이학 석사학위논문

Some Properties of SU(2)-Irreducibly Covariant Quantum Channels

(SU(2)에 기약으로 공변하는 양자채널의 성질)

2016년 2월

서울대학교 대학원

수 리 과 학 부

신 재 혁

SU(2)에 기약으로 공변하는 양자채널의 성질

Some properties of SU(2)-irreducibly covariant quantum channels

Some properties of SU(2)-irreducibly covariant quantum channels

by

Shin, Jae-Hyeok

Department of Mathematical Sciences

Seoul National University

A thesis submitted to the faculty of Seoul National University in partial fulfillment of the requirements for the degree of Master of Science in the Department of Mathematical Sciences . The study was conducted in accordance with Code of Research Ethics[1].

2015. 12. 9.

Approved by

Professor Lee, Hun Hee

[Advisor]

---

[1]Declaration of Ethical Conduct in Research: I, as a graduate student of Seoul National University, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance of my thesis advisor.

MMAS
2014-21188

신 재 혁. Shin, Jae-Hyeok. Some properties of SU(2)-irreducibly covariant quantum channels. SU(2)에 기약으로 공변하는 양자채널의 성질. Department of Mathematical Sciences . 2016년 2월. 25p. Advisor Prof. Lee, Hun Hee. Text in English.

ABSTRACT

In quantum information theory, there are few quantum channels whose specific formulas and properties are known. In this thesis, we introduce EPOSIC channels, a class of SU(2)-irreducibly covariant quantum channels, and compute their χ-capacity and entropy in some cases. We review the basics of group representation theory and quantum information theory, and we construct EPOSIC channels, a new class of quantum channels, using representation theory. We also study specific formulas and properties of EPOSIC channels.

Keywords: SU(2), EPOSIC channel, quantum channel
Student number: 2014-21188

Contents

Chapter 1. Introduction

Quantum information theory is a branch of science that quantum mechanics and information theory are combined. One of the important open questions in quantum information theory 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 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 [5]. The additivity conjecture in quantum information is that the classical capacity of a quantum channel is additive. A fundamental result of quantum information theory, "the quantum coding theorem" [7] and [8], implies that the classical capacity of a quantum channel Φ is given by

$$\lim_{n\to\infty} \frac{C_\chi(\Phi^{\otimes n})}{n}$$

where C_χ is the Holevo capacity. This shows that the additivity of the classical capacity can be inferred from the additivity of another quantity, known as the Holevo capacity. So, it is important to find counter-example of the additivity of the Holevo capacity or to prove the additivity of the Holevo capacity for some class of quantum channels. In 2008, Hastings [9] showed the existence of a counter-example to the additivity of the Holevo capacity, using a random construction. However, no explicit example was given. Moreover, there are few quantum channels whose specific formulas and properties are well-known.

In this thesis, we present a new class of quantum channels whose specific formulas is well-known from representation theory. And study their properties. The thesis consists of six chapters. In chapter 1, we introduce our motivation of the study. In chapter 2, we review the basic definitions and state all the related propositions and theorem from representation theory. Chapter 3 contains the definitions and all needed proposition about quantum channels. In chapter 4, we review the basic definitions and state all the related propositions from quantum information theory. Chapter 5 studies unitary representation of the compact group SU(2), and defines an SU(2)-equivariant isometry, and construct EPOSIC channels. And see that EPOSIC channels are the extreme points of SU(2)-irreducibly covariant channels. Chapter 6 studies the properties of SU(2)-irreducibly covariant channels.

Chapter 2. Basics in representation theory

In this thesis, we assume all vector spaces to be finite dimensional complex vector spaces. The construction of EPOSIC channels, to be introduced in chapter 5, depends heavily on the representations of the compact group SU(2). The present chapter contains background definitions and results from reprentation theory needed for the thesis. For more details, we refer the reader to [2].

Definition 2.1 (Topological group).
A topological group is a group G equipped with a topology with respect to which the group operations are continuous. i.e. $(x, y) \to xy$ and $x \to x^{-1}$ are both continuous. A compact group is a topological group whose topology is compact.

For example, the unit circle under complex multiplication with the usual topology is a compact topological group. For another example, the set of real numbers under the usual addition with the usual topology is a non-compact topological group.

Definition 2.2 (Unitary representation).
Let G be a topological group and H be a Hilbert space.
A unitary representation of G in H is a group homomorphism π from G into the group $U(H)$ of unitary operators on H that is continuous with repect to the strong operator topology.
That is, a map $\pi : G \to U(H)$ that satisfies $\pi(xy) = \pi(x)\pi(y)$ and $\pi(x^{-1}) = \pi(x)^{-1} = \pi(x)^*$, and $x \to \pi(x)u$ is continuous from G to H for any $u \in H$.
In this case, H is called the representation space of π.

For example, the group $SU(n)$ has representations in $\mathbb{C}^n$ given by matirx multiplication for any $n \in \mathbb{N}$.

Definition 2.3 (Irreducible representation).
Let (H, π) be a unitary representation of a topological group G. Suppose M is a closed subspace of H. M is called an invariant subspace for π if $\pi(g)M \subset M$ for all $g \in G$. If M is invariant and nontrivial, then the restriction of π to M, $\pi^M(g) = \pi(g)|M$, defines a representation of G on M, called a subrepresentation of π.
If π admits an invariant subspace that is nontrivial, then π is called reducible, otherwise π is irreducible.

We now introduce some standard terminology associated to unitary representations.

Definition 2.4 (G-equivariant map)**.** *[2]*
Let (H, π_H) *and* (K, π_K) *be two unitary representations of a topological group G.*
A G-equivariant map for π_H *and* π_K *is a bounded linear map* $T : H \to K$ *such that* $T\pi_H(g) = \pi_K(g)T$ *for all* $g \in G$.
A G-equivariant map is called an intertwing operator or an intertwiner.
The set of G-equivariant maps forms a vector spacae, denoted $B(H, K)^G$ *or* $C(\pi_H, \pi_K)$.
π_H *and* π_K *are (unitarily) G-equivalent if* $B(H, K)^G$ *contains a unitary operator* U, *so that* $\pi_K(x) = U\pi_H U^{-1}$.
In such a case, the spaces H *and* K *are called G-equivalent, or G-isomorphic.*

Definition 2.5.
Let H be a Hilbert space with orthonormal basis$=\{e_1, e_2, \cdots, e_n\}$.
Then un-normalized trace on B(H) is defined by the linear map

$$tr : B(H) \to \mathbb{C}$$
$$T \mapsto tr(T) = \sum_{i=1}^{n} < e_i|Te_j >_H$$

The definition of the trace does not depend on the choice of the basis.

If H and K are finite-dimensional, then B(H,K) is a Hilbert space endowed with the Hilbert-Schmidt inner product given by

$$< A|B >_{B(H,K)}= tr(A^*B) \ for \ A, B \in B(H, K)$$

Proposition 2.6.
Let (H, π_H) *and* (K, π_K) *be two unitary representations of a topological group G.*
Then the maps

$$\begin{aligned} \pi_H \otimes \pi_K : G &\to U(H \otimes K) \\ g &\mapsto \pi_H(g) \otimes \pi_K(g) \\ \pi_H \oplus \pi_K : G &\to U(H \oplus K) \\ g &\mapsto \pi_H(g) \oplus \pi_K(g) \\ \pi_{H,K} : G &\to U(B(H, K)) \\ g &\mapsto \pi_K(g)A\pi_H(g^{-1}) \end{aligned}$$

define unitary representations of G in $H \otimes K$, $H \oplus K$, $B(H, K)$ *respectively.*

Proof. Since the techniques to prove the three cases are same, we show only for $\pi_{H,K}$. It is straight forward to show that $\pi_{H,K}$ is a group homomorphism. And $\pi_{H,K} \in B(B(H, K))$ trivially.
Let $A, B \in B(H, K)$. Then

$$\begin{aligned} < A|\pi_{H,K}(g)B >_{B(H,K)} &= tr(A^*\pi_K(g)B\pi_H(g^{-1})) = tr(\pi_H(g^{-1})A^*\pi_K(g)B) \\ &= tr((\pi_{H,K}(g^{-1})A)^*B) =< \pi_{H,K}(g^{-1})A|B >_{B(H,K)} \end{aligned}$$

By the uniqueness of the adjoint map, we have $(\pi_{H,K}(g))^* = \pi_{H,K}(g^{-1})$.
By construction, $\pi_{H,K}$ is continuous with respect to the strong operator topology.

