}{m!(m-1)!} \qquad c_{1,m+1,1} = \frac{(m+1)}{m!(m+2)!}$$
$$c_{m,m,m-1} = \frac{3}{(m-1)!(m+2)!} \qquad c_{1,m+1,1} = \frac{(m+1)}{m!(m+2)!} \qquad c_{1,m-1,0} = \frac{1}{m!(m-1)!}$$

Lemma 5.2.9. *Let $m \in \mathbb{N}$.* then

1. $\varepsilon_0^j{}_{(m,m,m)} = (-1)^j \sqrt{\frac{1}{m+1}}, \qquad \varepsilon_{m-j}^{m-j+1}{}_{(1,m+1,1)} = -\sqrt{\frac{m-j+1}{m+2}}$ for $0 \leq j \leq m$.

2. If $m \geq 1$, then

(a) $\varepsilon_{m-j}^{m-j}{}_{(1,m-1,0)} = \sqrt{\frac{j}{m}}$ for $1 \leq j \leq m$.

(b) $\varepsilon_0^j{}_{(m,m-1,m-1)} = (-1)^j \sqrt{\frac{2(j+1)}{m(m+1)}}$ for $0 \leq j \leq m-1$.

Example 5.2.10. Let $m \in \mathbb{N}$.

1. For the channel $\Phi_{m,m,m} : End(P_0) \longrightarrow End(P_m)$ the coefficient is $\lambda_0 = \frac{1}{\sqrt{m+1}}$.

2. For the channel $\Phi_{0,m,0} : End(P_m) \longrightarrow End(P_0)$ the coefficient is $\lambda_0 = \sqrt{m+1}$.

Proof:

1. By Corollary 5.2.7, we have $\lambda_0 = \frac{\varepsilon_0^0{}_{(0,0,0)}\left(\varepsilon_0^m{}_{(m,m,m)}\right)^2}{m!\sqrt{c_{m,m,m}}}$.

   As $\varepsilon_0^0{}_{(0,0,0)} = 1$, and $\varepsilon_0^m{}_{(m,m,m)} = \frac{(-1)^m}{\sqrt{m+1}}$, then by Lemma 5.2.8, we get

$$\lambda_0 = \frac{\sqrt{m!(m+1)!}}{(m+1)!} = \frac{1}{\sqrt{m+1}}$$

2. By Corollary 5.2.7, we have

$$\lambda_0 = \frac{\sum_{j=0}^{m}(-1)^j \varepsilon_0^j{}_{(m,m,m)} \left(\varepsilon_{m-j}^{m-j}{}_{(0,m,0)}\right)^2}{\sqrt{c_{0,0,0}}}$$

   As $\varepsilon_0^j{}_{(m,m,m)} = \frac{(-1)^j}{\sqrt{m+1}}$, $\varepsilon_{m-j}^{m-j}{}_{(0,m,0)} = 1$ and $c_{0,0,0} = 1$ then

$$\lambda_0 = \sum_{j=0}^{m} \frac{1}{\sqrt{m+1}} = \sqrt{m+1}$$

∎

Example 5.2.11. Let $m \in \mathbb{N}$.

1. For the channel $\Phi_{m,m+1,m} : End(P_1) \longrightarrow End(P_m)$ the coefficients are $\lambda_0 = \sqrt{\frac{2}{m+1}}$ and $\lambda_2 = -\sqrt{\frac{2m}{3(m+1)(m+2)}}$.

2. For the channel $\Phi_{m,m-1,m-1} : End(P_1) \longrightarrow End(P_m)$ the coefficients are $\lambda_0 = \sqrt{\frac{2}{m+1}}$ and $\lambda_2 = \sqrt{\frac{2(m+2)}{3m(m+1)}}$.

Proof:

For each of the channel $\Phi_{m,m+1,m}$ and $\Phi_{m,m-1,m-1}$, we compute $\{\lambda_{2t} : t = 0, 1\}$.

1. By Corollary 5.2.7, we have

$$\lambda_{2t} = \frac{\sum_{j=0}^{1}(-1)^{t+j}\varepsilon_t^j{}_{(1,1,1-t)} \left(\varepsilon_{1-j}^{m-j+1}{}_{(m,m+1,m)}\right)^2}{m!\,\sqrt{c_{m,m,m-t}}}$$

For $t = 0, 1$. Thus

$$\lambda_0 = \frac{\sum_{j=0}^{1}(-1)^{j}\varepsilon_0^j{}_{(1,1,1)} \left(\varepsilon_{1-j}^{m-j+1}{}_{(m,m+1,m)}\right)^2}{m!\,\sqrt{c_{m,m,m}}}$$

and

$$\lambda_2 = \frac{\sum_{j=0}^{1}(-1)^{j+1}\varepsilon_1^j{}_{(1,1,0)} \left(\varepsilon_{1-j}^{m-j+1}{}_{(m,m+1,m)}\right)^2}{m!\,\sqrt{c_{m,m,m-1}}}$$

For $0 \le j \le 1$, we have $\varepsilon_{1-j}^{m-j+1}{}_{(m,m+1,m)} = \beta_{1-j,m,m-j+1}^{m,m+1,m} = (-1)^m\sqrt{\frac{2j!(m-j+1)!}{(m+2)!}}$, and

$\varepsilon_0^j{}_{(1,1,1)} = \frac{(-1)^j}{\sqrt{2}}$, $\varepsilon_1^j{}_{(1,1,0)} = \frac{1}{\sqrt{2}}$, thus

$$\lambda_0 = \frac{\sqrt{2}\sum_{j=0}^{1} j!(m-j+1)!}{(m+2)!m!\,\sqrt{c_{m,m,m}}} = \frac{\sqrt{2}\,(m+2)m!}{(m+2)!m!\,\sqrt{c_{m,m,m}}} = \sqrt{\frac{2}{m+1}}$$

and

$$\lambda_2 = \frac{\sqrt{2}\sum_{j=0}^{1}(-1)^{j+1} j!(m-j+1)!}{m!(m+2)!\,\sqrt{c_{m,m,m-1}}} = \frac{\sqrt{2}\,(-m)m!}{m!(m+2)!\,\sqrt{c_{m,m,m-1}}} = -\sqrt{\frac{2m}{3(m+1)(m+2)}}$$

2. Similarly, we have

$$\lambda_{2t} = \frac{\sum_{j=1}^{1}(-1)^{t+j}\varepsilon_t^j{}_{(1,1,1-t)} \left(\varepsilon_{1-j}^{m-j}{}_{(m,m-1,m-1)}\right)^2}{m!\,\sqrt{c_{m,m,m-t}}}$$

$$= \frac{(-1)^{t+1}\varepsilon_t^1{}_{(1,1,1-t)} \left(\varepsilon_0^{m-1}{}_{(m,m-1,m-1)}\right)^2}{m!\,\sqrt{c_{m,m,m-t}}}$$

Thus

$$\lambda_0 = \frac{-\varepsilon_0^1{}_{(1,1,1)} \left(\varepsilon_0^{m-1}{}_{(m,m-1,m-1)}\right)^2}{m! \sqrt{c_{m,m,m}}} = \frac{\sqrt{2}}{(m+1)! \sqrt{c_{m,m,m}}} = \sqrt{\frac{2}{m+1}}$$

and

$$\lambda_2 = \frac{\varepsilon_1^1{}_{(1,1,0)} \left(\varepsilon_0^{m-1}{}_{(m,m-1,m-1)}\right)^2}{m! \sqrt{c_{m,m,m-1}}} = \frac{\sqrt{2}}{(m+1)! \sqrt{c_{m,m,m-1}}} = \sqrt{\frac{2(m+2)}{3m(m+1)}}$$

∎

Example 5.2.12. Let $m \in \mathbb{N}$.

1. For the channel $\Phi_{1,m+1,1} : End(P_m) \longrightarrow End(P_1)$ the coefficients are $\lambda_0 = \sqrt{\frac{m+1}{2}}$ and $\lambda_2 = -\sqrt{\frac{m(m+1)}{6(m+2)}}$.

2. For the channel $\Phi_{1,m-1,0} : End(P_m) \longrightarrow End(P_1)$ the coefficients are $\lambda_0 = \sqrt{\frac{m+1}{2}}$ and $\lambda_2 = \sqrt{\frac{(m+1)(m+2)}{6m}}$.

Proof:

1. As

$$\lambda_{2t} = \frac{\sum_{j=0}^{m} (-1)^{t+j} \varepsilon_t^j{}_{(m,m,m-t)} \left(\varepsilon_{m-j}^{m-j+1}{}_{(1,m+1,1)}\right)^2}{\sqrt{c_{1,1,1-t}}}$$

we have

$$\lambda_0 = \frac{\sum_{j=0}^{m} m-j+1}{(m+2)\sqrt{m+1}\sqrt{c_{1,1,1}}} = \frac{\sqrt{2}\sum_{j=0}^{m} m-j+1}{(m+2)\sqrt{m+1}} = \frac{\sqrt{2}}{(m+2)\sqrt{m+1}} \sum_{j=1}^{m+1} j = \sqrt{\frac{m+1}{2}}$$

and

$$\lambda_2 = \frac{\sum_{j=0}^{m} (-1)^{j+1} \varepsilon_1^j{}_{(m,m,m-1)} \left(\varepsilon_{m-j}^{m-j+1}{}_{(1,m+1,1)}\right)^2}{\sqrt{c_{1,1,0}}} = \sqrt{2} \sum_{j=0}^{m} \frac{(-1)^{j+1}(m-j+1)}{m+2} \varepsilon_1^j{}_{(m,m,m-1)}$$

$$= -\sqrt{6}\sum_{j=0}^{m}\frac{(m-j+1)(m-2j)}{(m+2)\sqrt{m(m+1)(m+2)}}$$

(see Lemma 2.4.11).

That is

$$\lambda_2 = -\frac{1}{(m+2)}\sqrt{\frac{6}{m(m+1)(m+2)}}\sum_{j=0}^{m}(m-j+1)(m-2j)$$

However

$$\sum_{j=0}^{m}(m-j+1)(m-2j) = \sum_{j=0}^{m}(m^2+m)-(3m+2)j+2j^2$$

$$= (m^2+m)(m+1)-(3m+2)\sum_{j=0}^{m}j+2\sum_{j=0}^{m}j^2$$

$$= (m^2+m)(m+1)-(3m+2)\sum_{j=0}^{m}j+2\sum_{j=0}^{m}j^2$$

$$= (m^2+m)(m+1)-(3m+2)\frac{m(m+1)}{2}+2\frac{m(m+1)(2m+1)}{6}$$

$$= \frac{m(m+1)(m+2)}{6}$$

Thus $\lambda_2 = -\sqrt{\frac{m(m+1)}{6(m+2)}}$.

2. As

$$\lambda_{2t} = \frac{\sum_{j=1}^{m}(-1)^{t+j}\varepsilon_t^j{}_{(m,m,m-t)}\left(\varepsilon_{m-j}^{m-j}{}_{(1,m-1,0)}\right)^2}{\sqrt{c_{1,1,1-t}}}$$

then

$$\lambda_0 = \frac{\sum_{j=1}^{m}(-1)^{j}\varepsilon_0^j{}_{(m,m,m)}\left(\varepsilon_{m-j}^{m-j}{}_{(1,m-1,0)}\right)^2}{\sqrt{c_{1,1,1}}} = \sqrt{\frac{2}{(m+1)}}\frac{1}{m}\sum_{j=1}^{m}j = \sqrt{\frac{m+1}{2}}$$

$$\lambda_2 = \frac{\sum_{j=1}^{m}(-1)^{j+1}\varepsilon_1^j{}_{(m,m,m-1)}\left(\varepsilon_{m-j}^{m-j}{}_{(1,m-1,0)}\right)^2}{\sqrt{c_{1,1,0}}}$$

$$= \frac{\sqrt{2}}{m}\sum_{j=1}^{m}(-1)^{j+1}j\varepsilon^{j}_{1\,(m,m,m-1)}$$

$$= \frac{-1}{m}\sqrt{\frac{6}{m(m+1)(m+2)}}\sum_{j=1}^{m}j(m-2j)$$

(see Lemma 2.4.11(2)),

As

$$\sum_{j=1}^{m}j(m-2j) = m\sum_{j=1}^{m}j - 2\sum_{j=1}^{m}j^2$$

$$= m\,\frac{m(m+1)}{2} - 2\,\frac{m(m+1)(2m+1)}{6} = \frac{-m(m+1)(m+2)}{6}$$

we get,

$$\lambda_2 = \sqrt{\frac{(m+1)(m+2)}{6m}}$$

∎

Part II

The Minimal Output Entropy and The Entanglement Breaking Property of EPOSIC Channels

Chapter 6

The Minimal Output Entropy and The Entanglement Breaking Property of Quantum Channels

6.1 The minimal output entropy of quantum channels

The existence of noise in all information processing systems affects the transmission of information over a quantum channel. A well-known measure of a channel performance is the Minimal Output Entropy (MOE). In this section, we give the definition of minimal output entropy, and exhibit some of its properties.

Recall that if H is a Hilbert space, then $D(H)$ denotes the set of all states of H, i.e.

$$D(H) = \{\varrho \in End(H) : \varrho \geq 0, tr(\varrho) = 1\}$$

Definition 6.1.1. *Let H be a Hilbert space. The von Neumann entropy is a map* *defined on the state space of H as following*

$$S : D(H) \longrightarrow \mathbb{R}$$

$$S(\varrho) = -tr(\varrho \log_{\mathbf{2}} \varrho)$$

where $\varrho \in D(H)$.

Remark 6.1.2. For a state ϱ, the von Neumann entropy $S(\varrho) = \sum_i -\lambda_i \log_2 \lambda_i$ where $\{\lambda_i\}_i$ are the eigenvalues of ϱ. By convention, $0 \log_2 0 = 0$.

Recall that a pure state ϱ of H is a rank one projection in $End(H)$. i.e. $\varrho = ww^*$for some unit vector $w \in H$.

Theorem 6.1.3. [27, Thm.11.8, Thm.11.10, Sec.11.3.5]

1. The von Neumann entropy is a concave non-negative function, which is zero if and only if the state is pure.

2. In a d dimensional Hilbert space H, the von Neumann entropy for a state of H is at most $\log_2 d$. It is $\log_2 d$ if and only if the state is the maximal mixed state $\frac{I_d}{d}$.

Lemma 6.1.4. *[27, p.514] Let H and K be Hilbert spaces. For $\sigma_1 \otimes \sigma_2 \in D(H \otimes K)$, we have*

$$S(\sigma_1 \otimes \sigma_2) = S(\sigma_1) + S(\sigma_2)$$

Definition 6.1.5. *(The Minimal Output Entropy) Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel. The minimal output entropy (MOE), is defined by*

$$S_{min}(\Phi) = \min\{S(\Phi(\varrho)) : \varrho\, is\, a\, pure\, state\}$$

where S is the von Neumann entropy.

Remark 6.1.6. In the definition of minimal output entropy [24, 25], the minimum is taken over all the states in H. However, by the concavity of von Neumann entropy, the minimal output entropy will be achieved on a pure state.

Notation 6.1.7. Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel with Kraus operators $\{T_j : 1 \leq j \leq n\}$. For a pure state $\varrho = ww^*$ of H, let $U_{\Phi,\varrho}$ denote the set $\{u_j = T_j w \,: 1 \leq j \leq n\}$.

Remark 6.1.8. With the notation of 6.1.7, for a channel $\Phi : End(H) \longrightarrow End(K)$, and a pure state $\varrho = ww^*$ of H, we have

$$\Phi(ww^*) = \sum_{j=1}^{n} T_j w_j \,(T_j w)^* = \sum_{j=1}^{n} u_j u_j^*$$

is a state of K. Hence, the set $U_{\Phi,\varrho}$ must contain a nonzero vector.

The following lemma can be proved easily by contradiction.

Lemma 6.1.9. *Let H be a Hilbert space, and u, v are non zero vectors of H. If u and v are linearly independent, then uu^* and vv^* are linearly independent in $End(H)$.*

Proposition 6.1.10. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel. Then*

1. $S_{min}(\Phi) = 0$ if and only if there exist a pure state ϱ of H such that $\Phi(\varrho)$ is a pure state.

2. *If for each pure state ϱ of H, the set $U_{\Phi,\varrho}$ contains at least two linearly independent vectors, then $S_{min}(\Phi) \neq 0$.*

Proof:

By continuity of the von Neumann entropy, and compactness of the set of states [41, p.29], the minimum entropy is achieved. Thus, if $S_{min}(\Phi) = 0$ then there is a state ϱ such that $S(\Phi(\varrho)) = 0$. By Theorem 6.1.3, $\Phi(\varrho)$ is a pure state. The other direction follows from the definition of $S_{min}(\Phi)$. To show the second statement, let ϱ be a pure state. Since the set $U_{\Phi,\varrho}$ has at least two linearly independent vectors, then by Lemma 6.1.9, $\Phi(\varrho) = \sum_{u_j \in U_\varrho} u_j u_j^*$ has rank at least two. Hence, $\Phi(\varrho)$ is not pure for any pure state ϱ. The result follows from this and the first statement. ∎

Recall the definition of separable and entangled states, given in Definition 3.2.5.

Proposition 6.1.11. *Let H, K and E be Hilbert spaces.*

1. *If $\alpha : H \longrightarrow K \otimes E$ is an isometry, then the state $\alpha\varrho\alpha^* \in D(K \otimes E)$ is a pure state for any pure state $\varrho \in D(H)$.*

2. *Any separable pure state $\varrho \in D(K \otimes E)$ is a product of pure states.*

   i.e. $\exists\, \sigma_1 \in \mathcal{P}(K)$ and $\sigma_2 \in \mathcal{P}(E)$ such that $\varrho = \sigma_1 \otimes \sigma_2$.

