ZERO-ERROR CORRECTIBILITY AND PHASE RETRIEVABILITY FOR TWIRLING CHANNELS

Deguang Han

Department of Mathematics, University of Central Florida, Orlando, Florida 32816, USA
(e-mail: deguang.han@ucf.edu)

and

Kai Liu

Department of Mathematics, University of Central Florida, Orlando, Florida 32816, USA
(e-mail: kai.liu@ucf.edu)

(*Received April 11, 2023 — Revised August 15, 2023*)

A twirling channel is a quantum channel induced by a continuous unitary representation $\pi = \sum_i^{\oplus} m_i \pi_i$ on a compact group G, where π_i are inequivalent irreducible representations. Motivated by a recent work [8] on minimal mixed unitary rank of Φ_π, we explore the connections of the independence number, zero-error capacity, quantum codes, orthogonality index and phase retrievability of the quantum channel Φ_π with the irreducible representation multiplicities m_i and the irreducible representation dimensions $\dim H_{\pi_i}$. In particular, we show that the independence number of Φ_π is the sum of the multiplicities, the orthogonal index of Φ_π is exactly the sum of those representation dimensions, and the zero-error capacity is equal to $\log(\sum_{i=1}^d m_i)$. We also present a lower bound for the phase retrievability in terms of the minimal length of phase retrievable frames for $\mathbb{C}^n$.

Keywords: covariant quantum channels, twirling channels, independence number, quantum code, zero-error capacity, orthogonality index, phase retrievable frames.

1. Introduction

A quantum channel Φ is a completely positive trace-preserving (CPTP) linear map from an operator system $B(H)$ to an operator system $B(K)$, which has a Kraus representation of the form

$$\Phi(T) = \sum_{i=1}^{r} A_i T A_i^*, \quad \forall T \in B(H),$$

for some operators $A_1, \ldots, A_r \in B(H, K)$. In this representation, $A_1, \ldots, A_r$ are also referred as the Kraus operators of Φ. For a quantum channel Φ, the Choi–Jamiołkowski matrix [10, 27] is the matrix defined by

$$C_\Phi = [\Phi(E_{ij})]_{n\times n} = \sum_{i,j=1}^{n} E_{ij} \otimes \Phi(E_{ij}),$$

where $\{e_i\}_{i=1}^n$ is an orthonormal basis of H and E_{ij} is the rank-one operator $e_i \otimes e_j$. The *Choi rank* of Φ is the smallest integer r from the Kraus representations which is equal to the rank of C_Φ.

Covariant channels form a special and important type of quantum channels where certain symmetries are present in the quantum channel. In this paper we are interested in exploring the connections of some important concepts/quantities for a group representation induced quantum channels (also referred to as twirling channels) with its irreducible decomposition of the group representation.

For a compact group G, a continuous function $\pi : G \to U(H)$ is called a (finite-dimensional) unitary representation if $\pi(gh) = \pi(g)\pi(h)$. A subspace V of H is called π-invariant if $\pi(g)x \in V$ for all $g \in G$ and $x \in V$. A representation π is called irreducible if 0 and H are the only π-invariant subspaces. It is well known that any unitary representation π on a finite-dimensional Hilbert space H is the direct sum of irreducible representations. More precisely, there exists a unitary operator U on H such that

$$U\pi(g)U^* = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d,$$

where $m_i \in \mathbb{N}$ and $\pi_1, \ldots, \pi_d$ are inequivalent irreducible unitary representations of G acting on the Hilbert spaces $H_1, \ldots, H_d$, respectively. Clearly we have $\dim H = \sum_{i=1}^d m_i n_i$, where $n_i = \dim H_i$.