□

From now on, unless specified otherwise, the representation of G on $H \otimes K$, $H \oplus K$, *and* $B(H, K)$ will be taken to be the one as given in Proposition 2.6.

Proposition 2.7. *[1]*
Let (H, π_H) and (K, π_K) be two unitary representations of a topological group G.

The map $\Phi : B(H) \to B(K)$ 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* $A \in B(H)$ *and* $g \in G$

Proposition 2.8.
For i=1,2, let (H_i, π_{H_i}) and (K_i, π_{K_i}) be representations of a group G.
And let $\Phi_i : B(H_i) \to B(K_i)$ be G-equivariant maps. Then
i) 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.
ii) If Φ_1 and Φ_2 are composable, then their composition is also G-equivariant.

Example 2.9.
Let (H, π_H) and (K, π_K) be two unitary representations of a topological group G.
Define the linear map by

$$Tr_H : B(H \otimes K) \to B(K)$$
$$A \otimes B \mapsto tr(A)B$$

and extended by linearity, which is called the partial trace over H.
Then Tr_H is a G-equivariant map.

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

$$\begin{aligned}
&Tr_H((\pi_H(g) \otimes \pi_K(g))(A_1 \otimes A_2)(\pi_H^*(g) \otimes \pi_K^*(g))) \\
&= Tr_H(\pi_H(g)A_1\pi_H^*(g) \otimes \pi_K(g)A_2\pi_K^*(g)) = tr(\pi_H(g)A_1\pi_H^*(g))\pi_K(g)A_2\pi_K^*(g) \\
&= tr(A_1)\pi_K(g)A_2\pi_K^*(g) = \pi_K(g)Tr_H(A_1 \otimes A_2)\pi_K^*(g)
\end{aligned}$$

□

Example 2.10.
Let (H, π_H) and (K, π_K) be two unitary representations of a topological group G.
Define the linear map by

$$Ad_\alpha : B(H) \to B(K)$$
$$A \mapsto \alpha A \alpha^*$$

which is called the conjugation by α. Then
1. If α is G-equivariant, then α^* is G-equivariant.
2. If α is G-equivariant, then Ad_α is G-equivariant.

The following proposition is one of the fundamental result in representation theory relating operators in $B(H,K)^G$ to reducibility properties of π.

Proposition 2.11 (Schur's Lemma)**.** *[2]*
Let (H, π_H) and (K, π_K) be two unitary representations of G. If $\alpha : H \to K$ is a G-equivariant map, then either $\alpha \equiv 0$ or α is a G-isomorphism. In case of H=K and $\pi_H = \pi_K$, then $\alpha = cI_H$ for some $c \in \mathbb{C}$.

Corollary 2.12. *Let (H, π_H) be a unitary representation of G. Any two non isomorphic G-irreducible subspaces of H are mutually orthogonal.*

Proof. Let W_1 and W_2 be two non isomorphic G-irreducible subspaces of H, and let q_{W_1} and q_{W_2} be the associated orthogonal projections.

$$Claim: \ q_{W_i} \ are \ G-equivariant \ for \ i=1,2.$$

It's enough to show that for i=1. Let $h \in H \cong W \oplus W^{\perp}$. Then h=x+y for some $x \in W$ and $y \in W^{\perp}$. Then

$$q_{W_1}\pi_H(g)(h) = q_{W_1}(\pi_H(g)(x) + \pi_H(g)(y)) = \pi_H(g)(x) = \pi_H(g)q_{W_1}(h)$$

That is, q_{W_1} is G-equivariant. $\Diamond$

So $q_{W_1}q^*_{W_2} = q_{W_1}\iota_{W_2} : W_2 \to W_1$ is G-equivariant. Since W_1 and W_2 are non isomorphic, by Schur's lemma, $q_{W_1}\iota_{W_2} \equiv 0$. That is, W_1 and W_2 are orthogonal. □

Among many topological groups, compact groups have remarkable properties. We present the basic results of unitary representations of compact groups.

Proposition 2.13. *[2]*
If G is compact, then
1. every irreducible representation of G is finite dimensional.
2. every unitary representation of G is a direct sum of irreducible representations.

Proposition 2.14. *[11]*
Let (H, π_H) be an unitary representation of a compact group G.
There exists a decomposition

$$H = M_1^{\oplus c_1} \oplus M_2^{\oplus c_2} \oplus \cdots \oplus M_k^{\oplus c_k}$$

where M_i: G-irreducible distinct subspaces

Chapter 3. Basics in quantum channels

Quantum channels are the objects we mainly treat in the thesis. This chapter contains background definitions and propositions from both operator algebra and the quantum information theory about quantum channels which is needed to our study. For more details, we refer the reader to [4], [5], and [6].

Definition 3.1 (Completely positive maps)**.** *[4]*
Let H and K be Hilbert spaces. A linear map $\Phi : B(H) \to B(K)$ is said to be
- positive if $\Phi(A) \geq 0$ for any positive matrix $A \in B(H)$
- n-positive if $\Phi \otimes I_n$ is positive, where $\Phi \otimes I_n : B(H) \otimes \mathbb{M}_n(\mathbb{C}) \to B(K) \otimes \mathbb{M}_n(\mathbb{C})$ is the linear map such that $\Phi \otimes I_n(A \otimes B) = \Phi(A) \otimes B$ for $A \in B(H)$ 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 postive. However, the converse is not true. For example [12] p.5, the transpose map $T : \mathbb{M}_n(\mathbb{C}) \to \mathbb{M}_n(\mathbb{C})$ defined by taking $A \mapsto A^t$ is an example of a positive map that is not completely positive.
Now we introduce a quantum system which we treat in the thesis. A formal definition of a state is the following.

Definition 3.2. *[5]*
Let H be a Hilbert space.
1. A state is a density operator $\rho \in B(H)$, i.e, a positive operator in $B(H)$ taht has trace one.
Denote D(H) the set of all states of H, i.e. $D(H) = \{\rho \in B(H) : \rho \geq 0, tr(\rho) = 1\}$.
2. A state that is a rank one projection is called a pure state. An impure state is called a mixed state. Denote P(H) the set of all pure states of H.
i.e. $P(H) = \{\rho = ww^* : w \text{ is an unit vector in } H\}$.
3. The maximally mixed state of H is the state $\frac{1}{d_H} I_H$.

In quantum information theory, a quantum channel is a communication channel which can transmit quantum information between two quantum system. As Definition 3.2, since a quantum state is positive and has trace one, the output state transmitted by a quantum channel must be positve and have trace one. So, we can guess a quantum channel must be positve and trace-preserving.

Definition 3.3. *[4]*
A quantum channel $\Phi : B(H) \to B(K)$ is a linear completely positive trace-preserving map. A quantum channel Φ is said to be unital if $\Phi(\frac{1}{d_H} I_H) = \frac{1}{d_K} I_K$.
Denote $QC(H, K) := \{quantum\ channels\ from\ B(H)\ to\ B(K)\}$.

The next proposition gives us a method to construct a new quantum channel from given isometry. This technique is crucial in constructing EPOSIC channel, to be introduced in chapter 5.

Proposition 3.4. *[1]*
Let H and K be Hilbert spaces. For any $\alpha \in B(H, K)$, the map Ad_α is a linear completely positive map.
And Ad_α is a channel if and only if α is an isometry.

Proof. Let $A \geq 0$ in $B(H)$. Then there exists $B \in B(H)$ such that $A = BB^*$. So,

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

Let $n \in \mathbb{N}$. Note that $B(H) \otimes \mathbb{M}_n(\mathbb{C}) \cong B(H \otimes \mathbb{C}^n)$. So $Ad_\alpha \otimes I_n = Ad_{\alpha \otimes I_{\mathbb{C}^n}}$. That is, Ad_α is completely positive.
If α is an isometry, then $tr(Ad_\alpha(A)) = tr(\alpha A \alpha^*) = tr(A)$. That is, Ad_α is trace preserving. □

A quantum channel has many equivalent representations. We give some of those in this chapter.