Proof:

Let ϱ be a pure state. It straightforward to show that $\alpha\varrho\alpha^*$ is a state, we also have $(\alpha\varrho\alpha^*)^2 = \alpha\varrho\alpha^*\alpha\varrho\alpha^* = \alpha\varrho\alpha^*$, and $(\alpha\varrho\alpha^*)^* = \alpha\varrho\alpha^*$. Thus $\alpha\varrho\alpha^*$ is a projection, moreover $rank(\alpha\varrho\alpha^*) \leq \min\{rank(\alpha), rank(\varrho), rank(\alpha^*)\} \leq rank(\varrho) = 1$. Since there is no state with rank zero, the state $\alpha\varrho\alpha^*$ must have rank one.

For the second statement, assume that ϱ is a pure state such that $\varrho = \sum_k \lambda_k \varrho_k$, a convex combination of product states ϱ_k. Since any pure state is an extreme point in the set of the states [41, p.29], $\varrho = \varrho_k$ for each k. That is $\varrho = \sigma_1 \otimes \sigma_2$ for some $\sigma_1 \in D(K)$ and $\sigma_2 \in \mathcal{D}(E)$. By Theorem 6.1.3, and Lemma 6.1.4, we have

$$0 = S(\varrho) = S(\sigma_1) + S(\sigma_2)$$

hence $S(\sigma_1) = S(\sigma_2) = 0$, and both σ_1, and σ_2 are pure.

∎

Corollary 6.1.12. *Let H,K and E be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel with Stinespring representation (E, α). If Φ has nonzero minimal output entropy then for any pure state $\varrho \in D(H)$, the state $\alpha\varrho\alpha^* \in D(K \otimes E)$ is entangled.*

Proof:

Let ϱ be a pure state, and assume to the contrary that $\alpha\varrho\alpha^*$ is a separable state. By Proposition 6.1.11, there exist pure states $\sigma_1 \in \mathcal{P}(K)$, $\sigma_2 \in \mathcal{P}(E)$ such that $\alpha\varrho\alpha^* = \sigma_1 \otimes \sigma_2$. Consequently, $\Phi(\varrho) = Tr_E(\alpha\varrho\alpha^*) = Tr_E(\sigma_1 \otimes \sigma_2) = \sigma_1$ is pure. By Proposition 6.1.10, we get $S_{min}(\Phi) = 0$. ∎

6.2 The entanglement breaking property of quantum channels

A property of quantum channels that has been studied, and used to classify them is the elimination of entanglement between the input states of composite systems, see Definition 3.2.5. Channels having this property are called Entanglement Breaking. Here is a description by P. Shor [34] of the entanglement breaking channels.

> " Entanglement breaking channels are channels which destroy entanglement with other quantum systems. That is, when the input state is entangled between the input space H_{in} and another quantum system H_{ref} , the output of the channel is no longer entangled with the system H_{ref} ."

Recall that by Definition 3.2.5, the separable state in a composite system is a convex combination of product states.

Definition 6.2.1. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a completely positive map. We say Φ is entanglement breaking if $\Phi \otimes I_n(\varrho)$ is always* *separable for any $\varrho \in D(H \otimes \mathbb{C}^n)$, and for any $n \in \mathbb{N}$. An entanglement breaking trace preserving map is abbreviated as E.B.T.*

One checks easily (see [20, Thm.3]) that the set of entanglement breaking channels is a convex set. For a completely positive map Φ, it is evident that the state $\Phi \otimes I_n(\varrho)$ is separable for any separable state ϱ, so Φ will be entanglement breaking if $\Phi \otimes I_n$ maps any entangled state to a separable one. The next proposition is due to [20, Thm.4], see also [16, Pro.6.22, Pro.6.32].

Proposition 6.2.2. *Let H and K be Hilbert spaces. If $\Phi : End(H) \longrightarrow End(K)$ is a completely positive map, then the following statements are equivalent*

1. *Φ is entanglement breaking;*
2. *$\Phi \otimes I_n(uu^*)$ is separable, where $u = \frac{1}{\sqrt{d_H}} \sum_{i=1}^{d_H} e_i \otimes e_j$, and $\{e_i : 1 \leq i \leq d_H\}$ is an orthonormal basis for H;*
3. *Φ can be written in operator sum form using only Kraus operators of rank one.*

Recall the definition of the Choi-Jamiolkowski map, given in 1.2.26. By Lemma 1.2.30, we have $\Phi \otimes I_n(uu^*) = \frac{1}{d_H} C(\Phi)$, where $u = \frac{1}{\sqrt{d_H}} \sum_{i=1}^{d_H} e_i \otimes e_i$.

Corollary 6.2.3. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a completely positive map. The map Φ is entanglement breaking if and only if $\frac{1}{d_H} C(\Phi)$ is separable, where $C(\Phi)$ is the Choi matrix of Φ.*

The proof of the next lemma requires knowledge of the entanglement distillation, and its relation with separability, see [22], and the introduction in [4]. Assuming this, the next lemma follows from [21, Thm.1].

Lemma 6.2.4. *Let H and K be Hilbert spaces. For $\varrho \in D(H \otimes K)$, let $\varrho_H = Tr_K(\varrho)$, and $\varrho_K = Tr_H(\varrho)$ be the reduced density operators of ϱ on the subsystems H and K respectively. If $rank(\varrho) < \max\{rank(\varrho_H), rank(\varrho_K)\}$, then ϱ is not separable.*

The next proposition follows from Lemma 6.2.4, and Corollary 6.2.3. Recall that if Φ is a quantum channel Φ, then by Theorem 3.2.20, we have $Tr_K(C(\Phi)) = I_{\overline{H}}$.

Proposition 6.2.5. *Let H and K be Hilbert spaces of dimension d_H and d_K respectively. Let $\Phi : End(H) \to End(K)$ be a quantum channel with Choi matrix $C(\Phi)$. If $rank\,(C(\Phi)) < \max\{d_H, rank(Tr_{\overline{H}}(C(\Phi)))\}$ then Φ is not E.B.T*

The following statement, which is generalization of Theorem 6 of [20], is a corollary of both Proposition 6.2.5, and Corollary 3.2.23.

Corollary 6.2.6. *Let H and K be Hilbert spaces of dimension d_H and d_K respectively. If $\Phi : End(H) \to End(K)$ is a quantum channel, which can be written using Kraus operators fewer than $max\{d_H, rank(Tr_{\overline{H}}(C(\Phi))\}$ then Φ is not E.B.T.*

Recall by Proposition 4.5.4 that if $\{T_i : 1 \leq i \leq d\}$ are Kraus operators of a completely positive map Φ, then $\{T_i^* : 1 \leq i \leq d\}$ are Kraus operators of its dual map Φ^*.

Proposition 6.2.7. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a completely positive map. The map Φ is entanglement breaking if and only if its dual map Φ^* is entanglement breaking.*

Proof:

Assume that Φ is entanglement breaking, so by Proposition 6.2.2, there exist Kraus operators $\{T_j : 1 \leq j \leq k\}$ of Φ such that $rank(T_j) = 1$ for all $1 \leq j \leq k$. Since $T_j = uv^* \Longleftrightarrow T_j^* = vu^*$, then By Proposition 4.5.4, the map Φ^* has Kraus operators $\{T_i^* : 1 \leq i \leq d\}$ such that $rank(T_j^*) = 1$. Hence, it is entanglement breaking. By exchanging the role of Φ and Φ^*, the result follows. ∎

6.3 The additivity of the classical capacity of quantum channels

In this section, we justify the importance of studying the minimal output entropy, and the E.B.T property for a quantum channel. This section can be skipped with no impact on the rest of the thesis. The channel's capacity is defined to be the maximal rate of reliable communication through a channel [27, p.547]. In [2] Bennett and Shor classified three distinct capacities of a quantum channel. One of the important open questions is that of determining the capability of the channel to transmit classical information, which is known as the classical capacity of the channel. The Holevo capacity (product state capacity) is defined to be the classical capacity for the channel with the restriction that there are no entangled input states are allowed across many uses of the channel, see [27, p.554]. A fundamental result of quantum information theory, "The quantum coding theorem" [18], and [32], implies that the classical capacity of a quantum channel Φ is given by

$$\lim_{n\to\infty} \frac{\mathfrak{C}_\chi(\Phi^{\otimes n})}{n}$$

where $\mathfrak{C}_\chi$denotes the Holevo capacity.

In their attempts to increase the capacity of quantum channels, scientists studied whether running two channels in parallel will increase the total classical capacity of the two channels. Failing to do so, the capacity is called additive. In general, we have the following definition:

Definition 6.3.1. *Let $Q : \{\Phi : \Phi$ is a quantum channel $\} \longrightarrow \mathbb{R}$ be a map defined on the set of quantum channels. Then Q is said to be additive if*

$$Q(\Phi_1 \otimes \Phi_2) = Q(\Phi_1) + Q(\Phi_2)$$

for all quantum channels Φ_1 and Φ_2.

If the Holevo capacity is additive, then for the independent use for many copies of a quantum channel Φ, we have $\mathfrak{C}_\chi(\Phi^{\otimes n}) = n \cdot \mathfrak{C}_\chi(\Phi)$. This implies the coincidence between the classical capacity and Holevo capacity, and consequently implies the additivity of the classical capacity. The following proposition is an outstanding result of P. Shor in [36].

Proposition 6.3.2. *The Holevo capacity $\mathfrak{C}_\chi$ is additive if and only if the minimal output entropy S_{min} is additive.*

A conjecture that lasted many years was that the Holevo capacity is additive. Much research effort was directed to prove this conjecture, and for some special classes of quantum channels the additivity of minimal output entropy was proved. For example, tensoring the identity with any channel [1], the unital qubit channel [24], the depolarizing quantum channel [26], the phase damping channels [26], and the entanglement breaking channels [34]. However, an outstanding paper in 2008 by Hastings [11] disproved this conjecture. By giving a randomized construction of channels that violate the additivity of the minimal output entropy, he was able to show the existence of a channel Φ such that $S_{min}(\Phi \otimes \overline{\Phi}) \neq S_{min}(\Phi) + S_{min}(\overline{\Phi})$. Since then, the efforts redirected towards constructing an explicit example for the non-additivity of the minimal output entropy.

Proposition 6.3.3. *[17] For an independent use of quantum channels, the minimal output entropy is sub-additive. That is, if Φ_1, Φ_2 are two quantum channels that are used independently, then*

$$S_{min}(\Phi_1 \otimes \Phi_2) \leq S_{min}(\Phi_1) + S_{min}(\Phi_2)$$

The following proposition summarizes some results in both [15, p.95] and [34]. It presents special cases where the additivity of MOE holds.

Proposition 6.3.4. *Let Φ be a quantum channel such that $S_{min}(\Phi) = 0$ or Φ is an E.B.T channel. Then, for any arbitrary channel Ψ, we have*

$$S_{min}(\Phi \otimes \Psi) = S_{min}(\Psi \otimes \Phi) = S_{min}(\Phi) + S_{min}(\Psi)$$

Chapter 7

The Minimal Output Entropy and The Entanglement Breaking Property of EPOSIC Channels

The main results of this chapter:

- Proving that the minimal output entropy of EPOSIC channel is zero if only and only if the index h in $\Phi_{m,n,h}$ is zero (Proposition 7.1.1, and Corollary 7.1.7).
- Computing $S_{min}(\Phi_{m,1,1})$ for $m \in \mathbb{N}$ (Corollary 7.2.6).
- Finding a lower bound of the minimal output entropy of an element in $QC(P_1, P_m)^{SU(2)}$ (Proposition 7.2.13).
- Examining the E.B.T property of EPOSIC channels (Section 7.3).

7.1 The minimal output entropy of EPOSIC channel

In this section, we determine the EPOSIC channels with zero minimal output entropy. Recall that for $m \in \mathbb{N}$, the channel $\Phi_{m,0,0}$ is the identity channel on $End(P_m)$, and the channel $\Phi_{0,m,0} : End(P_m) \longrightarrow End(P_0)$ is given by $\Phi_{0,m,0}(A) = tr(A)$. As both takes a pure state to a pure state, both have a zero minimal output entropy. More generally, we have the following proposition:

Proposition 7.1.1. *For $m, n \in \mathbb{N}$, the channel $\Phi_{m,n,0}$ has zero minimal output entropy.*

Proof:

By Corollary 4.2.7, we have

$$\Phi_{m,n,0}(f_0^r f_0^{r^*}) = \sum_{j=0}^{0} \left(\varepsilon^j_{0\,(m,n,,0)}\right)^2 f^m_{l_{0j}} f^{m^*}_{l_{0j}} = f_0^m f_0^{m^*}$$

where $r = m + n$, and $\{f_i^k : 0 \le i \le k\}$ is the standard basis for P_k, $k \in \mathbb{N}$. The result follows by Proposition 6.1.10. ∎

Next, we show that the minimal output entropy of $\Phi_{m,n,h}$ is not zero if $h > 0$. The following lemma can be proved by direct computation using the formula in Corollary 2.3.13.

$$\varepsilon^j_{i\,(m,n,h)} = \sum_{s=\max\{0,j-i,j+h-n\}}^{\min\{h,j,j+m-i-h\}} \beta^{m,n,h}_{i,s,j}$$

Lemma 7.1.2. *For $m, n, h \in \mathbb{N}$ with $0 \le h \le \min\{m, n\}$ and $j \in B(i)$, let $\varepsilon_i^j := \varepsilon^j_{i\,(m,n,h)}$ and $r = m + n - 2h$, then we have:*

1. *$\varepsilon_i^0 \neq 0$, for $0 \le i \le m - h$;*

2. *$\varepsilon_i^{i-m+h} \neq 0$, for $m - h \le i \le r$;*

3. $\varepsilon_i^{i+h} \neq 0, \qquad$ *for* $0 \leq i \leq n-h$;

4. $\varepsilon_i^{n} \neq 0, \qquad$ *for* $n-h \leq i \leq r$.

Lemma 7.1.3. *Let* $m, n, h \in \mathbb{N}$ *with* $0 < h \leq \min\{m, n\}$*, and* $r = m+n-2h$*. For any* $0 \leq i \leq m+n-2h$*, we have*

$$\max\{0, -m+i+h\} < \min\{i+h,\, n\}.$$

Proof:

Let

$$j_1 = \max\{0, -m+i+h\} = \begin{cases} 0 & if \quad 0 \leq i \leq m-h \\ i-m+h & if \quad m-h \leq i \leq r \end{cases}$$

and

$$j_2 = \min\{i+h,\, n\} = \begin{cases} i+h & if \quad 0 \leq i \leq n-h \\ n & if \quad n-h \leq i \leq r \end{cases}$$

If $j_1 = 0$, then $j_1 < h \leq j_2$. Otherwise,

$$j_1 = i-(m-h) \leq \min\{i,\, r-m+h\} = \min\{i,\, n-h\} < \min\{i+h,\, n\} = j_2$$

∎

Recall the definition of $B(i) = \{j : \max\{0, -m+i+h\} \leq j \leq \min\{i+h,\, n\}\}$ in Notation 2.3.10.

Corollary 7.1.4. *For* $m, n, h \in \mathbb{N}$ *with* $0 < h \leq \min\{m, n\}$*, let* $r = m+n-2h$*. For each* $0 \leq i \leq r$*, there exist* $j_1, j_2 \in B(i)$ *such that* $j_1 < j_2$*, and*

$$\varepsilon_i^{j_1} \neq 0, \qquad \varepsilon_i^{j_2} \neq 0$$

Proof:

Let $j_1 = \max\{0, -m+i+h\}$ and $j_2 = \min\{i+h, n\}$. Both $j_1, j_2 \in B(i)$, and by Lemma 7.1.3 we have $j_1 < j_2$. By Lemma 7.1.2, both $\varepsilon_i^{j_1} \neq 0$ and $\varepsilon_i^{j_2} \neq 0$. ∎

Recall by Remark 4.2.3 that EPOSIC Kraus operators of $\Phi_{m,n,h}$ are given by

$$T_j = \sum_{i=\max\{0,j-h\}}^{\min\{r,m+j-h\}} \varepsilon_i^j \, f_{l_{ij}}^m f_i^{r^*}$$

for $0 \leq j \leq n$. Recall also by Notation 6.1.7, that for a quantum channel Φ with Kraus operators $\{T_j : 1 \leq j \leq n\}$, and for a pure state $\varrho = ww^*$ of H, the set $U_{\Phi,\varrho}$ denotes the vectors $\{u_j = T_j w : 1 \leq j \leq n\}$. The proof of the following lemma is via direct computation.