With the help of a characterization for mixed unitary quantum channels by the complement channels, it was proved recently in [8] that a unitary representation π induced quantum channel Φ_π has the minimal mixed unitary rank in the sense that its mixed unitary rank is the same as the Choi rank which is equal to $r = \sum_{i=1}^d (\dim H_i)^2$. Inspired by this, naturally one would like to know how the multiplicity vector $\mathbf{m} = (m_1, \ldots, m_d)$ and the dimension vector $\mathbf{n} = (n_1, \ldots, n_d)$ of the representation are related to several other concepts such as independence number, quantum codes, zero-error capability for the induced quantum channels. It is well known that independence numbers and quantum zero-error capacity are among the important quantities in quantum communication theory and they have been extensively studied in the literature cf. [2, 3, 6, 7, 17]. Additionally we are also interested in exploring some “dual versions" of these concepts that include the concepts of orthogonality index and phase retrievability. The phase retrievability of a quantum channel Φ, which was recently introduced in [29], concerns the ability of distinguishing the pure states from the input system by a positive operator-valued measure (POVM) or observables from the output system. The main purpose of this note is to obtain precise characterizations for all the above mentioned quantities for twirling channels Φ_π. More precisely we shall prove the following statements:

(i) $\alpha(\Phi_\pi) = \sum_{i=1}^d m_i$ is the independence number of Φ_π, and the zero-error capacity $C_0(\Phi_\pi)$ is equal to $\log(\sum_{i=1}^d m_i)$.

(ii) $\beta(\Phi_\pi) = \max\{m_1, \dots, m_d\}$ is the largest number m such that there exists a quantum code of dimension m.
(iii) $\sum_{i=1}^{d} n_i$ is the orthogonality index of Φ_π.
(iv) $\max\{n_1, \dots, n_d\}$ is the largest integer N such that there exists an N-dimensional subspace M with the property $\Phi_\pi(x \otimes y) = 0$ whenever $x \perp y$ and $x, y \in M$.
(v) $\max\{\beta(\Phi_\pi), \lfloor \frac{d}{4} + 1 \rfloor\}$ is a lower bound for the phase retrievability of Φ_π.

2. Preliminaries

We recall some notation, definitions and basic facts that are needed for the rest of this paper.

2.1. Notations

Here is a list of standard notation we will use in this paper: Let H, K be finite-dimensional Hilbert spaces over $\mathbb{C}$.

- $B(H, K)$ — the space of all the linear operators from H to K, write $B(H) = B(H, K)$ if $H = K$. In the case that $H = \mathbb{C}^n$ and $K = \mathbb{C}^m$, $B(H, K) = M_{m \times n}(\mathbb{C})$ and we use $M_n(\mathbb{C})$ for the case when $m = n$. We use I_H (or I if no confusion from the context) to denote the identity operator on H.
- $\langle A, B\rangle = \mathrm{tr}(AB^*)$ is the trace inner product on $B(H)$, and $U(H)$ is the group of unitary operators on a complex Hilbert space H.
- For a subset $\mathcal{A}$ of $B(H)$, the commutant $\mathcal{A}' = \{T \in B(H) : TA = AT, \forall A \in \mathcal{A}\}$.
- Let $x \in H, y \in K$. We will use $x \otimes y$ to denote the rank-one operator defined by $z \mapsto \langle z, y\rangle x$ for $z \in K$. Occasionally, $x \otimes y$ is also used to denote the tensor product in $H \otimes K$ and the readers should be able to distinguish them from the context.
- Let π be a unitary representation of a group G, we use $m\pi$ to denote the representation $\pi \oplus \cdots \oplus \pi$ (m-copies). Any unitary representation π on a finite-dimensional Hilbert space can be decomposed as
$$\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d,$$
where π_i are inequivalent irreducible unitary representations.
- For a unitary representation π of a group G on a Hilbert space H, we use $\mathcal{A}_\pi$ to denote the algebra generated by $\pi(G)$. Clearly $\mathcal{A}_\pi = \mathrm{span}\{\pi(g) : g \in G\}$ which is a C*-algebra.
- Two unitary representations $\pi : G \to U(H)$ and $\sigma : G \to U(K)$ are called *disjoint* if they have no equivalent subrepresentations, or equivalently the intertwining space is trivial, i.e.
$$\mathrm{Hom}(\pi, \sigma) = \{T \in B(H, K) : T\pi(g) = \sigma(g)T\} = \{0\}.$$
In particular, any two inequivalent irreducible representations are disjoint.
- $[d] = \{1, 2, \dots, d\}$.