Definition 3.5 (Stinespring representation)**.**
Let H and K be Hilbet spaces and $\Phi : B(H) \to B(K)$ be a quantum channel. A Stinespring representation of Φ is a pair (E, α) consisting of a Hilbert space E (an environment space), and an isometry $\alpha : H \to K \otimes E$ such that $\Phi(A) = Tr_E(\alpha A \alpha^*)$ for any $A \in B(H)$.

Definition 3.6 (Kraus representation)**.**
Let H and K be Hilbet spaces and $\Phi : B(H) \to B(K)$ be a completely positive map. A Kraus representation of Φ is a set of operators $\{T_j : 1 \leq j \leq k\} \subset B(H, K)$ 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 of Φ is required to satisfy the additional condition

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

.

Theorem 3.7. *[6]*
Let H and K be Hilbert spaces and $\Phi : B(H) \to B(K)$ be a linear map. The followings are equivalent:

1. Φ *is a quantum channel.*
2. Φ *has a Stinespring representation* (E, α)
3. Φ *has a Kraus representation.*

Note that a Stinespring represenation exists for any completely positive map [12] p.43.
From now on, we assume the Hilbet spaces H and K are representation spaces of G. And we restrict our study to a class of quantum channels that are also G-equivariant maps with respect to a given group G, called G-covariant channels.

Definition 3.8 (G-covariant Channels). *[4]*
Let (H, π_H) *and* (K, π_K) *be two unitary representations of a topological group G. A quantum channel* $\Phi : B(H) \to B(K)$ *is G-covariant if* $\Phi(\pi_H(g)A\pi_H^*(g)) = \pi_K(g)\Phi(A)\pi_K^*(g)$ *for all* $A \in B(H)$ *and* $g \in G$.
If both π_H *and* π_K *are irreducible representations, then* Φ *is called G-irreducibly covariant.*

We denote $QC(H, K)^G := \{G{-}covariant\ quantum\ channels\ from\ B(H)\ to\ B(K)\}$.

Example 3.9.
Tr_H *is a G-covariant channel.*

Proof. Since we know that Tr_H is a G-equivariant map, it's enough to show that Tr_H is a quantum channel. Note that Tr_H is a quantum channel with a Stinespring representation $(H, I_{H\otimes K})$. □

The following proposition is straightforward.

Proposition 3.10.
Let G be a topological group. The tensor product of G-covariant channels, and the composition of G-covariant channels are again G-covariant channels.

Proposition 3.11.
Let H, K, and E be Hilbert spaces. Let $\Phi : B(H) \to B(K)$ *be a quantum channel whose Stinespring representation is* (E, α).
If $\alpha : H \to K \otimes E$ *is G-equivariant, then* Φ *is G-covariant.*

Proof. By Example 3.9, the partial trace over E Tr_E is G-equivariant. By Example 2.10, Ad_α is G-equivariant. By Proposition 2.8 and definition of Stinespring represenation, $\Phi = Tr_E \circ Ad_\alpha$ is a G-covariant channel. □

Chapter 4. Basics in quantum information theory

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 chapter, we give the definition of MOE, minimal output Rényi entropy, and exhibit some of its properties. For more details, we refer the reader to [4].

Definition 4.1 (Entropy)**.**
Let H and K be a Hilbert space, $\rho \in D(H)$, and $\Phi \in QC(H, K)$.
The von Neumann entropy of a density operator ρ is defined by

$$S(\rho) = -tr(\rho log_2 \rho)$$

The minimal output entropy(MOE) of a quantum channel Φ is defined by

$$S_{min}(\Phi) = min\{S(\Phi(\rho)) : \rho \in D(H)\}$$

where S is the von Neumann entropy.

Note that $S(\rho) = \sum_i -\lambda_i log_2 \lambda_i$ where $\{\lambda_i\}_i$ are the eigenvalues of ρ. By convention, $0 log_2 0 = 0$.

Theorem 4.2.
1. The von Neumann entropy is a concave nonnegative function, which is zero if and only if the state is pure.
2. In a d dimentional 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 $\frac{I_H}{d}$.

In the definition of minimal output entropy, the minimum is taken over all the states in H. However, by the concavity of von Neumann entropy, the minimal output entropy is achieved on a pure state.

$$i.e. \ \ S_{min}(\Phi) = min\{S(\Phi(\rho)) : \rho \in P(H)\}$$

Proposition 4.3. *[1]*
Let H and K be Hilbert spaces and $\Phi : B(H) \to B(K)$ be a quantum channel. Then $S_{min}(\Phi) = 0$ if and only if there exist $\rho \in P(H)$ such that $\Phi(\rho) \in P(K)$.

Proof. By continuity of the von Neumann entropy and compactness of the set of states[6, p.29], the minimum entropy is achieved. The other direction is trivial. □

We introduce another entopy of a quantum channel, called minimal output Rényi entropy, which is important in that we can guess MOE using it.

Definition 4.4 (Rényi entropy)**.**
Let $p > 1$*,* H *and* K *be a Hilbert space,* $\rho \in D(H)$*, and* $\Phi \in QC(H, K)$*.*
The quantum Rényi entropy of order p of a density operator ρ *is defined by*

$$R_p(\rho) = \frac{1}{1-p} log_2 tr \rho^p$$

The minimal output Rényi entropy of order p of a quantum channel Φ *is defined by*

$$\check{R}_p(\Phi) = min\{R_p(\Phi(\rho)) : \rho \in D(H)\}$$

Remark 4.5. *[4]*
Let $p > 1$*,* H *and* K *be a Hilbert space,* $\rho \in D(H)$*, and* $\Phi \in QC(H, K)$*.*
(i) As $p \searrow 1$*,* $R_p(\rho) \nearrow S(\rho)$ *for any* $\rho \in D(H)$
(ii) $\lim_{p \searrow 1} \check{R}_p(\Phi) = S_{min}(\Phi)$ *for any* $\Phi \in QC(H, K)$

There is another important measure of a channel performance. A channel's capacity is defined to be the maximal rate of at which information can be reliably transmitted through the channel. The capacity has a maximum when the channel is an identity.

Notation 1.
A state ensemble $\{p_i, \rho_i\}_{i \in I}$ *is a finite probability distribution on D(H) ascribing* p_i *to* ρ_i *where I is a finite index set such that* $\sum_{i \in I} p_i = 1$

Definition 4.6 (Holevo capacity)**.**
The Holevo capacity of a channel $\Phi : B(H) \to B(K)$ *is defined by*

$$C_\chi(\Phi) := max_{\{p_i, \rho_i\}} \left[S\left(\Phi(\sum_i p_i \rho_i) \right) - \sum_i p_i S(\Phi(\rho_i)) \right]$$

where $\{p_i, \rho_i\}$*:a state ensemble*

The Holevo capacity is sometimes called the χ-capacity or the product state capacity. In a d dimentional Hilbert space H, the maximum of the Holevo capacity is $log_2 d$, which is occured when the channel is an identity on B(H). The Holevo capacity can be computed in another way other than definition for a number of interesting channels. We present one of those ways we will use in the thesis.

Theorem 4.7. *[4]*
Let (H, π_H) *and* (K, π_K) *be two irreducible representations of a topological group G. Suppose* $\Phi : B(H) \to B(K)$ *is a G-irreducibly covariant quantum channel. Then* $C_\chi(\Phi) = S\left(\Phi\left(\frac{I_H}{d_H}\right)\right) - S_{min}(\Phi)$*.*

Chapter 5. SU(2)-irreducible representations and covariant channels

By Proposition 3.4 and Example 2.10, if we have a G-equivariant isometry α, we can construct the G-covariant channel Ad_α. For the compact group SU(2), such a G-equivariant isometry is already studied and known with its specific formulas, by Clebsch and Gordan. According to the Clebsch-Gordan Decomposition [10] 87p, if H and K are two SU(2)-irreducible subspaces, then the SU(2)-space $K \otimes E$ is isomorphic to $\oplus_i H_i$ where H_i is SU(2)-irreducible subspace with multiplicity one. For each i, the inclusion map $\alpha_i : H_i \to K \otimes E$ is an SU(2)-equivariant isometry. In this chapter, we find an explicit formulas for the map α_i and construct the SU(2)-irreducibly covariant channel using α_i, called an EPOSIC channel. For more details, we refer the reader to [1], [13] and [14].