Lemma 7.1.5. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, $r = m+n-2h$, and $\{T_j : 0 \leq j \leq n\}$ be the EPOSIC Kraus operators of $\Phi_{m,n,h}$. For $w = \sum_{i=0}^{m+n-2h} w_i f_i^r \in P_{m+n-2h}$, we have*

$$T_j w = \sum_{i=\max\{0,j-h\}}^{\min\{r,m-h+j\}} w_i \varepsilon_i^j f_{i-j+h}^m$$

Proposition 7.1.6. *Let $m, n, h \in \mathbb{N}$ with $0 < h \leq \min\{m, n\}$, and $\Phi_{m,n,h}$ be the associated EPOSIC channel. For any pure state $\varrho \in End(P_{m+n-2h})$, the set $U_{\Phi_{m,n,h},\varrho}$ contains at least two linearly independent vectors.*

Proof:

Let $r = m+n-2h$ and ϱ be any pure state in $End(P_r)$. By Remark 3.2.4, $\varrho = ww^*$ for some unit vector $w \in P_r$. i.e

$$w = \sum_{i=0}^{r} w_i f_i^r, \qquad \sum_{i=0}^{r} |w_i|^2 = 1$$

Pick i_1 minimal so that $w_{i_1} \neq 0$. By Corollary 7.1.4, there exist $j_1 < j_2 \in B(i_1)$ such that $\varepsilon_{i_1}^{j_1} \neq 0$ and $\varepsilon_{i_1}^{j_2} \neq 0$. Since $j \in B(i_1) \iff \max\{0, j-h\} \leq i_1 \leq \min\{r, m-h+j\}$, then by Lemma 7.1.5, we have

$$u_{j_1} = T_{j_1} w = \sum_{i=\max\{0, j_1 - h\}}^{\min\{r, m-h+j_1\}} w_i \varepsilon_i^{j_1} f_{i-j_1+h}^m \neq 0$$

and

$$u_{j_2} = T_{j_2} w = \sum_{i=\max\{0, j_2 - h\}}^{\min\{r, m-h+j_2\}} w_i \varepsilon_i^{j_2} f_{i-j_2+h}^m \neq 0$$

If $U_{\Phi_{m,n,h},\varrho} = \{u_j : 0 \leq j \leq n\}$ doesn't contain two linearly independent vectors, then there exist $\alpha \neq 0$ such that $u_{j_2} = \alpha u_{j_1}$. In particular, comparing the coefficients of $f_{i_1 - j_2 + h}^m$, we obtain

$$0 \neq w_{i_1} \varepsilon_{i_1}^{j_2} = \alpha w_{i_2} \varepsilon_{i_2}^{j_1}$$

for some i_2, where $i_1 - j_2 + h = i_2 - j_1 + h$. i.e. $i_2 = i_1 - (j_2 - j_1) < i_1$ and $w_{i_2} \neq 0$, contradicting the minimality of i_1. ∎

The following corollary follows directly from the last proposition and Proposition 6.1.10.

Corollary 7.1.7. *Let* $m, n, h \in \mathbb{N}$ *with* $0 \lneqq h \leq \min\{m, n\}$*. Then* $S_{min}(\Phi_{m,n,h})$ *is nonzero.*

By the last corollary and Corollary 6.1.12, we have:

Corollary 7.1.8. *Let* $m, n, h \in \mathbb{N}$ *with* $0 \lneqq h \leq \min\{m, n\}$*. For any pure state* $\varrho \in D(P_{m+n-2h})$*, the state* $\alpha_{m,n,h} \varrho \alpha_{m,n,h}^* \in D(P_m \otimes P_n)$ *is a pure entangled.*

7.2 Examples and special cases

In this section, we give a systematic method to compute the minimal output entropy of $\Phi_{m,n,n}$, for $m, n \in \mathbb{N}$, and compute $S_{min}(\Phi_{m,1,1})$. We also give a bound for $S_{min}(\Phi)$, where $\Phi : End(P_1) \longrightarrow End(P_m)$ is an $SU(2)$-irreducibly covariant channel.

7.2.1 The minimal output entropy of $\Phi_{m,1,1}$

Lemma 7.2.1. *Let K be a finite dimensional Hilbert space, and $A \in End(K)$ such that $A = \sum_{j=1}^{n} u_j u_j^*$. If $\{u_j : 1 \le j \le n\}$ are linearly independent vectors in K, then there exist a basis for K such that the matrix represents A is in the form*

$$\begin{pmatrix} \langle u_1 | u_1 \rangle & \langle u_1 | u_2 \rangle & \cdots & \langle u_1 | u_n \rangle & 0 & \cdots & 0 \\ \langle u_2 | u_1 \rangle & \langle u_2 | u_2 \rangle & \cdots & \langle u_2 | u_n \rangle & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \langle u_n | u_1 \rangle & \langle u_n | u_2 \rangle & \cdots & \langle u_n | u_n \rangle & 0 & \cdots & 0 \\ 0 & 0 & & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & & 0 & 0 & \cdots & 0 \end{pmatrix}$$

A matrix in a such form is called Gram matrix.

Proof:

Let $\{u_{n+1}, u_{n+2}, ...u_{d_k}\}$ be a basis for the orthogonal subspace on $span\{u_j : 1 \le j \le n\}$ and $\mathcal{U} = \left\{u_1, u_2, ..., u_n, u_{n+1}, ...u_{d_k}\right\}$. The set $\mathcal{U}$ forms a basis for K. For each $u_k \in \mathcal{U}$, we have

$$Au_k = \sum_{j=1}^{n} u_j u_j^* (u_k) = \begin{cases} \sum_{j=1}^{n} \langle u_j | u_k \rangle u_j & if \quad 1 \le k \le n \\ 0 & if \quad k > n \end{cases}$$

The result follows by writing the matrix for A with respect to the basis $\mathcal{U}$. ∎

Corollary 7.2.2. *Let $m, n \in \mathbb{N}$ with $n \le m$, and ϱ be a pure state of P_{m-n}. The matrix representing $\Phi_{m,n,n}(\varrho)$ is in the form of a Gram matrix.*

Proof:

Let $\{T_j : 0 \leq j \leq n\}$ be the EPOSIC Kraus operators of $\Phi_{m,n,n} : End(P_{m-n}) \longrightarrow End(P_m)$, and $\varrho = ww^*$ where w is a unit vector in P_{m-n}. By Remark 6.1.8,

$$\Phi_{m,n,n}(\varrho) = \Phi_{m,n,n}(ww^*) = \sum_{j=0}^{n} u_j u_j^*$$

where $u_j = T_j w$. By Lemma 7.1.5,

$$u_j = T_j w = \sum_{i=0}^{m-n} w_i \varepsilon_i^j f_{i-j+n}^m = \sum_{k=n-j}^{m-j} w_{k+j-n} \varepsilon_{k+j-n}^j f_k^m$$

where $\varepsilon_i^j = \varepsilon_{i\,(m,n,n)}^j$. As the coefficients $\varepsilon_{i\,(m,n,n)}^j$ are nonzero (Corollary 2.3.15 (6)), it is clear that the set $\{u_j : 0 \leq j \leq n\}$ is linearly independent. The result follows by Lemma 7.2.1. ∎

Theoretically, we are now able to compute the minimal output entropy for $\Phi_{m,n,n}$ by computing the eigenvalues of the Gram matrix of $\Phi_{m,n,n}(\varrho)$ for any pure state ϱ, see Definition 6.1.5, and Remark 6.1.2. Due to the complicated computations, we only find the minimal output entropy of $\Phi_{m,1,1}$. Recall that for $m \in \mathbb{N} \setminus \{0\}$, the channel $\Phi_{m,1,1} : End(P_{m-1}) \longrightarrow End(P_m)$ has only two EPOSIC Kraus operators $\{T_0, T_1\}$, where $T_j : P_{m-1} \longrightarrow P_m,\ j = 1, 2$ as given in Definition 4.2.1. Let $\varrho = ww^*$ be a pure state in $End(P_{m-1})$, and $u_0 = T_0 w$, $u_1 = T_1 w$. By Corollary 7.2.2, there is exist a basis for P_m such that the matrix $\Phi_{m,1,1}(\varrho)$ is given by

$$\begin{pmatrix} \langle u_0 | u_0 \rangle & \langle u_0 | u_1 \rangle & 0 & \cdots & 0 \\ \langle u_1 | u_0 \rangle & \langle u_1 | u_1 \rangle & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Using the same notation above, we have

Proposition 7.2.3. *Let $m \in \mathbb{N} \setminus \{0\}$ and ww^* be a pure state in $End(P_{m-1})$. The eigenvalues of $\Phi_{m,1,1}(ww^*)$ are* $\{0, \lambda_1, \lambda_2\}$, where

$$\lambda_{1,2} = \frac{1 \pm \sqrt{1-4R}}{2}$$

with $R = \|u_0\|^2 \|u_1\|^2 - |\langle u_0 | u_1 \rangle|^2$.

The proof of the following lemma is purely computational, and is provided in Appendix **B**.

Lemma 7.2.4. *Let $m \in \mathbb{N} \setminus \{0\}$. Using the above notations, the minimal value of $\|u_0\|^2 \|u_1\|^2 - |\langle u_0 | u_1 \rangle|^2$ is $\frac{m}{(m+1)^2}$.*

Remark 7.2.5. Using Cauchy Schwartz inequality and Lemma 7.2.4, we have $0 \leq 1 - 4R \leq 1$ holds for any $m \geq 1$ which affirms that $\lambda_{1,2}$ are non-negative numbers.

By concavity of von Neumann entropy [27, p.516] and [41, Prop.13.4], we have that the von Neumann entropy of $\Phi_{m,1,1}(ww^*)$ achieves its minimum when the difference between λ_1 and λ_2 is maximal, this is when R is minimal. Consequently, by Remark 6.1.2, we get:

Corollary 7.2.6. *Let $m \in \mathbb{N} \setminus \{0\}$. Then*

$$S_{min}(\Phi_{m,1,1}) = -[\frac{1}{m+1} \log_2 \frac{1}{m+1} + \frac{m}{m+1} \log_2 \frac{m}{m+1}]$$

with the minimal output entropy achieved at the state $\varrho = f_0^{m-1} f_0^{m-1^*}$.

7.2.2 Lower bound of the minimal output entropy of an element in $QC(P_1, P_m)^{SU(2)}$

Recall that the set $QC(P_1, P_m)^{SU(2)}$ consists of all $SU(2)$-irreducibly covariant channels $\Phi : End(P_1) \longrightarrow End(P_m)$, and it is the convex hull of the EPOSIC channels

$EC(1,m)$ (Proposition 5.1.2). In this subsection, we find a lower bound of the minimal output entropy for these channels assuming $m \geq 5$. We begin by recalling some results from Chapter 4. The following lemma is a reformulation of the result in Lemma 4.6.1.

Lemma 7.2.7. *Let $m \in \mathbb{N}$ and $\Phi : End(P_1) \longrightarrow End(P_m)$ be an $SU(2)$-equivariant map. For a unit vector w in P_1, the states $\Phi(ww^*)$ and $\Phi(f_0^1 f_0^{1^*})$ have the same eigenvalues.*

Corollary 7.2.8. *Let $m \in \mathbb{N}$ and $\Phi : End(P_1) \longrightarrow End(P_m)$ be an $SU(2)$-covariant channel. Then*

$$S_{min}(\Phi) = S(\Phi(f_0^1 f_0^{1^*}))$$

By Lemma 4.6.2, we have

Example 7.2.9. Let $m \in \mathbb{N} \setminus \{0\}$. Then

1. $S_{min}(\Phi_{m,m+1,m}) = -\sum_{j=1}^{m+1} \frac{2j}{(m+1)(m+2)} \log_2 \frac{2j}{(m+1)(m+2)}$.
2. $S_{min}(\Phi_{m,m-1,m-1}) = -\sum_{j=1}^{m} \frac{2j}{m(m+1)} \log_2 \frac{2j}{m(m+1)}$.

Proposition 7.2.10. *Let $m \in \mathbb{N} \setminus \{0\}$, and $\Phi : End(P_1) \longrightarrow End(P_m)$ be an $SU(2)$-covariant channel. There exists $0 \leq p \leq 1$ such that the eigenvalues of $\Phi(f_0^1 f_0^{1^*})$ are*

$$\Big\{\lambda_j = \tfrac{2(m-j+1)}{(m+1)(m+2)}p + \tfrac{2j}{m(m+1)}(1-p),\ 0 \leq j \leq m\Big\}.$$

Proof:

Since $\Phi \in QC(P_1, P_m)^{SU(2)}$, then by Proposition 5.1.2, there exists $0 \leq p \leq 1$ such that

$$\Phi = p\Phi_{m,m+1,m} + (1-p)\Phi_{m,m-1,m-1}$$

By linearity of Φ, and by Lemma 4.6.2, we have

$$\Phi(f_0^1 f_0^{1^*}) = p\Phi_{m,m+1,m}(f_0^1 f_0^{1^*}) + (1-p)\Phi_{m,m-1,m-1}(f_0^1 f_0^{1^*})$$

$$= \frac{2p}{m+2} f_m^m f_m^{m^*} + \sum_{j=1}^{m} \left[\frac{2p(m-j+1)}{(m+1)(m+2)} + \frac{2(1-p)j}{m(m+1)} \right] f_{m-j}^m f_{m-j}^{m^*}$$

$$= \sum_{j=0}^{m} \left[\frac{2p(m-j+1)}{(m+1)(m+2)} + \frac{2(1-p)j}{m(m+1)} \right] f_{m-j}^m f_{m-j}^{m^*}$$

∎

By the above proposition, Corollary 7.2.8, and Remark 6.1.2, we have

Corollary 7.2.11. *Let $m \in \mathbb{N}$, and $\Phi : End(P_1) \longrightarrow End(P_m)$ be an $SU(2)$-covariant channel. There exists $0 \leq p \leq 1$ such that*

$$S_{min}(\Phi) = -\sum_{j=0}^{m} \lambda_j \log_2 \lambda_j$$

where $\lambda_j = \frac{2(m-j+1)}{(m+1)(m+2)}p + \frac{2j}{m(m+1)}(1-p)$.

Remark 7.2.12. The map $-x \ln x$ is increasing on $[0, \frac{1}{e}]$, and its integral $\frac{x^2}{4} - \frac{x^2 \ln x}{2}$ is an increasing map on $[0,1]$. Recall that by convention, $0 \ln 0 = 0$.

Proposition 7.2.13. *Let $m \in \mathbb{N}$ such that $m \geq 5$, and $\Phi : End(P_1) \longrightarrow End(P_m)$ be an $SU(2)$-covariant channel. Then*

$$S_{min}(\Phi) \geq \frac{1}{4ln2} \frac{(m-2)^2}{m^2(m+1)^2}$$

Proof:

By Corollary 7.2.11,

$$S_{min}(\Phi) = \frac{-1}{\ln 2} \sum_{j=0}^{m} \lambda_j \ln \lambda_j$$

where

$$\lambda_j = \frac{2(m-j+1)}{(m+1)(m+2)}p + \frac{2j}{m(m+1)}(1-p).$$

Let $f(x) = -x \ln x$, $g(x) = \int f(x)dx = \frac{x^2}{4} - \frac{x^2 \ln x}{2}$, $x_j = \frac{2(m-j+1)}{(m+1)(m+2)}$, and $y_j = \frac{2j}{m(m+1)}$. As

$x_j \leq \frac{2(m+1)}{(m+1)(m+2)} = \frac{2}{m+2}$ and $y_j \leq \frac{2m}{m(m+1)} = \frac{2}{m+1}$. For $m \geq 5$, we have

$$0 \leq \min\{x_j, y_j\} \leq px_j + (1-p)y_j \leq \max\{x_j, y_j\} \leq \frac{2}{m+1} \leq \frac{1}{3} < \frac{1}{e}$$

Thus, by Remark 7.2.12,

$$f(\min\{x_j, y_j\}) \leq f(px_j + (1-p)y_j)$$

As $\min\{x_j, y_j\} = y_j$ if and only if $j \leq \frac{m}{2}$, and $f(px_j + (1-p)y_j) \geq 0$ for any j, we have

$$\ln 2 \cdot S_{min}(\Phi) = \sum_{j=0}^{m} f(px_j + (1-p)y_j) \geq \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} f(px_j + (1-p)y_j)$$

$$\geq \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} f(\min\{x_j, y_j\}) = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} f\left(\frac{2j}{m(m+1)}\right) = \sum_{j=1}^{\lfloor \frac{m}{2} \rfloor} f\left(\frac{2j}{m(m+1)}\right)$$

As for $x \in [0, \lfloor \frac{m}{2} \rfloor]$, we have $0 \leq \frac{2x}{m(m+1)} \leq \frac{1}{e}$. Then for $j \in [0, \lfloor \frac{m}{2} \rfloor]$, we have

$$f\left(\frac{2j}{m(m+1)}\right) = \int_{j-1}^{j} f\left(\frac{2j}{m(m+1)}\right) dx \geq \int_{j-1}^{j} f\left(\frac{2x}{m(m+1)}\right) dx.$$

Consequently,

$$\ln 2 \cdot S_{min}(\Phi) \geq \sum_{j=1}^{\lfloor \frac{m}{2} \rfloor} \int_{j-1}^{j} f\left(\frac{2x}{m(m+1)}\right) dx = \int_{0}^{\lfloor \frac{m}{2} \rfloor} f\left(\frac{2x}{m(m+1)}\right) dx.$$

To compute the right hand side, let $u = \frac{2x}{m(m+1)}$ then

$$\int_{0}^{\lfloor \frac{m}{2} \rfloor} f\left(\frac{2x}{m(m+1)}\right) dx = \frac{m(m+1)}{2} \int_{0}^{\frac{2\lfloor \frac{m}{2} \rfloor}{m(m+1)}} (-u \ln u)\, du = g\left(\tfrac{2\lfloor \frac{m}{2} \rfloor}{m(m+1)}\right) - g(0)$$

but

$$g\left(\tfrac{2\lfloor \frac{m}{2} \rfloor}{m(m+1)}\right) \geq g\left(\tfrac{2(\frac{m}{2}-1)}{m(m+1)}\right) = g\left(\tfrac{m-2}{m(m+1)}\right) = \left(\frac{m-2}{m(m+1)}\right)^2 \left[\frac{1}{4} - \frac{\ln\left(\frac{m-2}{m(m+1)}\right)}{2}\right]$$

Since $\frac{m-2}{m(m+1)} < 1$, then $g\left(\frac{m-2}{m(m+1)}\right) > \frac{1}{4}\left(\frac{m-2}{m(m+1)}\right)^2$. Thus

$$S_{min}(\Phi) \geq \frac{1}{4 \ln 2}\left(\frac{m-2}{m(m+1)}\right)^2.$$

∎

7.3 The entanglement breaking property of EPOSIC channels

The present section examines the E.B.T property of EPOSIC channel. The E.B.T property of a quantum channel was reviewed in Section 6.2.