2.2. Quantum code, independent number and orthogonality index

Let $\Phi : B(H) \to B(K)$ be a quantum channel. Recall that a quantum code C for a noise quantum channel Φ is a subspace of the Hilbert space such that there exists another channel Ψ such that

$$\rho = \Psi \circ \Phi(\rho)$$

for any state ρ supported on C. In this case we say that C is correctable under the noise channel Φ.

Related to quantum code is the concept of *independence number* for a quantum channel Φ, which is the largest integer m such that there is an orthonormal set $\{x_k\}_{k=1}^m$ such that $x_k \otimes x_\ell \perp E_i^* E_j$ for all i, j and all $k \neq \ell$, where $\{E_i\}_{i=1}^r$ are Kraus operators of Φ. In what follows the independence number of Φ will be denoted by $\alpha(\Phi)$. This is the same largest integer m with which there exists a set of states $\rho_1, \ldots, \rho_m \in B(H)$ such that $\Phi(\rho_1), \ldots, \Phi(\rho_m)$ can be perfectly distinguished cf. [15]. The *zero-error capacity* of a channel Φ is defined in an asymptotic setting by

$$C_0(\Phi) = \lim_{n\to\infty} \frac{1}{n} \log \alpha(\Phi^{\otimes n}),$$

where $\Phi^{\otimes n}$ is the n-fold quantum channel defined on the $B(H^{\otimes n})$. It is well known that the zero-error capacity is even harder to compute than the independence number. In fact, it is not even known if it is in general a computable quantity in the sense of Turing cf. [17].

It is known that the independent number is also the largest integer $\alpha(\Phi)$ such that there exists an orthonormal set $\{x_i\}_{i=1}^N$ with the property $\Phi(x_i \otimes x_i) \perp \Phi(x_j \otimes x_j)$ for any $i \neq j$. Motivated by this we define the *orthogonality index* of Φ, denote it by $\gamma(\Phi)$, to be the largest number N such that there exist N nonzero vectors $\{x_i\}_{i=1}^N$ with the property $\Phi(x_i \otimes x_j) = 0$ for any $i \neq j$.

2.3. Covariant quantum channels

Let π and σ be unitary representations of a compact group G on $\mathbb{C}^n$ and $\mathbb{C}^m$, respectively. We say that Φ is (π, σ)-covariant if

$$\Phi(\pi(g)T\pi(g^{-1})) = \sigma(g)\Phi(T)\sigma(g^{-1})$$

holds for every $g \in G$.

Covariant quantum channels form an important class of channels since many challenging problems in quantum information theory are usually more tractable when certain symmetries are imposed on the channel. We refer to [5, 9, 14, 18–21, 30, 32, 33, 35] for some recent progresses on theoretical studies of covariant quantum channels. In particular, in their recent work [30], M. Mozrzymas, M. Studziński and N. Datta investigated the structure of covariant quantum channels with respect to an irreducible representation π for a finite group G, and obtained spectral decomposition of such covariant quantum channels in terms of representation characteristics of the group G.

There is a natural way, called channel twirling, to produce a (π, σ)-covariant quantum channel from any given quantum channel. Let $\Phi : B(H) \to B(K)$ be a quantum channel, and π, σ be two continuous unitary representations of a group G on H and K, respectively. Then

$$\Psi(T) = \int_G \sigma(g^{-1})\Phi(\pi(g)T\pi(g^{-1}))\sigma(g)d\mu(g)$$

is a (π, σ)-covariant quantum channel, where μ is the Haar measure of the compact group G. Note that

$$\Psi(T) = \frac{1}{|G|}\sum_{g\in G} \sigma(g^{-1})\Phi(\pi(g)T\pi(g^{-1}))\sigma(g)$$

if G is finite.

Now we consider a special type of covariant quantum channels (the ones twirled from the identity map). Let $\pi : G \to U(H)$ and $\sigma : G \to U(K)$ be two continuous unitary representations. We define a linear map $\Phi_{\pi,\sigma} : B(K, H) \to B(K, H)$ by

$$\Phi_{\pi,\sigma}(T) = \int_G \pi(g)T\sigma(g^{-1})d\mu(g)$$

and denote $\Phi_{\pi,\sigma}$ by Φ_π when $\pi = \sigma$. Then Φ_π is a π-covariant quantum channel which will be called a *π-induced twirling channel*. Twirling channels have a long history in the quantum information literature and have numerous applications. For example, channels of this form have been used in the contexts of quantum error correction, quantum data hiding, as well as in the study of quantum entanglement, and quantum coherence c.f [2, 4, 11, 37].