For $m \in \mathbb{N}$, let P_m be the space of homogeneous polynomials of degree m in the two variables $x_1,\ x_2$. Then P_m is a complex vector space of dimension m+1 with a basis $\{x_1^i x_2^{m-i}\}$. Define an inner product on P_m by $< x_1^l x_2^{m-l}, x_1^k x_2^{m-k} >= l!(m-l)!\delta_{lk}$. Then P_m is a Hilbert space. We choose the orthonormal basis for P_m given by the polynomials $\{f_l^m = a_m^l x_1^l x_2^{m-l} : 0 \le l \le m\}$ where $a_l^m = \frac{1}{\sqrt{l!(m-l)!}}$. This basis is called canonical [14] p.280.

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

Remark 5.1. *[14]*
For $m \in \mathbb{N}$, define $\pi_m : SU(2) \to B(P_m)$ by $(\pi_m(g)f)(x_1, x_2) = f((x_1, x_2)g) = f(ax_1 - \overline{b}x_2, bx_1 + \overline{a}x_2)$ for $f \in P_m$ and $g \in SU(2)$.
Note that the set $\{\pi_m : m \in \mathbb{N}\}$ constitutes the full list of the irreducible representations of SU(2)

In representation theory,

$$\pi_m \otimes \pi_n \cong \oplus_{h=0}^{min\{m,n\}} \pi_{m+n-2h}$$

is a classical result. Consequently, we obtain

$$P_m \otimes P_n \cong \oplus_{h=0}^{min\{m,n\}} P_{m+n-2h}$$

One remarkable fact is that the inclusion map from P_{m+n-2h} into $P_m \otimes P_n$ is an SU(2)-equivariant isometry for $0 \le h \le min\{m, n\}$. This is due to Clebsch and Gordan.

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 $P_m(x) \times P_n(y) \to \mathbb{C}[x, y]$ by $(f(x), g(y)) \mapsto f(x)g(y)$. Then it is a bilinear map. So we can extends to a linear map $T : P_m(x) \otimes P_n(y) \to \mathbb{C}[x, y]$ 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). The space $P_{m,n}$ has a basis consisting of

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

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

Definition 5.2.
For $m, n \in \mathbb{N}$, define the following maps on $P_m \otimes P_n$

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

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

Remark 5.3.
The operators $\Delta_{xy},\ \Delta_{yx},\ \Gamma_{xy},$ and Ω_{xy} are SU(2)-equivariant, and satisfies

$$\Delta_{xy}^* = \Delta_{yx}, \qquad \Gamma_{xy}^* = \Omega_{xy}$$

Theorem 5.4 (Clebsch-Gordan expansion)**.**
Let $m, n \in \mathbb{N}$ and $f(x, y) \in P_m \otimes P_n$.
Then

$$f(x, y) = \sum_{h=0}^{min\{m,n\}} c_{m,n,h} \Gamma_{xy}^h \Delta_{yx}^{n-h} \Delta_{xy}^{n-h} \Omega_{xy}^h (f(x, y))$$

where the coefficients $c_{m,n,h}$ *are determined by induction as follows:*
$c_{m,0,0} = 1$ *for* $m \in \mathbb{N}$. *And for* $n \geq 1$ *and* $0 \leq h \leq min\{m,n\}$,

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

Definition 5.5.
For $m, n, h \in \mathbb{N}$ *with* $0 \leq h \leq min\{m,n\}$, *let*

$$\begin{aligned} \alpha_{m,n,h} : P_{m+n-2h} &\to P_m \otimes P_n \\ f(x_1, x_2) &\mapsto \sqrt{c_{m,n,h}} \Gamma^h_{xy} \Delta^{n-h}_{yx}(f(x_1, x_2)) \end{aligned}$$

where $f(x_1, x_2) \in P_{m+n-2h}$.

$\alpha_{m,n,h}$ is the inclusion map from P_{m+n-2h} into $P_m \otimes P_n$ as mentioned above. By Remark5.3, the conjugate map of $\alpha_{m,n,h}$ is given by

$$\begin{aligned} \alpha^*_{m,n,h} : P_m \otimes P_n &\to P_{m+n-2h} \\ g(x_1, x_2, x_3, x_4) &\mapsto \sqrt{c_{m,n,h}} \Delta^{n-h}_{xy} \Omega^h_{xy}(g(x_1, x_2, x_3, x_4)) \end{aligned}$$

and $\alpha^*_{m,n,h}$ is also a SU(2)-equivariant map.
Note that $\alpha_{m,n,h}\alpha^*_{m,n,h}(g) = c_{m,n,h}\Gamma^h_{xy}\Delta^{n-h}_{yx}\Delta^{n-h}_{xy}\Omega^h_{xy}(g)$. By Clebsch-Gordan expansion, we obtain

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

Proposition 5.6.
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 isometry.*

Proof. Since Γ_{xy} and Δ_{yx} are SU(2)-equivariant, $\alpha_{m,n,h}$ is SU(2)-equivariant.
Let $0 \leq h, s \leq min\{m,n\}$. Then $\alpha^*_{m,n,h}\alpha_{m,n,s} : P_{m+n-2s} \to P_{m+n-2h}$ is an SU(2)-equivariant map and P_{m+n-2s}, P_{m+n-2h} are irreducible spaces. By Schur's lemma, we have

$$\alpha^*_{m,n,h}\alpha_{m,n,s} = \begin{cases} 0, & h \neq s \\ cI_{P_{m+n-2h}}, & h = s \end{cases}$$

for some $c \in \mathbb{C}$. Then we have

$$\alpha^*_{m,n,h} = \alpha^*_{m,n,h} I_{P_m \otimes P_n} = \alpha^*_{m,n,h} \sum_{s=0}^{min\{m,n\}} \alpha_{m,n,s}\alpha^*_{m,n,s} = cI_{P_{m+n-2h}}\alpha^*_{m,n,h} = c\alpha^*_{m,n,h}$$

Since $\alpha_{m,n,h}(x_1^{m+n-2h}) \neq 0$, $\alpha_{m,n,h} \neq 0$ *whence* $\alpha^*_{m,n,h} \neq 0$. Thus, c=1.
Since $\alpha^*_{m,n,h}\alpha_{m,n,h} = I_{P_{m+n-2h}}$, $\alpha_{m,n,h}$ is an isometry. □

As mentioned in first of this chapter, since $\alpha_{m,n,h}$ is an SU(2)-equivariant isometry, by Proposition 3.4 and Example 2.10, we have the G-irreducibly covariant channel $Ad_{\alpha_{m,n,h}}$. And we know that Tr_{P_n} is a SU(2)-irreducibly covariant channel. By Proposition 3.11, we can construct:

Proposition 5.7. *[1]*
For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq min\{m, n\}$. Define $\Phi_{m,n,h} : B(P_r) \to B(P_m)$ by $\Phi_{m,n,h}(A) = Tr_{P_n}(\alpha_{m,n,h} A \alpha^*_{m,n,h})$ for $A \in B(P_r)$.
Then $\Phi_{m,n,h}$ is an SU(2)-irreducibly covariant channel.

Proof. Note that $\Phi_{m,n,h} = Tr_{P_n} \circ Ad_{\alpha_{m,n,h}}$. □

We call the quantum channel $\Phi_{m,n,h}$ an EPOSIC channel. Denote by

$$EC(r, m) := \{all\ EPOSIC\ channels\ from\ B(P_r)\ into\ B(P_m)\}$$

and abbreviate EC(m,m) to EC(m).