Proposition 7.3.1. *For $m \in \mathbb{N}$, the channel $\Phi_{m,m,m}$ and $\Phi_{0,m,0}$ are E.B.T channels.*

Proof:

Let $\{T_j : 0 \leq j \leq m\}$ be the EPOSIC Kraus operator of $\Phi_{m,m,m}$. By Remark 4.2.3 (1), we have $rank(T_j) \leq 1$ (since $r = 0$). Thus, $\Phi_{m,m,m}$ can be written in Kraus representation using only rank one operators. By Proposition 6.2.2, $\Phi_{m,m,m}$ is E.B.T. We also have $\Phi_{0,m,0} = (m+1)\Phi^*_{m,m,m}$ is an E.B.T channel (see Proposition 6.2.7, and Proposition 4.5.6). ∎

Since the set of entanglement breaking maps is a convex set [20, Th.3] then by Proposition 5.1.2, we have:

Corollary 7.3.2. *For $m \in \mathbb{N}$, let $\Phi : End(P_0) \longrightarrow End(P_m)$ and $\Psi : End(P_m) \longrightarrow End(P_0)$ be $SU(2)$-covariant channels. The maps Φ and Ψ are E.B.T channels.*

The following proposition determines some special cases where the EPOSIC channels are not E.B.T. Recall that the EPOSIC channel $\Phi_{m,n,h}$ has exactly $(n+1)$ EPOSIC Kraus operators (Definition 4.2.1).

Proposition 7.3.3. *Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$. If $m > \min\{n, 2h\}$ then $\Phi_{m,n,h} : End(P_{m+n-2h}) \longrightarrow End(P_m)$ is not E.B.T. In particular, $\Phi_{m,h,h}$ is not E.B.T for any $0 \leq h < m$.*

Proof:

Assume that $m > \min\{n, 2h\}$. If $n \geq 2h$, then $dim(P_{m+n-2h}) \geq dim(P_m)$. Hence

$$n + 1 < m + 1 \leq dim(P_{m+n-2h}) = max\{dim(P_{m+n-2h}), rank(Tr_{\overline{P}_{m+n-2h}}(C(\Phi_{m,n,h})))\}$$

The result follows by Corollary 6.2.6, and the fact that $\Phi_{m,n,h}$ has $(n+1)$ EPOSIC Kraus operators. If $n \leq 2h$, then $n \geq 2(n-h)$. Since $m+n-2h > \min\{n, 2(n-h)\}$, then by Proposition 4.5.6, and the first case, we get that the channel

$$\Phi_{m+n-2h,n,n-h} = \tfrac{m+n-2h+1}{m+1}\Phi^*_{m,n,h}$$

is not E.B.T. The result follows by Proposition 6.2.7. ∎

Chapter 8

The Minimal Output Entropy of the Tensor Product of $SU(2)$-Irreducibly Covariant Channels

There are very few tools that can be used to understand the minimal output entropy of the tensor product of two channels in general. In this chapter, we restrict ourselves to the $SU(2)$-irreducibly covariant channels, and obtain a bound on the minimal output entropy for the tensor product of two of such channels.

The main results of this chapter:

- Obtaining a bound on the minimal output entropy for the tensor product of two $SU(2)$-irreducibly covariant channels (Corollary 8.2.4).

8.1 The tensor product of $SU(2)$-irreducibly covariant channels.

For $i = 1, 2$, let H_i, K_i be Hilbert spaces, and $\Phi_i \in End\,(End(H_i), End(K_i))$. Recall that $\Phi_1 \otimes \Phi_2$, the tensor product of Φ_1 and Φ_2, is the endomorphism from $End(H_1 \otimes H_2)$ to $End(K_1 \otimes K_2)$ such that

$$\Phi_1 \otimes \Phi_2\,(A_1 \otimes A_2) = \Phi_1(A_1) \otimes \Phi_2(A_2)$$

for $A_i \in End(H_i)$, $i = 1, 2$.

Notation 8.1.1. Let H be Hilbert space such that $H = \bigoplus_{i=1}^{m} W_i$, and W_i are subspaces of H. Let $\mathfrak{P}$ be the set of the corresponding orthogonal projections $\{q_i : 1 \le i \le m\}$. In this chapter, $E_{\mathfrak{P}}$ will denote the map $E_{\mathfrak{P}} : End(H) \longrightarrow \bigoplus_{i=1}^{m} End(W_i)$ defined by

$$E_{\mathfrak{P}}(A) = \sum_{i=1}^{m} q_i A q_i^*$$

For $i = 1, 2$, and $r_i, m_i \in \mathbb{N}$, let P_{r_i} (resp. P_{m_i}) be the $SU(2)$-irreducible Hilbert space of dimension $r_i + 1$ (resp. $m_i + 1$). Let $P_{r_1} \otimes P_{r_2} = \bigoplus_{k=0}^{\min\{r_1,r_2\}} V_k$ (resp. $P_{m_1} \otimes P_{m_2} = \bigoplus_{l=0}^{\min\{m_1,m_2\}} W_l$) be the decomposition of $P_{r_1} \otimes P_{r_2}$ (resp. $P_{m_1} \otimes P_{m_2}$) into a direct sum of $S(2)$-irreducible subspaces. By Proposition 1.2.5, Proposition 3.3.6, and Proposition 3.3.8, we have

Proposition 8.1.2. *With the notation above, if $\Phi_i : End(P_{r_i}) \longrightarrow End(P_{m_i})$, $i = 1, 2$ are $SU(2)$-covariant channels, then*

1. *For $0 \le k \le \min\{r_1, r_2\}$, the restriction of $\Phi_1 \otimes \Phi_2$ to $End(V_k)$*

$$\Phi_1 \otimes \Phi_2\,|_{End(V_k)} : End(V_k) \longrightarrow End(P_{m_1} \otimes P_{m_2})$$

   is an $SU(2)$-covariant channel.

2. *If* $\mathfrak{P} = \{q_l : 0 \leq l \leq \min\{m_1, m_2\}\}$ *is the set of orthogonal projections of* $P_{m_1} \otimes P_{m_2}$ *on the* $SU(2)$*-irreducible subspaces* W_l*, then the map*

$$E_{\mathfrak{P}}\left(\Phi_1 \otimes \Phi_2 \left|_{End(V_k)}\right.\right) : End(V_k) \longrightarrow \bigoplus_{l=0}^{\min\{m_1,m_2\}} End(W_l)$$

is an $SU(2)$*-covariant channel.*

Proposition 8.1.3. *Let* $E_{\mathfrak{P}}\left(\Phi_1 \otimes \Phi_2 \left|_{End(V_k)}\right.\right)$ *be the channel given in Proposition 8.1.2. For each* $0 \leq k \leq \min\{r_1, r_2\}$*, we have:*

$$E_{\mathfrak{P}}\left(\Phi_1 \otimes \Phi_2 \left|_{End(V_k)}\right.\right) = \sum_{l=0}^{\min\{m_1,m_2\}} \lambda_{k,l}\psi_{k,l}$$

where for $0 \leq l \leq \min\{m_1, m_2\}$*, the map* $\psi_{k,l} : End(V_k) \longrightarrow End(W_l)$ *is an* $SU(2)$*-irreducibly covariant channel, and* $\{\lambda_{k,l} : 0 \leq l \leq \min\{m_1, m_2\}\}$ *are non-negative real numbers with* $\sum_{l=0}^{\min(m_1,m_2\}} \lambda_{k,l} = 1$*.*

Proof:

The map

$$q_l\left(\Phi_1 \otimes \Phi_2 \left|_{End(V_k)}\right.\right) q_l^* : End(V_k) \longrightarrow End(W_l)$$

is a completely positive $SU(2)$-irreducibly equivariant map (note that this mapping is not necessarily trace preserving). By Corollary 5.1.6, it is a multiple of an $SU(2)$-irreducibly covariant channel, i.e. there exist $SU(2)$-covariant channel $\psi_{k,l} : End(V_k) \longrightarrow End(W_l)$, and a non-negative number $\lambda_{k,l}$ such that

$$q_l\left(\Phi_1 \otimes \Phi_2 \left|_{End(V_k)}\right.\right) q_l^* = \lambda_{k,l}\psi_{k,l}$$

Consequently,

$$\begin{aligned} E_{\mathfrak{P}}\left(\Phi_1 \otimes \Phi_2 \left|_{End(V_k)}\right.\right) &= \sum_{l=0}^{\min\{m_1,m_2\}} q_l\left(\Phi_1 \otimes \Phi_2 \left|_{End(V_k)}\right.\right) q_l^* \\ &= \sum_{l=0}^{\min\{m_1,m_2\}} \lambda_{k,l}\psi_{k,l} \end{aligned}$$

By taking the trace of both sides for any state ϱ, we get that

$$\sum_{l=0}^{\min\{m_1,m_2\}} \lambda_{k,l} = 1$$

∎

8.2 Bound for the minimal output entropy of the tensor product of two $SU(2)$-irreducibly covariant channels.

Recall the definition of von Neumann entropy, and the minimal output entropy given in Section 6.1. Recall also if W is a subspace of a Hilbert space H, then $End(W)$ isomorphic to a subspace of $End(H)$ via the map $A \longmapsto \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$, see also Remark 1.2.11.

Lemma 8.2.1. *Let H and K be Hilbert spaces, and W be a subspace of H. Let $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel. Then*

$$S_{min}(\Phi) \leq S_{min}(\Phi\,|End(W))$$

Proof:

Let $\varrho \in End(W)$ be a pure state, ϱ can be considered as a pure state in $End(H)$. Thus,

$$S_{min}(\Phi) = \min\{S(\varrho) : \varrho \in \mathcal{P}(H)\} \leq \min\{S(\varrho) : \varrho \in \mathcal{P}(W)\} = S_{min}(\Phi\,|End(W))$$

∎

The following result is proved in [12, p.226].

Lemma 8.2.2. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a unital quantum channel. Then $S(\varrho) \leq S(\Phi(\varrho))$ for $\varrho \in D(H)$, where S is the von Neumann entropy.*

Proposition 8.2.3. *Let H, K and L be Hilbert spaces. Let $\Phi : End(H) \longrightarrow End(K)$ be a quantum channel, and $\Psi : End(K) \longrightarrow End(L)$ be a unital quantum channel. Then $S(\Phi(\varrho)) \leq S(\Psi(\Phi(\varrho)))$ for $\varrho \in D(H)$. Consequently*

$$S_{min}(\Phi) \leq S_{min}(\Psi \circ \Phi).$$

Recall by Corollary 2.3.6 that for $r_i, m_i \in \mathbb{N},\ i = 1, 2$, the space $P_{r_1} \otimes P_{r_2} = \bigoplus_{k=0}^{\min\{r_1,r_2\}} V_k$ (resp. $P_{m_1} \otimes P_{m_2} = \bigoplus_{l=0}^{\min\{m_1,m_2\}} W_l$), where V_k (resp. W_l) is an $SU(2)$-irreducible space isomorphic to $P_{r_1+r_2-2k}$(resp $P_{m_1+m_2-2l}$). Keeping these notations, we have

Corollary 8.2.4. *Let $\Phi_1 : End(P_{r_1}) \longrightarrow End(P_{m_1})$ and $\Phi_2 : End(P_{r_2}) \longrightarrow End(P_{m_2})$ be $SU(2)$-covariant channels. For each $0 \leq k \leq \min\{r_1, r_2\}$, we have*

$$S_{min}(\Phi_1 \otimes \Phi_2) \leq S_{min}\left(\sum_{l=0}^{\min\{m_1,m_2\}} \lambda_{k,l}\psi_{k,l}\right)$$

where $\{\psi_{k,l} : End(V_k) \longrightarrow End(W_l), 0 \leq l \leq \min\{m_1, m_2\}\}$ are $SU(2)$-irreducibly covariant channels, and $\lambda_{k,l}$ are non-negative real numbers with $\sum_{l=0}^{\min(m_1,m_2\}} \lambda_{k,l} = 1$.

Proof:

Pick k such that $0 \leq k \leq \min\{r_1, r_2\}$, let V_k be the $SU(2)$-irreducible subspace of $P_{r_1} \otimes P_{r_2}$ of dimension $r_1 + r_2 - 2k$. By Lemma 8.2.1,

$$S_{min}(\Phi_1 \otimes \Phi_2) \leq S_{min}(\Phi_1 \otimes \Phi_2 \,|_{End(V_k)})$$

Let $\mathfrak{P} = \{q_l : 0 \leq l \leq \min\{m_1, m_2\}\}$ be the $SU(2)$-equivariant projections of $P_{m_1} \otimes P_{m_2}$ onto the subspaces W_l. By Proposition 3.3.8, the map $E_{\mathfrak{P}} : End(P_{m_1} \otimes P_{m_2}) \longrightarrow \bigoplus_{i=1}^{m} End(W_i)$ defined by

$$E_{\mathfrak{P}}(A) = \sum_{l=1}^{\min\{m_1,m_2\}} q_l A q_l^*$$

is a unital channel, so by Proposition 8.2.3, and Proposition 8.1.3, we have

$$S_{min}(\Phi_1 \otimes \Phi_2) \leq S_{min}(E_{\mathfrak{P}}(\Phi_1 \otimes \Phi_2 \mid_{End(V_k)})) = S_{min}\left(\sum_{l=0}^{\min\{m_1,m_2\}} \lambda_{k,l}\psi_{k,l}\right)$$

∎

Part III

Appendices

Appendix A

Background Results in Operator Algebras

A.1 Background definitions and lemmas

As in the rest of the thesis, we assume all vector spaces to be complex vector spaces of finite dimension.

Definition A.1.1. *[31, p.4] Let H be a vector space. A norm on H is a map*

$$\|\cdot\| : H \longrightarrow [0, \infty)$$

such that

1. $\|x + y\| \leq \|x\| + \|y\|$ *for all vectors* x, y *in* H.

2. $\|\alpha x\| = |\alpha| \, \|x\|$ *if* x *in* H *and* α *is a scalar.*

3. $\|x\| > 0$ *if* $x \neq 0$ *where* x *in* H.

A vector space that equipped with a norm is called a *normed space.*

Definition A.1.2. *Let H be a vector space. An inner (scalar) product on H is a map $\langle \cdot | \cdot \rangle : H \times H \longrightarrow \mathbb{C}$, which is*

1. *linear in the second argument,*
   i.e. $\langle x\,|\lambda y\rangle = \lambda\,\langle x\,|y\rangle$ *and* $\langle x\,|y+z\rangle = \langle x\,|y\rangle + \langle x\,|z\rangle$, *for all* x, y, z *in* H *and all scalars* $\lambda \in \mathbb{C}$.

2. *conjugate symmetric,*
   i.e. $\langle x\,|y\rangle = \overline{\langle y\,|x\rangle}$, *for all* x, y *in* H.

3. *positive definite, i.e.* $\langle x\,|x\rangle \geq 0$ *and* $\langle x\,|x\rangle = 0$ *if and only if* $x = 0$ *for all* x *in* H.

A vector space H with an inner product is called an *inner product space.*

Remark A.1.3. In the definition above, we follow the definition that most physicists use, as given in [10, p.1].

Lemma A.1.4. *Let* H *be a vector space. An inner product on* H *induces a norm on* H*, given by* $\|x\| = \sqrt{\langle x\,|x\rangle}$ *for* $x \in H$.

Definition A.1.5. *A Hilbert space is an inner product space that is complete as a normed space (with respect to the norm induced by its inner product).*

Definition A.1.6. *Let* H *be a vector space. The conjugate space* $\overline{H}$ *is the vector space with the same underlying abelian group as* H*, and with scalar multiplication* $(\lambda, v) \longmapsto \lambda.v = \overline{\lambda}v$.

If H is a Hilbert space, then $\overline{H}$ is also a Hilbert space endowed with the inner product defined by $\langle h_1\,|h_2\rangle_{\overline{H}} = \langle h_2\,|h_1\rangle_H$.

Notation A.1.7. For a Hilbert space H, let H^* denote the vector space of all linear forms on H. The space H^* is called the dual space of H.

Theorem A.1.8. [6, p.40] Let H be a Hilbert space. The map

$$T : H \longrightarrow H^*$$

$$h \longmapsto f_h : H \longrightarrow \mathbb{C}$$

$$x \longmapsto \langle h \, | x \rangle_{_H}$$

is isometric anti-isomorphism from H to H^*.

For vector spaces H and K, let $End(H, K)$ denote the vector space of linear maps from H to K. We write $End(H)$ for $End(H, H)$ and $I_{_H}$ for the identity map on H.

Definition A.1.9. *Let H be a Hilbert space, and $\{e_1, e_2, ...e_n\}$ be an orthonormal basis of H. The un-normalized trace on $End(H)$, is the linear map $tr : End(H) \longrightarrow \mathbb{C}$ defined by*

$$tr(T) = \sum_{i=1}^{n} \langle e_i \, | T e_i \rangle_{_H}$$

The definition of the trace does not depend on the choice of the basis.