Here is a list of properties that will be needed for the rest of this paper.

- $\mathcal{A}'_\pi = \mathrm{range}(\Phi_\pi)$;
- π is irreducible if and only if $\Phi_\pi(T) = \frac{1}{\dim H}\mathrm{tr}(T)I$ for every $T \in B(H)$;
- $\Phi_{\pi,\sigma} = 0$ if and only if π and σ are disjoint. In particular, $\Phi_{\pi,\sigma} = 0$ when π and σ are inequivalent irreducible representations.

2.4. Frames and phase-retrievability

Frame theory is closely related to operator-valued measures and consequently to quantum information theory. Phase retrieval property of a frame is probably the most relevant part to quantum information theory cf. [34]. Recall that a sequence $\{f_j\}_{j\in\mathbb{J}}$ is called a *frame* for a Hilbert space H if there are two positive constant numbers $A, B > 0$ such that

$$A\|x\|^2 \le \sum_{i\in I} |\langle x, f_i\rangle|^2 \le B\|x\|^2$$

holds for every $x \in H$. A frame is called a *tight frame* if $A = B$ and a *Parseval frame* if $A = B = 1$. A frame $\{f_j\}_{j\in\mathbb{J}}$ is a Parseval frame if and only if $\sum_{j\in\mathbb{J}} f_j \otimes f_j = I$.

Every frame $\{f_j\}_{j\in\mathbb{J}}$ is similar to a Parseval frame in the sense that there is an invertible operator $S \in B(H)$ such that $\{Sf_j\}_{j\in\mathbb{J}}$ is a Parseval frame. In the finite-dimensional case, a finite sequence $\{x_i\}_{i=1}^N$ is a frame for H if and only if $H = \mathrm{span}\{x_i : 1 \le i \le N\}$.

A *phase retrieval frame* for a Hilbert space H refers to a frame $\{f_j\}_{j\in\mathbb{J}}$ in H such that the magnitudes of the frame coefficients $\langle x, f_j\rangle$ of a signal $x \in H$ uniquely determine the rank-one state $x\otimes x$. More generally, a collection of operators $\{A_j\}_{\in\mathbb{J}}$ in $B(H)$ is called a *phase retrievable operator-valued frame* for H if the phaseless measurements $\langle A_j x, x\rangle$ uniquely determine $x\otimes x$. It is obvious that a (vector-valued) frame $\{f_j\}_{j\in\mathbb{J}}$ is phase retrievable if and only if $\{f_j\otimes f_j\}_{j\in\mathbb{J}}$ is a phase retrievable operator-valued frame. A natural question is to find the minimal length of a phase retrievable frame for $\mathbb{R}^n$ and $\mathbb{C}^n$.

For an n-dimensional Hilbert space H, we will use $\mathcal{I}_n$ to denote the smallest integer N such that there is a phase retrievable frame $\{x_j\}_{j=1}^N$ for H. The following is well known in the literature.

Proposition 2.1. *If H be an n-dimensional complex Hilbert space, then $\mathcal{I}_n \le 4n-4$. Moreover, every generic frame $\{f_j\}_{j=1}^N$ of length $N \ge 4n-4$ is phase retrievable.*

A positive operator-valued measure (POVM for short) or observables on a Hilbert space H is a collection of positive operators $\{F_i\}$ in $B(H)$ such that $\sum_{j\in\mathbb{J}} F_j = I_H$. A POVM $\{F_j\}_{j\in\mathbb{J}}$ is *information complete* (cf. [34]) if $\{\langle x, F_j x\rangle\}_{j\in\mathbb{J}}$ uniquely determines the pure state $x\otimes x$. In other words, an information complete POVM is a phase retrievable operator-valued frame. For a quantum channel $\Phi : B(H) \to B(K)$, its adjoint Φ^* is unital and hence $\{\Phi^*(F_j)\}_{j\in\mathbb{J}}$ is a POVM for H whenever $\{F_j\}_{j\in\mathbb{J}}$ is a POVM for K. In the Heisenberg picture of quantum channels, a POVM in K are the observables that are used to measure a state ρ in $B(H)$ with measurement $\langle \rho, \Phi^*(F_j)\rangle = \mathrm{tr}(\rho\Phi^*(F_j)) = \mathrm{tr}(\Phi(\rho)F_j)$.