Remark 5.8.
Let $r, m \in \mathbb{N}$. Then $EC(r, m) = \{\Phi_{m,r+m-2l,m-l} : 0 \leq l \leq min\{r, m\}\} = \{\Phi_{m,r-m+2h,h} : 0 \leq h \leq min\{m, r-m+2h\},\ r-m+2h \geq 0\}$.
Note that $(P_n, \alpha_{m,n,h})$ is a Stinespring representation of $\Phi_{m,n,h}$.
For $0 \leq j \leq n$, define $T_j : P_r \to P_m$ by $T_j = (I_{P_m} \otimes f_j^{n*})\alpha_{m,n,h}$. Then the set $\{T_j : 0 \leq j \leq n\}$ is a Kraus representation of $\Phi_{m,n,h}$. We call these Kraus opereators, the EPOSIC Kraus operators.

Now we introduce new notation:

Notation 2.
For $m, n, h \in \mathbb{N}$ with $0 \leq h \leq min\{m, n\}$, denote $r = m + n - 2h$, $0 \leq i \leq r$, $0 \leq j \leq n$, $0 \leq l \leq m$.
Define $B(i) := \{j : max\{0, -m+i+h\} \leq j \leq min\{i+h, n\}\}$ and $l_{ij} := i - j + h$.

The proof of Lemma 5.9 below is a direct computation. For the proof, we refer the reader to [1] Appendix B.

Lemma 5.9.
Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq min\{m, n\}$. Then

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

where

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

Corollary 5.10. *[1]*
Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq min\{m, n\}$. Then

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

$$where\ \varepsilon_i^j(m,n,h) = \sum_{s=max\{0,j-i,j+h-n\}}^{min\{h,j,j+m-i-h\}} \beta_{i,s,j}^{m,n,h}$$

Corollary 5.11.
Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq min\{m, n\}$ and $\{T_j : 0 \leq j \leq n\}$ are the EPOSIC Kraus operators of $\Phi_{m,n,h}$. Then for each $0 \leq j \leq n$

$$T_j(f_i^r) = \begin{cases} \varepsilon_i^j f_{l_{ij}}^m, & if\ j \in B(i) \qquad\qquad where\ \varepsilon_i^j\ is\ given\ in\ Corollary\ 5.10 \\ 0, & otherwise \qquad\qquad\qquad B(i)\ is\ given\ in\ Notation 2 \end{cases}$$

Proof.

$$T_j(f_i^r) = (I_{P_m} \otimes f_j^{n*})\alpha_{m,n,h}(f_i^r) = I_{P_m} \otimes f_j^{n*} \left(\sum_{j \in B(i)} \varepsilon_i^j(m,n,h) f_{l_{ij}}^m \otimes f_j^n \right)$$

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

by Corollary 5.10. □

Corollary 5.12.
Let $m, n, h \in \mathbb{N}$ with $0 \leq h \leq min\{m, n\}$. For $0 \leq i_1, i_2 \leq r$,

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

Proof. Let $\{T_j : 0 \leq j \leq n\}$ be the EPOSIC Kraus operators of $\Phi_{m,n,h}$. Then

$$\Phi_{m,n,h}(f_{i_1}^r f_{i_2}^{r\,*}) = \sum_{j=1}^{n} T_j f_{i_1}^r f_{i_2}^{r\,*} T_J^* = \sum_{j=1}^{n} (T_j f_{i_1}^r)(T_j f_{i_2}^r)^*$$

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

by Corollary 5.11. □

Here, we study SU(2)-irreducibly covariant channels. The rest of this chapter depends heavily on [1] Chapter 5. We will see that EC(r,m) consists of all the extreme points of $QC(P_r, P_m)^{SU(2)}$. This is why the name of the channels is EPOSIC(the Extreme Points Of SU(2)-Irreducibly Covariant channels).

Proposition 5.13. *[1]*
Let $r, m \in \mathbb{N}$. The set $QC(P_r, P_m)^{SU(2)}$ is the convex hull of EC(r,m).
Moreover, any element in $QC(P_r, P_m)^{SU(2)}$ is uniquely written as a convex combination of elements of $EC(r, m)$.

Proposition 5.14.
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. By Proposition 5.13, every element in EC(r,m) can not be written as a proper convex combination of elements of $QC(P_r, P_m)^{SU(2)}$ other than itself. That is, EC(r,m) are extreme points of $QC(P_r, P_m)^{SU(2)}$. Conversely, let Φ be an extreme point of $QC(P_r, P_m)^{SU(2)}$. Then it cannot be written as as convex combination of elements of $QC(P_r, P_m)^{SU(2)}$ other than itself. But $QC(P_r, P_m)^{SU(2)}$ is the convex hull of EC(r,m) by Proposition 5.13. Hence, Φ must be in EC(r,m). □

Chapter 6. Properties of SU(2)-irreducibly covariant channels

In this chapter, we compute the entropy and the Holevo capacity of EPOSIC channels. And using the relation between EPOSIC channels and SU(2)-irreducibly covariant channels, we determine the entropy and the capacity of SU(2)-irreducibly covariant channels. In addition to the result of [1], we give computation of the Rényi entropy and the Holevo capacity for some cases in this thesis. To compute the Holevo capacity of SU(2)-irreducibly covariant channels, we usually use Theorem 4.7. So, it is important to know the minimal output entropy of the channels. The next proposition enable us to determine when the minimal output entropy of an EPOSIC channel is zero.

Proposition 6.1. *[1]*
For $m, n, h \in \mathbb{N}$, the channel $S_{min}(\Phi_{m,n,h}) = 0$ if and only if $h = 0$.

The following proposition and corollary is newly presented in this thesis.

Proposition 6.2.

Let $M := min_{\Phi \in EC(r,m)} S_{min}(\Phi)$ and $\Phi \in QC(P_r, P_m)^{SU(2)}$. Then
i) $M \leq S_{min}(\Phi)$
ii) $0 \leq C_\chi(\Phi) \leq log_2(m+1) - M$

Proof. *i)* By continuity of von Neumann entropy and compactness of the set of states, the minimam output entropy is achievable. That is, there exists $\rho = ww^* \in P(P_r)$ such that $S(\Phi(\rho)) = S_{min}(\Phi)$. Since $co(EC(r,m)) = QC(P_r, P_m)^{SU(2)}$, if $|EC(r,m)| = t$, then $\Phi = \sum_{i=1}^t c_i \psi_i$ where $c_i \geq 0$, $\sum_{i=1}^t c_i = 1$, $\{\psi_1, \cdots, \psi_t\} = EC(r,m)$. So

$$S_{min}(\Phi) = S(\Phi(\rho)) = S\left(\sum_{i=1}^t c_i \psi_i(\rho)\right) \geq \sum_{i=1}^t c_i S\left(\psi_i(\rho)\right) \geq \sum_{i=1}^t c_i S_{min}(\psi_i) \geq \sum_{i=1}^t c_i M$$
$$= M$$

$$ii)\ 0 \leq C_\chi(\Phi) = S\left(\Phi\left(\frac{I_{P_r}}{r+1}\right)\right) - S_{min}(\Phi) \leq log_2(m+1) - S_{min}(\Phi) \leq log_2(m+1) - M$$

by Theorem 4.7 □

Corollary 6.3.
For $m \in \mathbb{N}$ and $0 \leq r \leq m-1$, $C_\chi(\Phi) < log_2(m+1)$ for any $\Phi \in QC(P_r, P_m)^{SU(2)}$

Proof. Note that EC(r,m)= $\{\Phi_{m,r-m+2h,h} : 0 \le h \le min\{m, r-m+2h\},\ r-m+2h \ge 0\}$. To be $r-m+2h \ge 0$ *with* $0 \le r \le m-1$, h must be equal or greater than 1. Since $S_{min}(\Phi_{m,n,h}) = 0$ if and only if $h = 0$, $S_{min}(\psi) > 0$ for any $\psi \in EC(r,m)$. Hence

$$M := min_{\psi \in EC(r,m)} S_{min}(\psi) > 0$$

By Proposition 6.2, $C_\chi(\Phi) \le log_2(m+1) - M < log_2(m+1)$. □

Now we compute measurement of SU(2)-irreducibly covariant channels such as the minimal output entropy. Since $EC(r,m) = \{\Phi_{m,r-m+2h,h} : 0 \le h \le min\{m, r-m+2h\},\ r-m+2h \ge 0\}$ is a finite set whose cardinality depends on the numbers r and m, it is possible to be easy for computing the measurement of the channels if $|EC(r,m)| \le 2$.