Lemma A.1.10. *Let H be a Hilbert space. For $T \in End(H)$, we have*

$$tr(T^*) = tr(\overline{T}) = \overline{tr(T)}.$$

For Hilbert spaces H and K, the space $End(H, K)$ endowed with the Hilbert-Schmidt inner product given by $\langle A \, | B \rangle_{_{End(H,K)}} = tr(A^* B)$ for $A, B \in End(H, K)$ is a Hilbert space.

Remark A.1.11. For $T \in End(H, K)$, $u \in H$ and $\lambda \in \mathbb{C}$, we have

$$T(\lambda.u) = T(\bar{\lambda} u) = \bar{\lambda} T(u) = \lambda.T(u)$$

Hence, the map T is also linear regarded as a map from $\overline{H}$ to $\overline{K}$. We use $\overline{T}$ to denote T when it is regarded as a map of $\overline{H}$ to $\overline{K}$.

Proposition A.1.12. *Let H and K be Hilbert spaces. The Hilbert spaces $End(\overline{H}, \overline{K})$ and $\overline{End(H, K)}$ are equal, and the Hilbert Schmidt inner product on them is the same.*

Definition A.1.13. *For Hilbert spaces H, K and $T \in End(H,K)$, the adjoint of T is the unique linear map $T^* \in End(K,H)$ such that*

$$\langle y \,| Tx \rangle_K = \langle T^* y \,| x \rangle_H \qquad \forall x \in H, \forall y \in K.$$

Definition A.1.14. *[10, p.6-8]Let H be a Hilbert space, and $T \in End(H)$. The operator$T$ is called Hermitian (self adjoint) if $T = T^*$. A positive operator T (denoted by $T \geq 0$), is a Hermitian operator with non-negative eigenvalues. An orthogonal projection T is a positive operator with an eigenvalues belongs to $\{0,1\}$. i.e. $T^2 = T = T^*$. Finally, T is a unitary operator if T satisfy $TT^* = T^*T = I_H$.*

Lemma A.1.15. *[10, p.6] Let H be a Hilbert space, and $T \in End(H)$. The following are equivalent:*

1. *T is a positive operator.*
2. *$T = SS^*$ for some $S \in End(H)$.*
3. *$\langle Tw \,| w \rangle_H \geq 0$ for any $w \in H$.*

Lemma A.1.16. *Let K be a Hilbert space. For $T \in End(K)$ and $0 \neq w \in K$, we have*

$$\langle T \,| ww^* \rangle_{End(K)} = \langle Tw \,| w \rangle_K .$$

Proof:

Let $\{f_i : 1 \leq i \leq d_K\}$ be an orthonormal basis for K with $f_1 = \frac{w}{\|w\|}$. We hence have:

$$\begin{aligned}\langle T \,| ww^* \rangle_{End(K)} = tr(T^* ww^*) &= \sum_{i=1}^{d_K} \langle f_i \,| T^* ww^* f_i \rangle_K \\ &= \langle f_1 \,| T^* ww^* f_1 \rangle_K = \left\langle \frac{w}{\|w\|} \,\middle|\, T^* ww^* \left(\frac{w}{\|w\|}\right) \right\rangle_K \\ &= \langle w \,| T^* w \rangle_K = \langle Tw \,| w \rangle_K .\end{aligned}$$

∎

Proposition A.1.17. *Let K be a Hilbert space, and $T \in End(K)$. The operator T is positive if and only if $\langle T \,|X \rangle_{End(K)} \geq 0$ for all positive X.*

Proof:

If T and X are positive, then $T = T_1 T_1^*$, $X = X_1 X_1^*$ for some $T_1, X_1 \in End(K)$, and

$$\langle T \,|X \rangle_{End(K)} = \langle T_1 T_1^* \,|X_1 X_1^* \rangle_{End(K)} = tr\,(T_1 T_1^* X_1 X_1^*) = tr\,((T_1^* X_1)^* \, T_1^* X_1) \geq 0.$$

For the other direction, assume that $\langle T \,|X \rangle_{End(K)} \geq 0$ for all positive X. As ww^* is positive for any $w \in K$, we have

$$\langle Tw \,|w \rangle_K = \langle T \,|ww^* \rangle_{End(K)} \geq 0$$

and T is positive. ∎

Definition A.1.18. *Let H be a Hilbert space, and W_1, W_2 be subspaces of H. We say the spaces W_1 and W_2 are mutually orthogonal if $\langle u_1 \mid u_2 \rangle_H = 0$ for every $u_1 \in W_1$ and $u_2 \in W_2$.*

Recall that if $H_1, H_2, ..., H_n$ Hilbert spaces, their (external) direct sum denoted by $\bigoplus_{i=1}^{n} H_i$, is the $\{(h_1, h_2, ..., h_n) : h_i \in H_i\}$. It is a Hilbert space with the inner product given by $\langle (h_1, h_2, ..., h_n) \mid (k_1, k_2, ..., k_n) \rangle = \sum_{i=1}^{n} \langle h_i \mid k_i \rangle_{H_i}$.

Definition A.1.19. *Let H be a Hilbert space, and $H_1, H_2, ..., H_n$ be subspaces of H, such that $H = H_1 + H_2 + \cdots\cdots + H_n$, and $H_i \cap \left(\sum_{i \neq j} H_j \right) = \{0\}$, then H is called the (internal) direct sum of $\{H_i : 1 \leq i \leq n\}$. If $H_1, H_2, ..., H_n$ are mutually orthogonal subspaces of H, then H is called the orthogonal direct sum of $\{H_i : 1 \leq i \leq n\}$.*

If $H_1, H_2, ..., H_n$ are subspaces of a Hilbert space H, satisfying the conditions in Definition A.1.19, we identify the internal direct sum of $\{H_i : 1 \leq i \leq n\}$ with their external direct sum $\bigoplus_{i=1}^{n} H_i$ via

$$h = h_1 + h_2 + \cdots + h_n \longleftrightarrow (h_1, h_2, \cdots, h_n)$$

Definition A.1.20. *For $i = 1, 2$, let H_i and K_i be Hilbert spaces, and $\phi_i \in End(H_i, K_i)$. Then $\phi_1 \oplus \phi_2 : H_1 \oplus H_2 \longrightarrow K_1 \oplus K_2$ is the endomorphism given by*

$$\phi_1 \oplus \phi_2 (h_1, h_2) = (\phi_1 (h_1), \phi_2 (h_2))$$

for $(h_1, h_2) \in H_1 \oplus H_2$.

Let H and K be two vector spaces, consider the free vector space $L = \mathbb{C}(H \times K)$. By identifying $H \times K$ as a subset of L, one considers in L the subspace N generated by the elements of the form

$$(\lambda_1 h_1 + \lambda_2 h_2, \mu_1 k_1 + \mu_2 k_2) - \lambda_1\mu_1(h_1, k_1) - \lambda_1\mu_2(h_1, k_2) - \lambda_2\mu_1(h_2, k_1) - \lambda_2\mu_2(h_2, k_2)$$

The tensor product of H and K, denoted by $H \otimes K$ is defined to be the quotient vector space L/N. For $h \in H$ and $k \in K$, the element $h \otimes k$ denotes the element of $H \otimes K$ represented by the element (h, k) of L/N. The tensor product of H and K can be abstractly characterized as following:

Definition A.1.21. *Let H and K be two vector spaces. The tensor product of H and K is a vector space $H \otimes K$ with a bilinear map $\Theta : H \times K \longrightarrow H \otimes K$ which is universal in the following sense, if $\Psi : H \times K \longrightarrow V$ is bilinear map into some vector space V, then there exists a unique linear map $T : H \otimes K \longrightarrow V$ such that $T \circ \Theta = \Psi$. We denote $\Theta(h, k)$ by $h \otimes k$, so the map T is characterized by $T(h \otimes k) = \Psi(h, k)$. The space $H \otimes \mathbb{C}$ is identified with H via the unitary map $h \otimes \lambda \longmapsto \lambda h$.*

Proposition A.1.22. *Let H and K be two vector spaces. If $\{e_1, e_2, ...e_n\}$ and $\{f_1, f_2, ...f_m\}$ are bases for H and K respectively, then $\{e_i \otimes f_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ forms a basis for $H \otimes K$. In particular $dim(H \otimes K) = dim(H) \cdot dim(K)$.*

Example A.1.23.

1. $\mathbb{C}^m \otimes \mathbb{C}^n \simeq \mathbb{C}^{mn}$.

2. For vector spaces H and K, we have $End(H, K) \simeq K \otimes H^*$.

According to the example above, the space $End(H, K)$ is generated by $\{xy^* : x \in K, y \in H\}$, where y^* denotes the linear form on H given by $y^*(z) = \langle y \,|z \rangle_H$, and xy^* denotes the map $xy^*(z) = \langle y \,|z \rangle_H x$ for any $z \in H$.

Proposition A.1.24. *For $i = 1, 2$, let H_i and K_i be vector spaces. If $S \in End(H_1, H_2)$ and $T \in End(K_1, K_2)$, then there exists a unique linear map denoted $S \otimes T$ from $H_1 \otimes K_1$ to $H_2 \otimes K_2$ characterized by $S \otimes T(h \otimes k) = S(h) \otimes T(k)$. If S and T are isomorphisms, then $S \otimes T$ is an isomorphism with inverse $S^{-1} \otimes T^{-1}$.*

Proposition A.1.25. *For $i = 1, 2$, let H_i and K_i be vector spaces. There exist a linear isomorphism $T : End(H_1, H_2) \otimes End(K_1, K_2) \longrightarrow End(H_1 \otimes K_1, H_2 \otimes K_2)$ given by*

$$T(A \otimes B)(h_1, k_1) = A(h_1) \otimes B(k_1)$$

for $A \otimes B \in End(H_1, H_2) \otimes End(K_1, K_2)$, and extending linearly.

Lemma A.1.26. *Let H and K be inner product spaces whose inner products are given by $\langle \cdot \,|\cdot \rangle_H$ and $\langle \cdot \,|\cdot \rangle_K$ respectively. There exists a unique inner product on $H \otimes K$ such that $\langle h_1 \otimes k_1 \,|h_2 \otimes k_2 \rangle_{H \otimes K} = \langle h_1 \,|h_2 \rangle_H \langle k_1 \,|k_2 \rangle_H$. If H and K are Hilbert spaces, then $H \otimes K$ is a Hilbert space.*

For the following proposition see [3, p.69, p.74].

Proposition A.1.27. *Let (H, π_H) and (K, π_K) be two representations of a group G. The tensor product $\pi_H \otimes \pi_K$ (resp. the direct sum $\pi_H \oplus \pi_K$) defines a representation of G in $H \otimes K$ (resp. $H \oplus K$) given by*

$$g \longmapsto \pi_{H(g)} \otimes \pi_{K(g)}$$

$$(resp. \qquad g \longmapsto \pi_{H}(g) \oplus \pi_{K}(g))$$

A.2 Positive and completely positive maps

Definition A.2.1. *Let H and K be two Hilbert spaces. A linear map $\Phi : End(H) \longrightarrow End(K)$ is*

- *positive if $\Phi(A) \geq 0$ for any positive $A \in End(H)$.*
- *n-positive if $\Phi \otimes I_n$ is a positive map, where $\Phi \otimes I_n$ denotes the linear map from $End(H) \otimes \mathbb{M}_n$ into $End(K) \otimes \mathbb{M}_n$, such that*

  $$\Phi \otimes I_n \,(A \otimes B) = \Phi(A) \otimes B$$

  for all $A \in End(H)$ and $B \in \mathbb{M}_n$.
- *completely positive if it is n-positive for each $n \geq 1$.*

Before stating the next proposition, we introduce the following maps that are needed for the proof.

Notation A.2.2. For $k \geq 2$,

- let ι_k denote the canonical inclusion of $\mathbb{C}^{k-1}$ in $\mathbb{C}^k \simeq \mathbb{C}^{k-1} \times \mathbb{C}$ given by

  $$\iota_k : \mathbb{C}^{k-1} \longrightarrow \mathbb{C}^k$$

  $$x \longmapsto (x, 0)$$

  for $x \in \mathbb{C}^{k-1}$. The adjoint map of ι_k is the projection $\iota_k^* : \mathbb{C}^k \longrightarrow \mathbb{C}^{k-1}$ that maps the first $k-1$ component of $x \in \mathbb{C}^k$ to themselves, and the last one to the zero.

- For a Hilbert space H, let
  - σ_{H} denote the map $I_{H} \otimes \iota_k : H \otimes \mathbb{C}^{k-1} \longrightarrow H \otimes \mathbb{C}^k$.
  - σ_{H}^{*} denote the adjoint map of σ_{H}, $I_{H} \otimes \iota_k^{*} : H \otimes \mathbb{C}^{k} \longrightarrow H \otimes \mathbb{C}^{k-1}$.

Proposition A.2.3. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a linear map. For $k \geq 2$, if Φ is k-positive, then it is $(k-1)$-positive.*

Proof:

Assume that Φ is k-positive. By Proposition 3.2.13, using the same notation in A.2.3, we have

$$Ad_{\sigma_H} : End(H) \otimes \mathbb{M}_{k-1} \longrightarrow End(H) \otimes \mathbb{M}_k$$

$$Ad_{\sigma_K^*} : End(K) \otimes \mathbb{M}_{k} \longrightarrow End(K) \otimes \mathbb{M}_{k-1}$$

and

$$\Phi \otimes I_k : End(H) \otimes \mathbb{M}_{k} \longrightarrow End(K) \otimes \mathbb{M}_k$$

are positive maps, so is the maps composition $Ad_{\sigma_K^*} \circ (\Phi \otimes I_k) \circ Ad_{\sigma_H} : End(H) \otimes \mathbb{M}_{k-1} \longrightarrow End(K) \otimes \mathbb{M}_{k-1}$ which $\Phi \otimes I_{k-1}$. ∎

Proposition A.2.4. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a linear map. The map Φ is positive if and only if $\langle \Phi(A) \,|B \rangle_{End(K)} \geq 0$ for $A \in End(H)$ and $B \in End(K)$ such that $A, B \geq 0$.*

Proof:

Let $A \in End(H)$ and $B \in End(K)$ such that $A, B \geq 0$. Assume that Φ is positive, then $\Phi(A) \geq 0$. Thus, there exist $X, Y \in End(K)$ such that $\Phi(A) = XX^*$ and $B = YY^*$. Hence,

$$\langle \Phi(A) \,|B \rangle_{End(K)} = \langle XX^* \,|YY^* \rangle_{End(K)} = tr(XX^*YY^*) = tr((X^*Y)^* X^*Y) \geq 0.$$

The other direction, follows by Proposition A.1.17. ∎

Recall (by Definition 4.5.1) that the dual of a linear map $\Phi : End(H) \longrightarrow End(K)$ is the unique map $\Phi^* : End(K) \longrightarrow End(H)$ such that

$$\langle B \,|\Phi(A) \rangle_{End(K)} = \langle \Phi^*(B) \,| A \rangle_{End(H)}$$

for all $A \in End(H)$ and $B \in End(K)$.

Proposition A.2.5. *Let H and K be Hilbert spaces, and $\Phi : End(H) \longrightarrow End(K)$ be a linear map. Then*

1. *Φ is a positive map if and only if Φ^* is positive.*

2. *Φ is completely positive if and only if Φ^* is completely positive.*

3. *Φ^* is trace preserving map if and only if $\Phi(I_H) = I_K$.*

Proof:

The proof of (1) and (2) follows directly from Proposition A.2.4, as $(\Phi \otimes I_n)^* = \Phi^* \otimes I_n$ for each n. For (3), note that for any $T \in End(K)$, we have

$$tr(\Phi^*(T)) = \langle I_H \,|\Phi^*(T) \rangle_{End(H)} = \langle \Phi(I_H) \,|T \rangle_{End(K)}$$

and

$$tr(T) = \langle I_K \,|T \rangle_{End(K)}$$

Hence, Φ^* is trace preserving if and only if $\langle \Phi(I_H) \,|T \rangle_{End(K)} = \langle I_K \,|T \rangle_{End(K)}$ for each $T \in End(K)$. i.e. if and only if $\Phi(I_H) = I_K$. ∎

Proposition A.2.6. *Let (H, π_H) and (K, π_K) be two unitary representations of a group G. A linear map $\Phi : End(H) \longrightarrow End(K)$ is G-equivariant if and only if Φ^* is G-equivariant.*

Proof:

Assume Φ is G-equivariant. By Proposition 1.2.4,

$$\Phi(\pi_{H(g)} A \pi^*_{H(g)}) = \pi_{K(g)} \Phi(A) \pi^*_{K(g)} \qquad \forall g \in G$$

i.e.

$$\Phi \circ Ad_{\pi_{H(g)}} = Ad_{\pi_{K(g)}} \circ \Phi \qquad \forall g \in G$$

hence

$$\Phi^* \circ Ad_{\pi_{K(g)}} = Ad_{\pi_{H(g)}} \circ \Phi^* \qquad \forall g \in G$$

i.e

Φ^* is G-equivariant.

As $(\Phi^*)^* = \Phi$, the other direction also holds. ∎

A.3 Covariant Stinespring dilation theorem

In this section, we state and give a proof of a special case of the covariant Stinespring dilation theorem. The general case can be proved with some modification. The following is a special case of the Stinespring dilation theorem [28, p.43-45].