In this thesis, we compute $S_{min}(\Phi)$ *and* $\check{R}_p(\Phi)$ for any $\Phi \in QC(P_1, P_m)^{SU(2)},\ m \in \mathbb{N}$. $S_{min}(\Phi)$ have been computed by [1], but $\check{R}_p(\Phi)$ is newly computed. In that case, $EC(1,m) = \{\Phi_{m,m+1,m}, \Phi_{m,m-1,m-1}\}$ and the standard basis for P_1 is given by $f_0^1(x_1,x_2) = x_2$ and $f_1^1(x_1,x_2) = x_1$.

Lemma 6.4. *[1]*
Let $m \in \mathbb{N}$ *and* $w \in P_1$ *with* $\|w\| = 1$. *Then*
i) There exists $g \in SU(2)$ *such that* $\pi_1(g)(f_0^1) = w$.
ii) If $\Phi : B(P_1) \to B(P_m)$ *is an SU(2)-equivariant map, then the matrices* $\Phi(ww^*)$ *and* $\Phi(f_0^1 {f_0^1}^*)$ *are similar.*

Proof. i) Since $P_1 =< f_0^1, f_1^1 >$, $w = w_0 f_0^1 + w_1 f_1^1$ for some $w_0, w_1 \in \mathbb{C}$ with $|w_0|^2 + |w_1|^2 = 1$. Choose $g = \begin{pmatrix} \overline{w_0} & w_1 \\ -\overline{w_1} & w_0 \end{pmatrix} \in SU(2)$

$$\begin{aligned} \textit{Then } (\pi_1(g) f_0^1)(x_1,x_2) &= f_0^1(\overline{w_0}x_1 - \overline{w_1}x_2, w_1x_1 + w_0x_2) = w_1x_1 + w_0x_2 \\ &= w_0 f_0^1(x_1,x_2) + w_1 f_1^1(x_1,x_2) = w(x_1,x_2) \end{aligned}$$

ii) Since Φ is SU(2)-equivariant and by i),

$$\Phi(ww^*) = \Phi(\pi_1(g) f_0^1 {f_0^1}^* \pi_1^*(g)) = \pi_m(g) \Phi(f_0^1 {f_0^1}^*) \pi_m^*(g)$$

□

Lemma 6.5. *[1]*

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

Proof. Direct from Corollary 5.12 and the formula of ε_i^j. □

Theorem 6.6.
Let $m \in \mathbb{N}$ and $\Phi \in QC(P_1, P_m)^{SU(2)}$. Then there exists $p \in [0,1]$ such that the eigenvalues of $\Phi(f_0^1 {f_0^1}^*)$ are

$$\{\lambda_j = \frac{2(m-j+1)}{(m+1)(m+2)}p + \frac{2j}{m(m+1)}(1-p)\}$$

In that cases, $S_{min}(\Phi) = -\sum_{j=0}^{m} \lambda_j log_2 \lambda_j$ and $\check{R}_p(\Phi) = \frac{1}{1-p} log_2 \left(\sum_{j=0}^{m} {\lambda_j}^p\right)$

Proof. Since $\Phi \in QC(P_1, P_m)^{SU(2)} = co\,(EC(1,m)) = co\,(\{\Phi_{m,m+1,m}, \Phi_{m,m-1,m-1}\})$, there exists $p \in [0,1]$ such that $\Phi = p\Phi_{m,m+1,m} + (1-p)\Phi_{m,m-1,m-1}$. So

$$\Phi(f_0^1 {f_0^1}^*) = p\Phi_{m,m+1,m}(f_0^1 {f_0^1}^*) + (1-p)\Phi_{m,m-1,m-1}(f_0^1 {f_0^1}^*)$$
$$= \frac{2p}{m+2} f_m^m f_m^m + + \sum_{j=1}^{m} \left(p\frac{2(m-j+1)}{(m+1)(m+2)} + (1-p)\frac{2j}{m(m+1)}\right) f_{m-j}^m {f_{m-j}^m}^*$$
$$= \sum_{j=0}^{m} \left(p\frac{2(m-j+1)}{(m+1)(m+2)} + (1-p)\frac{2j}{m(m+1)}\right) f_{m-j}^m {f_{m-j}^m}^* = \sum_{j=0}^{m} \lambda_j f_{m-j}^m {f_{m-j}^m}^*$$

Hence, $S_{min}(\Phi) = S(\Phi(ww^*)) = S(\phi(f_0^1 {f_0^1}^*)) = -\sum_{j=0}^{m} \lambda_j log_2 \lambda_j$

$$\check{R}_p(\Phi) = R_p(\Phi(ww^*)) = R_p(\phi(f_0^1 {f_0^1}^*)) = \frac{1}{1-p} log_2 \left(\sum_{j=0}^{m} {\lambda_j}^p\right)$$

□

Note that $C_\chi(\Phi) = S\left(\Phi\left(\frac{I_H}{d_H}\right)\right) - S_{min}(\Phi)$. To compute the Holevo capacity of EPOSIC channels, we need to compute its minimal output entropy and von Neumann entropy of $\Phi_{m,n,h}\left(\frac{I_{P_r}}{r+1}\right)$.

Remark 6.7.
We can compute $\Phi_{m,n,h}\left(\frac{I_{P_r}}{r+1}\right)$ for any $m, n, h \in \mathbb{N}$ with $0 \le h \le m+n-2h$.

Proof.

$$S\left(\Phi_{m,n,h}\left(\frac{I_{P_r}}{r+1}\right)\right) = S\left(\Phi_{m,n,h}\left(\sum_{i=0}^{r} \frac{1}{r+1} f_i^r {f_i^r}^*\right)\right) = S\left(\sum_{i=0}^{r} \sum_{j \in B(i)} \frac{{\varepsilon_j^i}^2}{r+1} f_{l_{ij}}^m {f_{l_{ij}}^m}^*\right)$$
$$=^{calculation} S\left(\sum_{l=0}^{m} a_l f_l^m {f_l^m}^*\right) = -\sum_{l=0}^{m} a_l log_2 a_l$$

□

So, it is relatively easy to compute the capacity of EPOSIC channels. Now we compute $S_{min}(\Phi_{m,1,1}),\ C_\chi(\Phi_{m,1,1}),\ and\ \check{R}_p(\Phi_{m,1,1})$ for any $m \ge 1$. $S_{min}(\Phi_{m,1,1})$ have been computed by [1], but $C_\chi(\Phi_{m,1,1}),\ and\ \check{R}_p(\Phi_{m,1,1})$ are newly computed.

Lemma 6.8. *[1]*
Let K be a finite dimensional Hilbert space, and $A \in B(K)$ such that $A = \sum_{j=1}^{n} u_j {u_j}^*$. If $\{u_j : 0 \le j \le n\}$ are linearly independent vectors in K, then there exist a basis for K such that the matrix represents A is in the form

$$\begin{pmatrix} < u_1|u_1 > & < u_1|u_2 > & \cdots & < u_1|u_n > & 0 & \cdots & 0 \\ < u_2|u_1 > & < u_2|u_2 > & \cdots & < u_2|u_n > & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ < u_n|u_1 > & < u_n|u_2 > & \cdots & < u_n|u_n > & 0 & \cdots & 0 \\ 0 & 0 & & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & & 0 & 0 & \cdots & 0 \end{pmatrix}$$

A matrix in a such form is called Gram matrix.

Proof. Let $\{u_{n+1}, u_{n+2}, \cdots, u_{d_k}\}$ be a basis for the orthogonal complement of $< u_j : 1 \le j \le n >$ in K. Set $U = \{u_1, u_2, \cdots, u_n, u_{n+1}, u_{n+2}, \cdots, u_{d_k}\}$. Then U forms a basis for K. For each $u_k \in U$, we have

$$Au_k = \sum_{j=1}^{n} u_j {u_j}^*(u_k) = \begin{cases} \sum_{j=1}^{n} < u_j|u_k > u_j, & 1 \le k \le n \\ 0, & k > n \end{cases}$$

The result follows by writing the matrix for A with repect to the basis U. □

Corollary 6.9. *[1]*
Let $m, n \in \mathbb{N}$ with $n \le m$, and $\rho \in P(P_{m-n})$. Then the matrix representing $\Phi_{m,n,n}(\rho)$ is in the form of a Gram matrix.

Proof. Let $\{T_j : 0 \le j \le n\}$ be the EPOSIC Kraus operators of $\Phi_{m,n,n}$, and $\rho = ww^*$ where w is a unit vector in $P_r = P_{m-n}$. Then

$$\Phi_{m,n,n}(ww^*) = \sum_{j=0}^{n} u_j {u_j}^* \textit{ where } u_j = T_j w = \sum_{i=0}^{m-n} w_i \varepsilon_i^j f_{i-j+n}^m = \sum_{k=n-j}^{m-j} w_{k+j-n} \varepsilon_{k+j-n}^j f_k^m$$

Since $\varepsilon_i^j(m, n, n)$ are nonzero, the set $\{u_j : 0 \le j \le n\}$ is linearly independent. By Lemma 6.8, the result follows. □

Note that for $m \in \mathbb{N}$, the EPOSIC channel $\Phi_{m,1,1} : B(P_{m-1}) \to B(P_m)$ has two Kraus operator $\{T_0, T_1\}$. Let $w = \sum_{i=0}^{m-1} w_i f_i^{m-1} \in P_{m-1}$ and $\rho = ww^*$. Then $u_0 = T_0 w = \sum_{i=1}^{m} \varepsilon_{i-1}^0 w_{i-1} f_i^m$ and $u_1 = T_1 w = \sum_{i=0}^{m-1} \varepsilon_i^1 w_i f_i^m$ by Corollary 5.11. By Corollary 6.9, there exists a basis for P_m such that the matrix $\Phi_{m,1,1}$ is represented by

$$A := \begin{pmatrix} <u_0|u_1> & <u_0|u_1> & 0 & \cdots & 0 \\ <u_1|u_0> & <u_1|u_1> & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

The characteristic polynomial of A is given by

$$p(\lambda) = det(\lambda I - A) = \lambda^2 - (\|u_0\|^2 + \|u_1\|^2)\lambda + \|u_0\|^2\|u_1\|^2 - |<u_0|u_1>|^2$$

Set R:=$\|u_0\|^2\|u_1\|^2 - |<u_0|u_1>|^2$.

Lemma 6.10.
For $m \in \mathbb{N}$ and $\varepsilon_i^j := \varepsilon_i^j(m,1,1)$, we have

$$\varepsilon_i^0 = \sqrt{\frac{i+1}{m+1}},\ \varepsilon_i^1 = -\sqrt{\frac{m-i}{m+1}}\ for\ 0 \leq i \leq m-1$$

By Lemma 6.10, we obtain

$$\begin{aligned} \|u_0\|^2 + \|u_1\|^2 &= \sum_{i=0}^{m-1}(\varepsilon_i^0)^2 w_i^2 + \sum_{i=0}^{m-1}(\varepsilon_i^1)^2 w_i^2 = \sum_{i=0}^{m-1}(\varepsilon_i^0)^2 + (\varepsilon_i^1)^2 w_i^2 \\ &= \sum_{i=0}^{m-1}\frac{i+1}{m+1} + \frac{m-i}{m+1}w_i^2 = \sum_{i=0}^{m-1} w_i^2 = 1 \end{aligned}$$

Hence $p(\lambda) = \lambda^2 - \lambda + R$. So $p(\lambda) = 0$ implies $\lambda = \frac{1 \pm \sqrt{1-4R}}{2}$.
Since $\Phi_{m,1,1}$ is completely positive and ww^* is positive, the eigenvalues are nonnegative real numbers. So $0 \leq 1 - 4R \leq 1$.

Lemma 6.11.
For $m \in \mathbb{N}$, the minimum value of R=$\|u_0\|^2\|u_1\|^2 - |<u_0|u_1>|^2$ is $\frac{m}{(m+1)^2}$.

Proof.

$$Note\ that\ <u_0,u_1>= \sum_{i=1}^{m-1}\varepsilon_{i-1}^0\overline{w_{i-1}}\varepsilon_i^1 w_i = \sum_{i=1}^{m-1}\varepsilon_{i-1}^0 w_i \varepsilon_i^1\overline{w_{i-1}} =<v_0,v_1>$$

$$where\ v_0 = \sum_{i=1}^{m-1}\varepsilon_{i-1}^0 w_i f_i^m, v_1 = \sum_{i=1}^{m-1}\varepsilon_i^1\overline{w_{i-1}}f_i^m$$

$$Then\ \|v_0\|^2 = \sum_{i=1}^{m-1}(\varepsilon_{i-1}^0)^2|w_i|^2 = \sum_{i=1}^{m-1}(\varepsilon_{i-1}^0)^2|w_i|^2 + \frac{\|w\|^2}{m+1} - \frac{\|w\|^2}{m+1}$$

$$= \frac{1}{m+1}|w_0|^2 + \sum_{i=1}^{m-1}\left((\varepsilon_{i-1}^0)^2 + \frac{1}{m+1}\right)|w_i|^2 - \frac{\|w\|^2}{m+1}$$

Since $\varepsilon_i^0 = \sqrt{\frac{i+1}{m+1}}$, $\varepsilon_0^0 = \frac{1}{m+1}$ and $(\varepsilon_{i-1}^0)^2 + \frac{1}{m+1} = (\varepsilon_i^0)^2$. Hence

$$\|v_0\|^2 = (\varepsilon_0^0)^2|w_0|^2 + \sum_{i=1}^{m-1}(\varepsilon_i^0)^2|w_i|^2 - \frac{1}{m+1} = \sum_{i=0}^{m-1}(\varepsilon_i^0)^2|w_i|^2 - \frac{1}{m+1}$$
$$= \sum_{i=1}^{m}(\varepsilon_{i-1}^0)^2|w_{i-1}|^2 - \frac{1}{m+1} = \|u_0\|^2 - \frac{1}{m+1}$$

By same argument, $\|v_1\|^2 = \|u_1\|^2 - \frac{1}{m+1}$. So

$$| < u_0|u_1 > |^2 = | < v_0|v_1 > |^2 \leq \|v_0\|^2\|v_1\|^2 = (\|u_0\|^2 - \frac{1}{m+1})(\|u_1\|^2 - \frac{1}{m+1})$$
$$= \|u_0\|^2\|u_1\|^2 - \frac{1}{m+1}(\|u_0\|^2 + \|u_1\|^2) + \frac{1}{(m+1)^2} = \|u_0\|^2\|u_1\|^2 - \frac{m}{(m+1)^2}$$

Thus $R = \|u_0\|^2\|u_1\|^2 - | < u_0|u_1 > |^2 \geq \frac{m}{(m+1)^2}$
Since $R_{f_0^{m-1}} = \frac{m}{(m+1)^2}$, we conclude $\frac{m}{(m+1)^2}$ is the minimum value of R. □

By concavity of von Neumann entropy, $S(\Phi_{m,1,1}(ww^*))$ achieves its minimum when the difference between the two eigenvalues of $\Phi_{m,1,1}(ww^*)$ is maximum. This happens when R takes its minimum value. Hence, we obtain

Theorem 6.12. *[1]*

$$S_{min}(\Phi_{m,1,1}) = S(\Phi_{m,1,1}(f_0^{m-1}f_0^{m-1^*})) = -(\frac{1}{m+1}log_2\frac{1}{m+1} + \frac{m}{m+1}log_2\frac{m}{m+1})$$

Proof.

$$\lambda = \frac{1}{2}\left(1 \pm \sqrt{1 - 4R_{f_0^{m-1}}}\right) = \frac{1}{2}\left(1 \pm \sqrt{1 - 4\frac{m}{(m+1)^2}}\right) = \frac{1}{2}\left(1 \pm \frac{m-1}{m+1}\right)$$
$$= \frac{m}{m+1} \; or \; \frac{1}{m+1}$$

□

The following two theorems are newly computed in this thesis.