Theorem A.3.1. Let H be finite dimensional Hilbert spaces, and $\Phi : \mathbb{M}_n(\mathbb{C}) \longrightarrow End(H)$ be a completely positive map. Then there exists a Hilbert space $\mathcal{K}$, a unital $*$-homomorphism $\pi : \mathbb{M}_n(\mathbb{C}) \longrightarrow End(\mathcal{K})$, and a bounded operator $V : H \longrightarrow \mathcal{K}$ with $\|\Phi(I_n)\| = \|V\|^2$ such that

$$\Phi(A) = V^* \pi(A) V \qquad \forall A \in \mathbb{M}_n(\mathbb{C})$$

Remark A.3.2. If G is a group and $\rho : G \longrightarrow End(\mathbb{C}^n)$ a representation of G in $\mathbb{C}^n$ then $Ad_\rho : G \longrightarrow End(\mathbb{M}_n)$ where $Ad_\rho(g) = Ad_{\rho(g)}$ is a representation of G in $\mathbb{M}_n(\mathbb{C})$.

Following the proof's steps of Stinespring dilation theorem in [28, p.43-45], we give a proof of the following theorem :

Theorem A.3.3. (Covariant Stinespring dilation theorem) Let $n \in \mathbb{N}$, H be a finite dimensional Hilbert space, (H, ρ_H) and $(\mathbb{C}^n, \rho_n)$ be two unitary representations of a group G, and $\Phi : \mathbb{M}_n(\mathbb{C}) \longrightarrow End(H)$ be a completely positive G-equivariant map. Then there exist

1. a finite dimensional Hilbert space $\mathcal{K}$ with a unitary representation σ of G in $\mathcal{K}$,
2. a G-equivariant unital $*-$homomorphism $\pi : \mathbb{M}_n(\mathbb{C}) \longrightarrow End(\mathcal{K})$, and
3. a G-equivariant bounded operator $V : K \longrightarrow \mathcal{K}$ such that

$$\Phi(A) = V^* \pi(A) V \qquad \forall A \in \mathbb{M}_n(\mathbb{C})$$

Proof:

We follow the scheme of the proof given in [28, p.43-45]. On the algebraic tensor product $\mathbb{M}_n(\mathbb{C}) \otimes H$, we consider the pre-inner product $\langle \cdot | \cdot \rangle$ defined for $A, B \in \mathbb{M}_n(\mathbb{C})$ and $x, y \in H$ by $\langle A \otimes x | A \otimes y \rangle = \langle \Phi(B^*A)x | y \rangle_H$ where $\langle \cdot | \cdot \rangle_H$ is the inner product on H. As $\Phi \circ Ad_{\rho_n(g)} = Ad_{\rho_H(g)} \circ \Phi$, $\forall g \in G$, then for all $A, B \in \mathbb{M}_n(\mathbb{C})$ and $x, y \in H$, we have

$$\begin{aligned}
&\left\langle Ad_{\rho_n(g)} \otimes \rho_H(g) (A \otimes x) \,\middle|\, Ad_{\rho_n(g)} \otimes \rho_H(g) (B \otimes y) \right\rangle \\
&\qquad = \left\langle Ad_{\rho_n(g)}(A) \otimes \rho_H(g)(x) \,\middle|\, Ad_{\rho_n(g)}(B) \otimes \rho_H(g)(y) \right\rangle \\
&\qquad = \left\langle \Phi\left(\left(Ad_{\rho_n(g)}(B)\right)^* Ad_{\rho_n(g)}(A) \right) \rho_H(g)(x) \,|\, \rho_H(g)(y) \right\rangle_H \\
&\qquad = \left\langle \Phi\left(Ad_{\rho_n(g)}(B^*A) \right) \rho_H(g)(x) \,|\, \rho_H(g)(y) \right\rangle_H \\
&\qquad = \left\langle \rho_H(g) \Phi(B^*A) \left(\rho_H(g)\right)^* \rho_H(g)(x) \,|\, \rho_H(g)(y) \right\rangle_H \\
&\qquad = \left\langle \rho_H(g) \Phi(B^*A)(x) \,|\, \rho_H(g)(y) \right\rangle_H
\end{aligned}$$

$$= \left\langle \Phi\left(B^{*}A\right)(x)\,|y\right\rangle_{H} = \left\langle A\otimes x\,|B\otimes y\right\rangle.$$

Therefore, the map $\langle\cdot\,|\cdot\rangle$ is G -invariant under the action of $\rho = Ad_{\rho_n(g)} \otimes \rho_H$. Thus, the subspace (as checked in [28])

$$\mathcal{N} = \{u \in \mathbb{M}_n(\mathbb{C}) \otimes H : \langle u\,|v\rangle = 0\,\forall\, v \in \mathbb{M}_n(\mathbb{C}) \otimes H\}$$

is G-invariant under ρ. Hence, the induced bilinear form on $\mathcal{K} = \left(\mathbb{M}_n(\mathbb{C}) \otimes H\right)/\mathcal{N}$ is a G-invariant inner product with respect to the action of G on $\mathcal{K}$ given by

$$\sigma_{(g)}(u+\mathcal{N}) = \rho_{(g)}(u) + \mathcal{N}.$$

For $A \in \mathbb{M}_n(\mathbb{C})$, the linear map $\pi(A) : \mathbb{M}_n \otimes H \longrightarrow \mathbb{M}_n \otimes H$ defined by

$$\pi(A)\left(\sum A_i \otimes x_i\right) = \sum AA_i \otimes x_i$$

satisfies

$$\begin{aligned}
\left(Ad_{\rho(g)}\pi(A)\right)\left(\sum A_i \otimes x_i\right) &= \left(\rho_{(g)}\pi(A)\rho^{*}{}_{(g)}\right)\left(\sum A_i \otimes x_i\right)\\
&= \rho_{(g)}\pi(A)\left(\sum \rho_n^{*}(g)A_i\rho_n(g) \otimes \rho^{*}_{H(g)}\left(x_i\right)\right)\\
&= \rho_{(g)}\left(\sum A\rho_n^{*}(g)A_i\rho_n(g) \otimes \rho^{*}_{H(g)}\left(x_i\right)\right)\\
&= \sum \rho_n(g)\left(A\rho_n^{*}(g)A_i\rho_n(g)\right)\rho_n^{*}(g) \otimes \rho_{H(g)}\rho^{*}_{H(g)}\left(x_i\right)\\
&= \left(\sum \rho_n(g)A\rho_n^{*}(g)A_i \otimes x_i\right) = \pi \circ Ad_{\rho_n(g)}(A)\left(\sum a_i \otimes x_i\right).
\end{aligned}$$

So, π is a G-equivariant map for the action $Ad_{\rho_n(g)}$ on $\mathbb{M}_n\left(\mathbb{C}\right)$ and Ad_{ρ} on $End(\mathbb{M}_n \otimes H)$ with $\varrho = Ad_{\rho_n(g)} \otimes \rho_H$. As shown in [28, p.43-45] $\pi(A)$ leaves $\mathcal{N}$ invariant and thus extends to a bounded linear operator on $\mathcal{K}$, which is G-equivariant. Then $\pi : \mathbb{M}_n \longrightarrow End(\mathcal{K})$ is a unital $*$-homomorphism such that for each $A \in \mathbb{M}_n\left(\mathbb{C}\right)$, $g \in G$ and $u + \mathcal{N} \in \mathcal{K}$, we have

$$\left(Ad_{\sigma(g)}\pi(A)\right)(u+\mathcal{N}) = \left(\sigma_{(g)}\pi(a)\sigma^{*}{}_{(g)}\right)(u+\mathcal{N})$$

$$= \rho_{(g)}\pi(A)\rho^*{}_{(g)}(u) + \mathcal{N} = \pi \circ Ad_{\rho_{n(g)}}(A)(u) + \mathcal{N}$$

$$= \pi \circ Ad_{\rho_{n(g)}}(A)(u + \mathcal{N}).$$

So, $Ad_{\sigma(g)} \circ \pi = \pi \circ Ad_{\rho_{n(g)}}$, and π is G-equivariant for the actions $Ad_{\rho_{n(g)}}$ on $\mathbb{M}_n(\mathbb{C})$ and Ad_σ on $End(\mathcal{K})$. The map $V : H \longrightarrow \mathcal{K}$ defined by $V(x) = I_n \otimes x + \mathcal{N}$ satisfies

$$V(\rho_{H(g)}(x)) = I_n \otimes \rho_{H(g)}(x) + \mathcal{N}$$

$$= Ad_{\rho_{n(g)}}(I_n) \otimes \rho_{H(g)}(x) + \mathcal{N}$$

$$= Ad_{\rho_{n(g)}} \otimes \rho_{H(g)}(I_n \otimes x + \mathcal{N})$$

$$= \sigma_{(g)} V(x)$$

As shown in [28, p.43-45], or by direct computation

$$\Phi(A) = V^* \pi(A) V$$

for each $A \in \mathbb{M}_n(\mathbb{C})$. ∎

Appendix B

Deferred Proofs

B.1 Deferred proofs in chapter 2

The proof of Lemma 2.2.3

Recall that for $m, n \in \mathbb{N}$, we identify the spaces $P_m \otimes P_n$ and $P_{m,n}$, and by Remark 2.2.1, we have

$$\rho_{m(g)} \otimes \rho_{n(g)} f(x, y) = f(ax_1 - \bar{b}x_2, bx_1 + \bar{a}x_2, ay_1 - \bar{b}y_2, by_1 + \bar{a}y_2)$$

where $f(x, y) := f(x_1, x_2, y_1, y_2) \in P_m \otimes P_n$, and $g = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \in SU(2)$. Intuitively, the action of $SU(2)$ on any polynomial $f(x, y)$ in $P_m \otimes P_n$, is by replacing x_1 by $ax_1 - \bar{b}x_2$, x_2 by $bx_1 + \bar{a}x_2$, y_1 by $ay_1 - \bar{b}y_2$ and y_2 by $by_1 + \bar{a}y_2$. The next lemma is direct computations on the standard bases elements for $P_{m-1} \otimes P_n$ and $P_m \otimes P_{n-1}$

Lemma B.1.1. *For $m, n \in \mathbb{N}$. Let $M_{x_i} : P_{m-1} \otimes P_n \longrightarrow P_m \otimes P_n$, and $M_{y_i} : P_m \otimes P_{n-1} \longrightarrow P_m \otimes P_n$ denote the multiplication by x_i and y_i respectively. Then*

$\left(\frac{\partial}{\partial x_i}\right)^* = M_{x_i}$ and $\left(\frac{\partial}{\partial y_i}\right)^* = M_{y_i}$ for each $i = 1, 2$.

Recall the maps Δ_{xy} , Δ_{yx} , Γ_{xy} and Ω_{xy} in Definition 2.2.2.

Lemma B.1.2. *The operators Δ_{xy} , Δ_{yx} , Γ_{xy} and Ω_{xy} are $SU(2)$-equivariant, and satisfy*

$$\Delta^*_{xy} = \Delta_{yx}, \qquad \Gamma^*_{xy} = \Omega_{xy}$$

Proof:

Let $x := (x_1, x_2)$, $y = (y_1, y_2)$, $f(x, y) \in P_m \otimes P_n$, and $g = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \in SU(2)$. Using Remark 2.2.1, we get

$$\frac{\partial}{\partial x_1}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right) = a\frac{\partial}{\partial x_1}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right) + b\frac{\partial}{\partial x_2}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right)$$

and

$$\frac{\partial}{\partial x_2}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right) = -\bar{b}\frac{\partial}{\partial x_1}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right) + \bar{a}\frac{\partial}{\partial x_2}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right)$$

Hence,

$$\begin{aligned}
\Delta_{yx}(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)) &= y_1\frac{\partial}{\partial x_1}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right) + y_2\frac{\partial}{\partial x_2}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right) \\
&= (ay_1 - \bar{b}y_2)\frac{\partial}{\partial x_1}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right) + (by_1 + \bar{a}y_2)\frac{\partial}{\partial x_2}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x,y)\right) \\
&= \left(\rho_{m-1}(g) \otimes \rho_{n+1}(g)\right)\left(y_1\frac{\partial}{\partial x_1} f\left((x,y)\right) + y_2\frac{\partial}{\partial x_2} f\left((x,y)\right)\right) \\
&= \left(\rho_{m-1}(g) \otimes \rho_{n+1}(g)\right)\Delta_{yx}(f(x,y)).
\end{aligned}$$

i.e. Δ_{yx} is $SU(2)$-equivariant.

By Lemma B.1.1, we have

$$\left\langle \Delta_{xy}\left(f(x,y)\right) | g(x,y) \right\rangle_{P_{m+1}\otimes P_{n-1}} = \left\langle f(x,y) \,|\, \Delta_{yx}\left(g(x,y)\right) \right\rangle_{P_m \otimes P_n}$$

for $g(x, y) \in P_{m+1} \otimes P_{n-1}$, then $\Delta^*_{yx} = \Delta_{xy}$. By Proposition 1.2.7, the map Δ_{xy} is also $SU(2)$-equivariant.

Similarly, we have:

$$\left(\rho_{m+1}(g) \otimes \rho_{n+1}(g)\right)\Gamma_{xy}\left(f(x,y)\right) = \left(\rho_{m+1}(g) \otimes \rho_{n+1}(g)\right)\left(\left(x_1y_2 - y_1x_2\right) f(x,y)\right)$$

$= \left[(ax_1 - \bar{b}x_2)(by_1 + \bar{a}y_2) - (ay_1 - \bar{b}y_2)(bx_1 + \bar{a}x_2)\right] f(ax_1 - \bar{b}x_2, bx_1 + \bar{a}x_2, ay_1 - \bar{b}y_2, by_1 + \bar{a}y_2)$

$= (a\bar{a}x_1y_2 - b\bar{b}x_2y_1 + b\bar{b}x_1y_2 - a\bar{a}x_2y_1)\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x_1, x_2, y_1, y_2)\right)$

$= (a\bar{a} + b\bar{b})(x_1y_2 - x_2y_1)\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x_1, x_2, y_1, y_2)\right)$

$= det(g)(x_1y_2 - x_2y_1)\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x, y)\right)$

$= \Gamma_{xy}\left(\rho_{m(g)} \otimes \rho_{n(g)} f(x, y)\right)$

Thus Γ_{xy} is $SU(2)$-equivariant. By Lemma B.1.1, we have

$$\left\langle \Gamma_{xy}\left(f(x,y)\right) \middle| g(x,y) \right\rangle_{P_{m+1} \otimes P_{n+1}} = \left\langle f(x,y) \middle| \Omega_{xy}\left(g(x,y)\right) \right\rangle_{P_m \otimes P_n}$$

for $g(x,y) \in P_{m+1} \otimes P_{n+1}$, which gives $\Gamma^*_{xy} = \Omega_{xy}$. By Proposition 1.2.7, Ω_{xy} is $SU(2)$-equivariant.

∎

The proof of Lemma 2.3.11

Recall the isometry $\alpha_{m,n,h}$ in Definition 2.3.2.

Lemma B.1.3. *For $m, n, h \in \mathbb{N}$ with $0 \le h \le \min\{m, n\}$, let $r = m + n - 2h$. Using the standard basis for P_k where $k \in \{m, n, r\}$, we have:*

1. $\alpha_{m,n,h}\left(f^r_i\right) = \sum_{s=0}^{h} \sum_{j=\max\{s,-m+i+h+s\}}^{\min\{i+s,\, n-h+s\}} \beta^{m,n,h}_{i,s,j}\, f^m_{l_{ij}} \otimes f^n_j$

2. $\alpha^*_{m,n,h}\left(f^m_l \otimes f^n_j\right) = \begin{cases} \left(\sum_{s=\max\{0,h-l,h+j-n\}}^{\min\{h,j,m-l\}} \beta^{m,n,h}_{l+j-h,s,j}\right) f^r_{l+j-h} & if \quad 0 \le l + j - h \le r \\ 0 & otherwise \end{cases}$

$$where\ \beta^{m,n,h}_{i,s,j} = (-1)^s \frac{\binom{h}{s}\binom{n-h}{j-s}\binom{m-h}{i-j+s}}{(m-h)!}\sqrt{\frac{c_{m,n,h} r!\ m!\ n!}{\binom{r}{i}\binom{m}{i-j+h}\binom{n}{j}}}$$

Proof:

Recall that the standard basic element of P_k is $f^k_i = a^i_k x^i_1 x^{k-i}_2$ where $a^i_k = \frac{1}{\sqrt{i!(k-i)!}}$. As

$$\Delta^{n-h}_{yx} = \left(y_1 \frac{\partial}{\partial x_1} + y_2 \frac{\partial}{\partial x_2}\right)^{n-h} = \sum_{t=0}^{n-h} \binom{n-h}{t} y^t_1 y^{n-h-t}_2 \frac{\partial^t}{\partial x^t_1}\frac{\partial^{n-h-t}}{\partial x^{n-h-t}_2}$$

and

$$\Gamma^h_{xy} = (x_1y_2 - y_1x_2)^h = \sum_{s=0}^{h} (-1)^s \binom{h}{s} (x_1y_2)^{h-s}\ (x_2y_1)^s$$

by the definition of $\alpha_{m,n,h}$, we have:

For $0 \leq i \leq r$

$$\alpha_{m,n,h}(f^r_i) = \sqrt{c_{m,n,h}} a^i_r \sum_{s=0}^{h}\sum_{t=0}^{n-h} (-1)^s \binom{h}{s}\binom{n-h}{t} x^{h-s}_1 x^s_2 y^{(t+s)}_1 y^{n-(s+t)}_2 \frac{\partial^t}{\partial x^t_1} x^i_1 \frac{\partial^{n-h-t}}{\partial x^{n-h-t}_2} x^{r-i}_2$$

But

$$\frac{\partial^t}{\partial x^t_1} x^i_1 \frac{\partial^{n-h-t}}{\partial x^{n-h-t}_2} x^{r-i}_2 = \begin{cases} \frac{i!(r-i)!}{(i-t)!(m-h-i+t)!}\ x^{i-t}_1 x^{m+t-h-i}_2 & -m+i+h \leq t \leq i \\ \\ 0 & otherwise \end{cases}$$

Thus, we can rewrite the above sum as

$$\alpha_{m,n,h}(f^r_i) = \sqrt{c_{m,n,h}} a^i_r \sum_{s=0}^{h} \sum_{t=\max\{0,-m+i+h\}}^{\min\{i,\,n-h\}} \mathcal{U}(m,n,h,i,s,t) x^{h-(s+t)+i}_1 x^{m+(s+t)-h-i}_2 y^{(t+s)}_1 y^{n-(s+t)}_2$$

where $\mathcal{U}(m,n,h,i,s,t) = (-1)^s \binom{h}{s}\binom{n-h}{t} \frac{i!(r-i)!}{(i-t)!(m-h-i+t)!}$.