Theorem 6.13.
Let $p > 1$ and $m \in \mathbb{N}$. Then

$$\check{R}_p(\Phi_{m,1,1}) = R_p(\Phi_{m,1,1}(f_0^{m-1}f_0^{m-1^*}))$$
$$= \frac{1}{1-p}log_2\left(\left(\frac{1}{2} + \frac{1}{2}\sqrt{1 - \frac{4m}{(m+1)^2}}\right)^p + \left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - \frac{4m}{(m+1)^2}}\right)^p\right)$$

Proof. By above argument, there exist a basis in P_m such that

$$\Phi_{m,1,1}(ww^*)^p = \begin{pmatrix} \lambda_0^p & 0 & 0 & \cdots & 0 \\ 0 & \lambda_1^p & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

where $\lambda_0 = \frac{1+\sqrt{1-4R}}{2}$ and $\lambda_1 = \frac{1-\sqrt{1-4R}}{2}$

So, $R_p(\Phi_{m,1,1}(ww^*)) = \frac{1}{1-p}log_2(\lambda_0^p + \lambda_1^p)$.

Set $b := \frac{1}{2}\sqrt{1-4R}$. Then $0 \le b \le \frac{1}{2}$ since $0 \le 1-4R \le 1$. Define $g(b) := \lambda_0^p + \lambda_1^p$.

Since $p > 1 \Rightarrow \frac{1}{1-p} < 0$ and $log_2(x)$ is increasing on $(0, \infty)$, $R_p(\Phi_{m,1,1}(ww^*))$ has minimum when g(b) has maximum. Note that

$$g'(b) = p\lambda_0^{p-1}\frac{d\lambda_0}{db} + p\lambda_1^{p-1}\frac{d\lambda_1}{db} = p\left(\frac{1}{2}+b\right)^{p-1} - p\left(\frac{1}{2}-b\right)^{p-1} \ge 0 \; for \; 0 \le b \le \frac{1}{2}$$

Hence g is increasing function on $[0, \frac{1}{2}]$. Since b has maximum when R has minimum, g(b) has maximum when $R = \frac{m}{(m+1)^2}$ and $w = f_0^{m-1}$. Thus,

$$\begin{aligned} &\check{R}_p(\Phi_{m,1,1}) = R_p(\Phi_{m,1,1}(f_0^{m-1}f_0^{m-1*})) \\ &= \frac{1}{1-p}log_2\left(\left(\frac{1}{2}+\frac{1}{2}\sqrt{1-\frac{4m}{(m+1)^2}}\right)^p + \left(\frac{1}{2}-\frac{1}{2}\sqrt{1-\frac{4m}{(m+1)^2}}\right)^p\right) \end{aligned}$$

□

Theorem 6.14.

$$C_\chi(\Phi_{m,1,1}) = \frac{m}{m+1}\left(log_2\frac{m}{m+1} - log_2\frac{1}{m+1}\right)$$

Proof. Note that $B(i) = \{j : 0 \le j \le 1\}$ for any $0 \le i \le m-1 = r$. Then

$$S\left(\Phi_{m,1,1}\left(\frac{I_{P_{m-1}}}{m}\right)\right) = S\left(\sum_{i=1}^{m-1}\frac{1}{m}\left((\varepsilon_i^0)^2 f_{i+1}^m f_{i+1}^{m\;*} + (\varepsilon_i^1)^2 f_i^m f_i^{m*}\right)\right) \; by \; Corollary \; 5.12$$

$$= S\left(\frac{1}{m}(\varepsilon_0^1)^2 f_0^m f_0^{m*} + \sum_{i=1}^{m-1}\frac{1}{m}\left((\varepsilon_{i-1}^0)^2 + (\varepsilon_i^1)^2\right) f_i^m f_i^{m*} + \frac{1}{m}(\varepsilon_{m-1}^0)^2 f_m^m f_m^{m*}\right)$$

$$= S\left(\frac{1}{m}\frac{m}{m+1}f_0^m f_0^{m*} + \sum_{i=1}^{m-1}\frac{1}{m}\left((\varepsilon_i^0)^2 - \frac{1}{m+1} + (\varepsilon_i^1)^2\right) f_i^m f_i^{m*} + \frac{1}{m}\frac{m}{m+1}f_m^m f_m^{m*}\right)$$

$$= S\left(\frac{1}{m+1}f_0^m f_0^{m*} + \sum_{i=1}^{m-1}\frac{1}{m}\left(1 - \frac{1}{m+1}\right) f_i^m f_i^{m*} + \frac{1}{m+1}f_m^m f_m^{m*}\right)$$

$$= S\left(\frac{1}{m+1}f_0^m f_0^{m*} + \sum_{i=1}^{m-1}\frac{1}{m+1}f_i^m f_i^{m*} + \frac{1}{m+1}f_m^m f_m^{m*}\right) = S\left(\sum_{i=0}^{m}\frac{1}{m+1}f_i^m f_i^{m*}\right)$$

$$= -\sum_{i=0}^{m}\frac{1}{m+1}log_2\left(\frac{1}{m+1}\right) = -log_2(\frac{1}{m+1})$$

Hence

$$C_\chi(\Phi_{m,1,1}) = S\left(\Phi_{m,1,1}\left(\frac{I_{P_{m-1}}}{m}\right)\right) - S_{min}(\Phi_{m,1,1})$$
$$= -log_2(\frac{1}{m+1}) + \frac{1}{m+1}log_2\frac{1}{m+1} + \frac{m}{m+1}log_2\frac{m}{m+1}$$
$$= \frac{m}{m+1}\left(log_2\frac{m}{m+1} - log_2\frac{1}{m+1}\right)$$

□

References

[1] M. Nuwairan, SU(2)-Irreducibly Covariant Quantum Channels and Some Applications (2015).

[2] G. Falland, A course in Abstract Harmonic Analysis, CRC press, 1995.

[3] A. Holevo, The additivity problem in quantum information theory, Section Lectures, ICM 2006 Madrid, Mathematical Aspect of Computer Science, 2006.

[4] A. Holevo, Quantum systems, Channels, Information: A mathematical introduction, Walter de Gruyter GmbH, Berlin/Boston, 2012.

[5] M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge university press, UK, 2000.

[6] J. Watrous, CS 766/QIC Theory of Quantum Information, Lectures, Institute for Quantum Computing, University of Waterloo (Fall 2011).

[7] A. Holevo, The capacity of quantum communication channel with general signal states, IEEE Trans. Inform. Theory 44 (1) (1998) 269-272.

[8] B. Schumacher, M. Westmoreland, Sending classical information via noisy quantum channel, Phys.Rev.A 56 (1) (1997) 131-138.

[9] M. Hastings, Super additivity of communication capacity using entangled inputs, Nature Physics 5 (2009) 255-257.

[10] T. Brocker and T. Dieck, Representations of Compact Lie Groups, Springer-Verlag New York Inc. 1985.

[11] W. Fulton and J. Harris, Representation Theory A first course, Springer-Verlag, 1991.

[12] V. Paulsen, Completely bounded maps and operator algebras, Campbridge university press, UK, 2002.

[13] C. Procesi, Lie Groups An Approach through Invariants and Represenatations, Springer Science+ Business Media, LLC, 2007.

[14] N.Ja. Vilenkin, A.U. Kilmyk, Representation of Lie Groups and Special Functions, Volume 1 :Simplest Lie Groups, Special Functions and Integral Transforms. Kluwer academic publishers. Dordrecht/Boston/London, 1991.

Summary

Some properties of SU(2)-irreducibly covariant quantum channels

양자정보학에서 정확한 공식과 성질이 잘 알려진 양자채널은 많이 존재하지 않는다. 본 학위논문에서는 군 SU(2)에 기약으로 공변하는 양자채널인 EPOSIC 채널을 소개하고, 그것의 χ-용량과 엔트로피를 계산한다. 군 표현론과 양자정보학의 기초를 복습하고, 군 표현론을 이용하여 새로운 양자채널들의 집합인 EPOSIC 채널을 만든다. 또한 EPOSIC 채널의 구체적인 공식과 성질들을 알아본다.

주요어: SU(2), EPOSIC 채널, 양자채널

학번: 2014-21188