Changing the summation variable in the inner sum to $j = s+t$, we obtain

$$\alpha_{m,n,h}(f^r_i) = \sqrt{c_{m,n,h}} a^i_r \sum_{s=0}^{h} \sum_{j=\max\{s,-m+i+h+s\}}^{\min\{i+s,\,n-h+s\}} (-1)^s \binom{h}{s}\binom{n-h}{j-s} \frac{i!(r-i)!}{(i-j+s)!(m-h-i+j-s)!} x^{l_{ij}}_1 x^{m-l_{ij}}_2 y^j_1 y^{n-j}_2$$

Finally, as $\dfrac{a_r^i}{a_m^{l_{ij}} a_n^j} = \sqrt{\frac{j!\, l_{ij}!(m-l_{ij})!(n-j)!}{i!(r-i)!}}$, then

$$\alpha_{m,n,h}\left(f_i^r\right) = \sqrt{c_{m,n,h}} \sum_{s=0}^{h} \sum_{j=\max\{s,-m+i+h+s\}}^{\min\{i+s,\, n-h+s\}} (-1)^s \frac{\binom{h}{s}\binom{n-h}{j-s}\binom{m-h}{i-j+s}}{(m-h)!} \sqrt{\frac{r!\ m!\ n!}{\binom{r}{i}\binom{m}{l_{ij}}\binom{n}{j}}}\ f_{l_{ij}}^m\ f_j^n$$

$$= \sum_{s=0}^{h} \sum_{j=\max\{s,-m+i+h+s\}}^{\min\{i+s,\, n-h+s\}} \beta_{i,s,j}^{m,n,h}\ f_{l_{ij}}^m \otimes f_j^n$$

In similar way, As

$$\Delta_{xy}^{n-h} = \sum_{t=0}^{n-h} \binom{n-h}{t} x_1^{n-h-t} x_2^t \frac{\partial^{n-h-t}}{\partial y_1^{n-h-t}} \frac{\partial^t}{\partial y_2^t}$$

and

$$\Omega_{xy}^h = \sum_{s=0}^{h} (-1)^s \binom{h}{s} \frac{\partial^{h-s}}{\partial x_1^{h-s}} \frac{\partial^s}{\partial x_2^s} \frac{\partial^{h-s}}{\partial y_2^{h-s}} \frac{\partial^s}{\partial y_1^s}$$

then by Lemma 2.3.4, we have

$$\alpha_{m,n,h}^*\left(f_l^m \otimes f_j^n\right)$$

$$= \sqrt{c_{m,n,h}}\ a_m^l a_n^j \sum_{t=0}^{n-h} \sum_{s=0}^{h} (-1)^s \binom{h}{s}\binom{n-h}{t} x_1^{n-h-t} x_2^t \frac{\partial^{h-s}}{\partial x_1^{h-s}}\left(x_1^l\right) \frac{\partial^s}{\partial x_2^s}\left(x_2^{m-l}\right) \frac{\partial^{n-h-t+s}}{\partial y_1^{n-h-t+s}}\, y_1^j \frac{\partial^{h-s+t}}{\partial y_2^{h-s+t}}\, y_2^{n-j}$$

$$= \sqrt{c_{m,n,h}}\ a_m^l a_n^j \sum_{s=0}^{h} \sum_{t=0}^{n-h} (-1)^s \binom{h}{s}\binom{n-h}{t} x_1^{n-h-t} x_2^t \frac{\partial^{h-s}}{\partial x_1^{h-s}}\left(x_1^l\right) \frac{\partial^s}{\partial x_2^s}\left(x_2^{m-l}\right) \frac{\partial^{n-h-t+s}}{\partial y_1^{n-h-t+s}}\, y_1^j \frac{\partial^{h-s+t}}{\partial y_2^{h-s+t}}\, y_2^{n-j}$$

but

$$\frac{\partial^{n-h-t+s}}{\partial y_1^{n-h-t+s}}\, y_1^j \frac{\partial^{h-s+t}}{\partial y_2^{h-s+t}}\, y_2^{n-j} = \begin{cases} j!\,(n-j)! & s = t-n+h+j \\ 0 & otherwise \end{cases}$$

and

$$\frac{\partial^{h-s}}{\partial x_1^{h-s}}\left(x_1^l\right) \frac{\partial^s}{\partial x_2^s}\left(x_2^{m-l}\right) = \begin{cases} \frac{l!}{(l-h+s)!}\, x_1^{l-h+s}\ \frac{(m-l)!}{(m-l-s)!}\, x_2^{m-l-s} & h-l \le s \le m-l \\ 0 & otherwise \end{cases}$$

As for $0 \le t \le n-h$ we have $h+j-n \le s \le j$, then

$$\frac{\partial^{h-s}}{\partial x_1^{h-s}}\left(x_1^l\right)\frac{\partial^s}{\partial x_2^s}\left(x_2^{m-l}\right)\frac{\partial^{n-h-t+s}}{\partial y_1^{n-h-t+s}}\,y_1^j\,\frac{\partial^{h-s+t}}{\partial y_2^{h-s+t}}\,y_2^{n-j}$$

$$= \begin{cases} \frac{j!\,(n-j)!l!(m-l)!}{(l-h+s)!(m-l-s)!}\,x_1^{l-h+s}\,x_2^{m-l-s} & \max\{h-l,h+j-n\}\leq s\leq \min\{j,m-l\} \\ \\ 0 & otherwise \end{cases}$$

As for $h+j-n\leq s\leq j$, the condition $h-l\leq s\leq m-l$ is equivalent to $0\leq l+j-h\leq r$, we have

- If l and j satisfy $0\leq l+j-h\leq r$, then

  Hence

$$\alpha^*_{m,n,h}\left(f_l^m\otimes f_j^n\right) = \sqrt{c_{m,n,h}}\,a_m^l a_n^j\sum_{s=\max\{0,h-l,h+j-n\}}^{\min\{h,j,m-l\}}(-1)^s\binom{h}{s}\binom{n-h}{j-s}\frac{j!\,(n-j)!l!(m-l)!}{(l-h+s)!(m-l-s)!}\,x_1^{l+j-h}\,x_2^{r-l-j+h}$$

$$= \left(\sum_{s=\max\{0,h-l,h+j-n\}}^{\min\{h,j,m-l\}}(-1)^s\,\frac{\binom{n-h}{j-s}\binom{h}{s}\binom{m-h}{l-h+s}}{(m-h)!}\sqrt{\frac{c_{m,n,h}r!\,m!\,n!}{\binom{m}{l}\binom{n}{j}\binom{r}{l+j-h}}}\right)a_r^{l+j-h}x_1^{l+j-h}\,x_2^{r-l-j+h}$$

$$= \left(\sum_{s=\max\{0,h-l,h+j-n\}}^{\min\{h,j,m-l\}}\beta^{m,n,h}_{l+j-h,s,j}\right)f^r_{l+j-h}.$$

- Otherwise, $\alpha^*_{m,n,h}\left(f_l^m\otimes f_j^n\right)=0.$

∎

The proof of Corollary 2.3.15

Recall that

$$\varepsilon_{i\,(m,n,h)}^{j} = \sum_{s=\max\{0,j-i,j+h-n\}}^{\min\{h,j,j+m-i-h\}}\beta^{m,n,h}_{i,s,j}$$

where $\beta^{m,n,h}_{i,s,j} = (-1)^s\,\frac{\binom{h}{s}\binom{n-h}{j-s}\binom{m-h}{i-j+s}}{(m-h)!}\sqrt{\frac{c_{m,n,h}r!\;m!\;n!}{\binom{r}{i}\binom{m}{i-j+h}\binom{n}{j}}}.$

Corollary B.1.4. *For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, let $r = m + n - 2h$. The matrix coefficients $\varepsilon_i^j := \varepsilon_{i\,(m,n,h)}^j$ of the isometry $\alpha_{m,n,h}$ satisfy*

1. $\varepsilon_i^j = (-1)^h \varepsilon_{r-i}^{n-j}$ *for any* $0 \leq i \leq r$ *and* $j \in B(i)$.
2. $\varepsilon_i^{i+h} = \beta_{i,h,h+i}^{m,n,h}$ *for any* $i \leq n - h$.
3. *For* $n - h \leq i \leq r$, $\varepsilon_i^n = \beta_{i,h,n}^{m,n,h} = (-1)^h \left|\beta_{i,h,n}^{m,n,h}\right| \neq 0$.
4. *For* $j \in B(0)$, *we have* $\varepsilon_0^j = \beta_{0,j,j}^{m,n,h} = (-1)^j \left|\beta_{0,j,j}^{m,n,h}\right| \neq 0$.
5. *For* $0 \leq i \leq m - h$ *we have* $\varepsilon_i^0 = \beta_{i,0,0}^{m,n,h} \neq 0$.
6. *For* $j \in B(i)$, *we have* $\varepsilon_{i\,(m,n,n)}^j = \beta_{i,j,j}^{m,n,n}$ *and* $\varepsilon_{i\,(m,n,0)}^j = \beta_{i,0,j}^{m,n,0}$

Proof:

(1) Let $g_0 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. By the $SU(2)$-equivariance of $\alpha_{m,n,h}$, we have

$$(\rho_m(g_0) \otimes \rho_n(g_0))\alpha_{m,n,h}\rho_r^*(g_0)(f_i^r) = \alpha_{m,n,h}(f_i^r)$$

for $0 \leq i \leq r$.

As

- $\rho_r^*(g_0)\left(f_i^r\right) = (-1)^{r-i} f_{r-i}^r$,
- $\rho_m(g_0)\left(f_l^m\right) = (-1)^l f_{m-l}^m$, and
- $\rho_n(g_0)\left(f_j^n\right) = (-1)^j f_{n-j}^n$

using Corollary 2.3.13, the above equation can be written as

$$(-1)^h \sum_{s=\max\{0,-m+r-i+h\}}^{\min\{r-i+h,\, n\}} \varepsilon_{r-i}^s\, f_{l_{i(n-s)}}^m \otimes f_{n-s}^n = \sum_{j=\max\{0,-m+i+h\}}^{\min\{i+h,\, n\}} \varepsilon_i^j\, f_{l_{ij}}^m \otimes f_j^n$$

Let $t = n - s$.

Since $n - \max\{0, -m + r - i + h\} = \min\{i + h,\, n\}$, and

$n - \min\{r-i+h,\, n\} = \max\{0, -m+i+h\}$, we have:

$$(-1)^h \sum_{t=\max\{0,-m+i+h\}}^{\min\{i+h,\,n\}} \varepsilon_{r-i}^{n-t}\, f_{l_{it}}^m \otimes f_t^n = \sum_{j=\max\{0,-m+i+h\}}^{\min\{i+h,\,n\}} \varepsilon_i^j\, f_{l_{ij}}^m \otimes f_j^n$$

By the linearly independence of the vectors $f_l^m \otimes f_j^n$, the last equality implies that $(-1)^h \varepsilon_{r-i}^{n-j} = \varepsilon_i^j$ for any j such that $\max\{0, -m+i+h\} \le j \le \min\{i+h,\, n\}$.

The other statements follow by direct computations. ∎

The proof of Lemma 2.4.11

Lemma B.1.5. *For $m \in \mathbb{N} \setminus \{0\}$.*

$$\sum_{k=0}^{m-1} \frac{\binom{m-1}{k}^2}{\binom{m}{k+1}\binom{m}{k}} = \frac{m(m+1)(m+2)}{6m^2}$$

Proof:

$$\sum_{k=0}^{m-1} \frac{\binom{m-1}{k}^2}{\binom{m}{k+1}\binom{m}{k}} = \frac{1}{m^2}\sum_{k=0}^{m-1}(k+1)(m-k) = \frac{1}{m^2}\sum_{k=1}^{m} k(m-k+1) = \frac{1}{m^2}\left[\sum_{k=1}^{m} k(m+1) - \sum_{k=1}^{m} k^2\right]$$

Since

$$\sum_{k=1}^{m} k = \frac{m(m+1)}{2}, \text{ and } \qquad \sum_{k=1}^{m} k^2 = \frac{m(m+1)(2m+1)}{6} \text{ the result follows.}$$ ∎

Recall that $B(i) := \{j : \max\{0, -m+i+h\} \le j \le \min\{i+h,\, n\}\}$.

Lemma B.1.6. *Let $m \in \mathbb{N} \setminus \{0\}$ and $\varepsilon_i^j := \varepsilon_{i\,(m,m,m-1)}^j$. The following identities hold*

1. $\varepsilon_0^j = (-1)^j \sqrt{\frac{6(j+1)(m-j)}{m(m+1)(m+2)}}$ *for* $0 \le j \le m-1$.

2. $\varepsilon_1^j = (-1)^j \sqrt{\frac{3}{m(m+1)(m+2)}}(m-2j)$ *for* $0 \le j \le m$.

3. $\varepsilon_2^j = (-1)^{j-1}\sqrt{\frac{6j(m-j+1)}{m(m+1)(m+2)}}$ *for* $1 \le j \le m$.

Proof:

1. For $j \in B(0) = \{j : 0 \le j \le m-1\}$, using Lemma B.1.5, we have

$$\varepsilon_0^j = \sum_{s=\max\{0,j,j-1\}}^{\min\{m-1,j,j+1\}} \beta_{0,s,j}^{m,m,m-1} = \sum_{s=j}^{j} \beta_{0,s,j}^{m,m,m-1} = \beta_{0,j,j}^{m,m,m-1} = (-1)^j\sqrt{\frac{6(j+1)(m-j)}{m(m+1)(m+2)}}$$

2. For $j \in B(1) = \{j : 0 \le j \le m\}$, we have

$$\varepsilon_1^j = \sum_{s=\max\{0,,j-1\}}^{\min\{m-1,j\}} \beta_{1,s,j}^{m,m,m-1} = \begin{cases} \beta_{1,0,0}^{m,m,m-1} & j=0 \\ \beta_{1,j-1,j}^{m,m,m-1} + \beta_{1,j,j}^{m,m,m-1} & 1 \le j \le m-1 \\ \beta_{1,m-1,m}^{m,m,m-1} & j=m \end{cases}$$

by Lemma B.1.5, we get:

- $\beta_{1,0,0}^{m,m,m-1} = \sqrt{\frac{3m}{(m+1)(m+2)}}$.
- $\beta_{1,j-1,j}^{m,m,m-1} + \beta_{1,j,j}^{m,m,m-1} = (-1)^j\sqrt{\frac{3}{m(m+1)(m+2)}}(m-2j)$ for any $1 \le j \le m-1$.
- $\beta_{1,m-1,m}^{m,m,m-1} = (-1)^{m-1}\sqrt{\frac{3m}{(m+1)(m+2)}}$.

In all cases, we have $\varepsilon_1^j = (-1)^j\sqrt{\frac{3}{m(m+1)(m+2)}}(m-2j)$.

3. Similarly for $j \in B(2) = \{j : 1 \le j \le m\}$, we have

$$\varepsilon_2^j = \sum_{s=\max\{0,,j-2,j-1\}}^{\min\{m-1,j,j-1\}} \beta_{2,s,j}^{m,m,m-1} = \sum_{s=,j-1}^{,j-1} \beta_{2,s,j}^{m,m,m-1} = \beta_{2,j-1,j}^{m,m,m-1} = (-1)^{j-1}\sqrt{\frac{6j(m-j+1)}{m(m+1)(m+2)}}.$$

∎

B.2 Proofs in chapter 5

The proof of Theorem 5.2.2

Recall the definition of direct sum of operator in Definition 5.2.1.

Theorem B.2.1. Let G be a group. Let $H = \bigoplus_{t=1}^{r} W_t$ where $\{W_t : 1 \leq t \leq r\}$ are nonequivalent G-irreducible spaces, and $K = \bigoplus_{s=1}^{m} V_s$ where $\{V_s : 1 \leq s \leq m\}$ are nonequivalent G-irreducible space. If there exist $k \in \mathbb{N}$, such that

1. For each $1 \leq t \leq k$, $W_t \simeq V_t$ via a G-equivariant isomorphism
$$\psi_t : W_t \longrightarrow V_t$$
2. For each $t > k$ the subspace W_t is not equivalent to any of the V_s for any $1 \leq s \leq m$.

Then, for any G-equivariant map $\Phi : H \longrightarrow K$, there exist $\lambda_1, \lambda_2, \ldots\ldots\ldots, \lambda_k$ such that Φ is the orthogonal direct sum of the operators $\{\lambda_t \psi_t : 1 \leq t \leq k\}$

i.e.
$$\Phi = \bigoplus_{t=1}^{k} \lambda_t \psi_t$$

Proof:

By the assumption in (1) and (2), and since the multiplicities of the subspaces W_t and V_s, in H and K are one, we have $W_t \ncong V_s$ for any $s \neq t$. Let ι_t, ι_s and q_t, q_s denote the inclusion maps, and the orthogonal projections of W_t and V_s respectively. As the maps ι_t, ι_s,q_t, q_s are G-equivariant maps (Lemma 1.2.10), the maps composition
$$q_s \Phi \iota_t : W_t \longrightarrow V_s$$
is G-equivariant for any any $1 \leq s \leq m$ and $1 \leq t \leq r$. By Schur's Lemma 1.2.12, the map $q_s \Phi \iota_t$ is a zero map for $s \neq t$.

If $s = t$, then by Schur's Lemma a gain, the map $\psi_t^{-1} q_t \Phi \iota_t : W_t \longrightarrow W_t$ is multiple of the identity. i.e. $\psi_t^{-1} q_t \Phi \iota_t = \lambda_t I_{W_t}$ for some $\lambda_t \in \mathbb{C}$. That is

$$\Phi\mid_{W_t} = \lambda_t \psi_t$$

For $u \in H = \bigoplus_{t=1}^{r} W_t$, we have

$$\Phi(u) = \Phi(u_1, u_2, ...u_r) \qquad u_t \in W_t$$

Thus

$$\Phi(u) = (\lambda_1 \psi_1(u_1), \lambda_2 \psi_2(u_2), ..., \lambda_k \psi_k(u_k), 0, .., 0)$$

∎

B.3 Proofs in Chapter 7

The proof of Lemma 7.2.4

Recall that for $m \in \mathbb{N} \setminus \{0\}$, the EPOSIC Kraus channel $\Phi_{m,1,1} : End(P_{m-1}) \longrightarrow End(P_m)$ has two Kraus operator $\{T_0, T_1\}$ (Definition 4.2.1). For a pure state $\varrho = ww^*$ in $End(P_{m-1})$, the set $U_{\Phi_{m,n,n,\varrho}} = \{u_0, u_1\}$ where $u_j = T_j w$, $j = 1, 2$, by Remark 6.1.8, we have $\Phi_{m,1,1}(ww^*) = \sum_{j=0}^{i} u_j u_j^*$. The following lemma follows by direct computations using the formula $\varepsilon_{i\,(m,n,h)}^{j} = \sum_{s=\max\{0,j-i,j+h-n\}}^{\min\{h,j,j+m-i-h\}} \beta_{i,s,j}^{m,n,h}$ given in Corollary 2.3.13. Item (3) follows as $\Phi_{m,1,1}$ is trace preserving.

Lemma B.3.1. *For $m \in \mathbb{N} \setminus \{0\}$ and $\varepsilon_i^j := \varepsilon_{i\,(m,1,1)}^{j}$, we have*

1. $\varepsilon_l^0 = \sqrt{\frac{l+1}{m+1}}$, $\quad \varepsilon_l^1 = -\sqrt{\frac{m-l}{m+1}}$, $\quad$ *and* $(\varepsilon_l^0)^2 + (\varepsilon_l^1)^2 = 1$, $\qquad$ *for* $0 \le l \le m-1$.
2. $(\varepsilon_l^0)^2 = (\varepsilon_{l-1}^0)^2 + \frac{1}{m+1}$, $\quad$ *and* $(\varepsilon_{l-1}^1)^2 = (\varepsilon_l^1)^2 + \frac{1}{m+1}$, $\qquad$ *for* $1 \le l \le m-1$.

3. $\|u_0\|^2 + \|u_1\|^2 = 1$.

Following the same notations in Proposition 7.2.3, we have

Lemma B.3.2. *Let $m \in \mathbb{N} \setminus \{0\}$. The minimal value of $R = \|u_0\|^2 \|u_1\|^2 - |\langle u_0 | u_1 \rangle|^2$ is $\frac{m}{(m+1)^2}$.*

Proof:

Let $w = \sum_{l=0}^{m-1} w_l f_l^{m-1} \in P_{m-1}$ be a unit vector. By Lemma 7.1.5, we have
$u_0 = \sum_{l=1}^{m} \varepsilon_{l-1}^0 w_{l-1} f_l^m$ and $u_1 = \sum_{l=0}^{m-1} \varepsilon_l^1 w_l f_l^m$.
Thus

$$\langle u_0 | u_1 \rangle = \sum_{l=1}^{m-1} \varepsilon_{l-1}^0 \overline{w}_{l-1} \varepsilon_l^1 w_l = \sum_{l=1}^{m-1} \varepsilon_{l-1}^0 w_l \varepsilon_l^1 \overline{w}_{l-1} = \langle v_0 | v_1 \rangle$$

where $v_0 = \sum_{l=1}^{m-1} \varepsilon_{l-1}^0 w_l f_l^m$, and $v_1 = \sum_{l=1}^{m-1} \varepsilon_l^1 w_{l-1} f_l^m$.

Using Lemma B.3.1, we obtain

$$\|v_0\|^2 = \sum_{l=1}^{m-1} \left(\varepsilon_{l-1}^0\right)^2 |w_l|^2 = \sum_{l=1}^{m-1} \left(\varepsilon_{l-1}^0\right)^2 |w_l|^2 + \frac{\|w\|^2}{m+1} - \frac{\|w\|^2}{m+1}$$

$$= \frac{1}{m+1} |w_0|^2 + \sum_{l=1}^{m-1} \left(\left(\varepsilon_{l-1}^0\right)^2 + \frac{1}{m+1}\right) |w_l|^2 - \frac{\|w\|^2}{m+1}$$

$$= \left(\varepsilon_0^0\right)^2 |w_0|^2 + \sum_{l=1}^{m-1} \left(\varepsilon_l^0\right)^2 |w_l|^2 - \frac{1}{m+1}$$

Note that $\|w\|^2 = \sum_{l=0}^{m-1} |w_l|^2 = 1$.
Thus

$$\|v_0\|^2 = \sum_{l=0}^{m-1} \left(\varepsilon_l^0\right)^2 |w_l|^2 - \frac{1}{m+1} = \sum_{l=1}^{m} \left(\varepsilon_{l-1}^0\right)^2 |w_{l-1}|^2 - \frac{1}{m+1} = \|u_0\|^2 - \frac{1}{m+1}$$

Similarly $\|v_1\|^2 = \|u_1\|^2 - \frac{1}{m+1}$. So

$$|\langle u_0 | u_1 \rangle|^2 = |\langle v_0 | v_1 \rangle|^2 \leq \|v_0\|^2 \|v_1\|^2 = \left(\|u_0\|^2 - \frac{1}{m+1}\right)\left(\|u_1\|^2 - \frac{1}{m+1}\right)$$

$$= \|u_0\|^2 \|u_1\|^2 - \tfrac{1}{m+1} \left(\|u_0\|^2 + \|u_1\|^2\right) + \tfrac{1}{(m+1)^2} = \|u_0\|^2 \|u_1\|^2 - \tfrac{m}{(m+1)^2}$$

Thus

$$R = \|u_0\|^2 \|u_1\|^2 - |\langle u_0 | u_1 \rangle|^2 \geq \tfrac{m}{(m+1)^2}$$

and $\frac{m}{(m+1)^2}$ is a lower bound for R. To verify that $\frac{m}{(m+1)^2}$ is the minimal value of R, compute R at $w_0 = (1, 0, \ldots, 0)^t$ to get $R_{w_0} = \frac{m}{(m+1)^2}$. ∎

Appendix C

List of Equations That Are Used in The Computation

For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq \min\{m, n\}$, let $r = m + n - 2h$ then

- $c_{m,n,h} = \dfrac{((m-h)!)^2}{r!\ m!\ n! \left(\displaystyle\sum_{j=0}^{h} \frac{\binom{h}{j}^2}{\binom{m}{h-j}\binom{n}{j}} \right)}$

- $\beta_{i,s,j}^{m,n,h} = (-1)^s \, \dfrac{\binom{h}{s}\binom{n-h}{j-s}\binom{m-h}{i-j+s}}{(m-h)!} \sqrt{\dfrac{c_{m,n,h} r!\ m!\ n!}{\binom{r}{i}\binom{m}{i-j+h}\binom{n}{j}}}.$

- $\varepsilon_{i\,(m,n,h)}^{j} = \displaystyle\sum_{s=\max\{0,j-i,j+h-n\}}^{\min\{h,j,j+m-i-h\}} \beta_{i,s,j}^{m,n,h}.$

- $l_{ij} = h + i - j.$

- For $0 \leq i \leq r$, $B(i) = \{j : \max\{0, -m+i+h\} \leq j \leq \min\{i+h,\, n\}\}.$

- $\left\{f_l^m = a_m^l x_1^l x_2^{m-l} : 0 \leq l \leq m\right\}$ where $a_m^l = \frac{1}{\sqrt{l!(m-l)!}}$.

- $J_m(f_l^m) = (-1)^l f_{m-l}^m$ and $J_m^*(f_l^m) = (-1)^{m-l} f_{m-l}^m$.

- $P_m \otimes P_n \simeq \bigoplus_{h=0}^{\min\{m,n\}} P_{m+n-2h}$.

- $\alpha_{m,n,h}\left(f_i^r\right) = \sum_{j \in B(i)} \varepsilon_i^j{}_{(m,n,h)}\, f_{l_{ij}}^m \otimes f_j^n$.

- $\eta_{m,n,h} = \left(I_{P_m} \otimes J_n\right) \alpha_{m,n,h} : P_{m+n-2h} \longrightarrow P_m \otimes \overline{P}_n$.

- $\alpha_{m,n,h}^*\left(f_l^m \otimes f_j^n\right) = \begin{cases} \varepsilon_{l+j-h}^j f_{l+j-h}^r & if \quad 0 \leq l+j-h \leq r \\ \\ 0 & otherwise \end{cases}$.

- $\Phi_{m,n,h}(f_{i_1}^r f_{i_2}^{r^*}) = \sum_{j \in B(i_1) \cap B(i_2)} \varepsilon_{i_1}^j \varepsilon_{i_2}^j f_{l_{i_1 j}}^m f_{l_{i_2 j}}^{m^*}$.

- $C(\Phi_{m,n,h}) = \sum_{i_1, i_2 = 0}^{r} \left(\sum_{j \in B(i_1) \cap B(i_2)} \varepsilon_{i_1}^j \varepsilon_{i_2}^j f_{l_{i_1 j}}^m f_{l_{i_2 j}}^{m^*} \right) \otimes E_{i_1 i_2}$.

- $C(\Phi_{m,n,h}) = \frac{r+1}{n+1} q_{m,r,m-h}$.

- $\lambda_{2t} = \frac{\sum_{j=m-h}^{r} (-1)^{t+j} \varepsilon_t^j{}_{(r,r,r-t)} \left(\varepsilon_{r-j}^{r-j+h}{}_{(m,n,h)}\right)^2}{m! \sqrt{c_{m,m,m-t}}}$

- $\sum_{k=1}^{m} k = \frac{m(m+1)}{2}$, and $\sum_{k=1}^{m} k^2 = \frac{m(m+1)(2m+1)}{6}$.

- $\sum_{k=1}^{m} k(m-k+1) = \frac{m(m+1)(m+2)}{6}$ and $\sum_{k=1}^{m} k(k+1) = \frac{m(m+1)(m+2)}{3}$.

Bibliography

[1] G. Amosov, A. Holevo and R. Werner, On some additivity problems in Quantum Information Theory, *Probl. Inf. Transm* **36** (2000) 305-313.

[2] C.H. Bennett and P.W. Shor, Quantum Information Theory, *IEEE Trans. Info. Theory*, Vol **44** (6) (1998) 2724–2748.

[3] T. Brocker and T. Dieck, **Representations of Compact Lie Groups**, Springer-Verlag New York Inc. 1985.

[4] L. Chen, and D. Dokovic, Distillability and PPT entanglement of low-rank quantum states, *Journal of Physics. A, Mathematical and Theoretical*, **44** (28) (2011).

[5] M. Choi, Completely positive linear maps on complex matrices, *Linear Algebra. Appl.* **10** (1975) 285-290.

[6] Y. Eidelman, V. Milman, and A. Tsolomitis, **Functional analysis An introduction**, American Mathematical Society, Volume **66**, ISBN 0-8218-3646-3.

[7] M. Fannes, B. Haegeman, M. Mosonyi, and D. Vanpeteghem, Additivity of minimal entropy output for a class of covariant channels, preprint (2004), arXiv: quant-ph/0410195.

[8] G. Folland, **A course in Abstract Harmonic Analysis**, CRC press, 1995.

[9] W. Fulton and J. Harris, **Representation Theory A first Course**, Springer-Verlag,1991.

[10] P. Harpe and V. Jones. An introduction to C^*-Algebras. Chapter 1 to 9. Universite de Geneve. Section de Mathematiques, 1995.

[11] M. Hastings, Super additivity of communication capacity using entangled inputs, *Nature Physics* **5** (2009) 255-257.

[12] M. Hayashi, **Quantum Information An Introduction**, Springer-Verlag Berlin Heidelberg, 2006.

[13] E. Hewitt and K. A. Ross **Abstract Harmonic Analysis I**, Second Edition, A Series of Comprehensive studies in Mathematics 115, Springer-Verlag, 1979.

[14] A. Holevo, Additivity conjecture and covariant channel, *Int. J. Quant.Inform.* **3** (1) (2005) 41-48.

[15] A. Holevo, Complementary channel and the additivity problem, *Theory Probab. Appl.* Vol **51** (1) (2007) 92-100.

[16] A. Holevo, **Quantum systems, Channels, Information: A Mathematical Introduction**, Walter de Gruyter GmbH, Berlin/Boston, 2012.

[17] A. Holevo, The additivity problem in quantum information theory, Section Lectures, ICM 2006 Madrid, Mathematical Aspect of Computer Science, 2006.

[18] A. Holevo, The capacity of quantum communication channel with general signal states, *IEEE Trans. Inform. Theory* **44** (1) (1998) 269-272.

[19] A. Holevo and V. Giovannetti, Quantum channels and their entropic characteristics, *Rep. Prog. Phys.***75** (2012) 046001 (30pp).

[20] M. Horodecki, P. Shor, and M. Ruskai, General Entanglement Breaking Channels, *Rev.Math.Phys* **15**, (2003) 629-641 .

[21] P. Horodecki, J.Smolin, B.Terhal, and A.Thapliyal, Rank two bipartite bound entangled states do not exist, em J. Theor. Computer Science **292**, (2003) 589-596.

[22] M. Horodecki, and M. Horodecki, Reduction criterion of separability and limits for a class of protocols of entanglement distillation, preprint (1998), arXiv: quant-ph/9708015.

[23] A. Jamiołkowski, Linear transformations which preserve trace and positive semi definiteness of operators, *Reports on Mathematical Physics*, **3** (4) (1972) 275-278.

[24] C. King, Additivity for unital qubit channels, *Journal of Mathematical Physics.* Vol **43**(10), 2002.

[25] C. King and M. Ruskai, Minimal entropy of states emerging from noisy quantum channels, *IEEE Tran. Info. Theory*, **47**, 192-209 (2001).

[26] C. King, The capacity of the quantum depolarizing channel, *IEEE Transactions on Information Theory*, **49**, 221 (2003).

[27] M. Nielsen, I. Chuang, **Quantum Computation and Quantum Information**, Cambridge university press,UK, 2000.

[28] V. Paulsen, **Completely bounded maps and operator algebras**, Cambridge university press, UK, 2002.

[29] C. Procesi, **Lie Groups An Approach through Invariants and Representations**, Springer Science+ Business Media, LLC, 2007.

[30] A. Robert, **Introduction to the Representation Theory of Compact and Locally Compact Groups**, Cambridge University Press, UK, 1983.

[31] W. Rudin, **Functional Analysis**, McGraw-Hill, Inc. (1973).

[32] B. Schumacher, and M. Westmoreland, Sending classical information via noisy quantum channel, *Phys.Rev.A* **56** (1) (1997) 131-138.

[33] J.-P. Serre, **Linear Representations of Finite Groups**, Springer-Verlag New York Inc. 1977.

[34] P. Shor, Additivity of the Classical Capacity of Entanglement-Breaking Quantum channels, *J.Math.Phys.*Vol **43**, (9) (2002) 4334-4340 .

[35] P. Shor, Capacities of quantum channels and how to find them, *Mathematical Programming* **97** (2003) 311-335 .

[36] P. Shor, Equivalence of additivity questions in quantum information theory, *Commun. Math. Phys.* **246** (3) (2004).

[37] B. Simon, **Representation of finite and compact groups**, American Mathematical Society, Graduate Studies in Mathematics, Volume **10**, (1996).

[38] S. Sternberg, **Group Theory And Physics**, Cambridge University Press, UK, 1994.

[39] N.Ja. Vilenkin, A.U. Klimyk, **Representation of Lie Groups and Special Functions**, Volume **1** :Simplest Lie Groups, Special Functions and Integral Transforms. Kluwer academic publishers. Dordrecht/Boston/London, 1991.

[40] K.Vollbrecht and R. Werner, Entanglement measures under symmetry, *Phys.Rev.A* **64**, 2011.

[41] J. Watrous, CS 766/QIC Theory of Quantum Information, Lectures, Institute for Quantum Computing, University of Waterloo (Fall 2011).