It is important that a quantum channel Φ admits a POVM on K that distinguishes the pure states from H (cf. [13, 36]). Such a quantum channel was called in [29] *phase retrievable*, and some characterizations were discussed in terms of the Kraus operators. Clearly many quantum channels are not phase retrievable. For this reason, we introduce the following definition.

Definition 2.1. A subspace M of H is called *phase retrievable* under a quantum channel $\Phi : B(H) \to B(K)$ if there exists a POVM $\{F_j\}_{j\in\mathbb{J}}$ in $B(K)$ such that $\{P_M\Phi^*(F_j)P_M\}_{j\in\mathbb{J}}$ is a phase retrievable operator-valued frame for M, where P_M is the orthogonal projection onto M.

We will point out later that M is called phase retrievable subspace for Φ if and only if Φ is pure state injective on M, i.e. $\Phi(x\otimes x) = \Phi(y\otimes y)$ implies that $x\otimes x = y\otimes y$ for $x, y \in M$. The *phase retrievability index* $\mathrm{pr}(\Phi_\pi)$ is defined to be the largest integer k such that there exits a k-dimensional subspace $M \subset H$ such that M is phase retrievable under Φ. We will examine $\mathrm{pr}(\Phi_\pi)$ in Section 5.

3. Quantum codes and independence numbers of Φ_π

Recall that a quantum code C for a noise quantum channel Φ is a subspace of the Hilbert space such that there exists another channel Ψ such that

$$\rho = \Psi \circ \Phi(\rho)$$

for any state ρ supported on C. We need the following lemma.

LEMMA 3.1. *Let C be a subspace of H, and let P be the orthogonal projections onto C. Suppose Φ is a quantum channel with Kraus operators $\{E_i\}_{i=1}^r$. Then the following are equivalent:*

(i) *C is a quantum code for Φ.*
(ii) *There exists a Hermitian matrix $A = [a_{ij}]$ such that $PE_i^*E_jP = a_{ij}P$ holds for all i, j.*
(iii) *For any orthonormal basis $\{x_k\}_{k=1}^m$ of C, $x_k \otimes x_\ell \perp E_i^*E_j$ for all i, j and all $k \neq \ell$.*
(iv) *For any orthonormal basis $\{x_k\}_{k=1}^m$ of C, $\Phi(x_k \otimes x_k) \perp \Phi(x_\ell \otimes x_\ell)$ for any $k \neq \ell$.*

Proof: The equivalence of (i), (ii) and (iii) are well known (cf. Theorem 5.2 [6]). (iii) $\Leftrightarrow$ (iv): Note that

$$\langle \Phi(x_k \otimes x_k), \Phi(x_\ell \otimes x_\ell)\rangle = \sum_{i,j=1}^{r} \mathrm{tr}((E_ix_k \otimes E_ix_k)(E_jx_\ell \otimes E_jx_\ell))$$

and $\mathrm{tr}((E_ix_k \otimes E_ix_k)(E_jx_\ell \otimes E_jx_\ell)) \geq 0$. Therefore $\langle \Phi(x_i \otimes x_i), \Phi(x_j \otimes x_j)\rangle = 0$ if and only if

$$|\langle E_jx_\ell, E_ix_k\rangle|^2 = \mathrm{tr}((E_ix_k \otimes E_ix_k)(E_jx_\ell \otimes E_jx_\ell) = 0. \qquad \square$$

By Lemma 3.1, the independence number m for a quantum channel Φ is the largest integer m such that there is an orthonormal set $\{x_k\}_{k=1}^m$ such that $\Phi(x_k \otimes x_k)$ and $\Phi(x_\ell \otimes x_\ell)$ are orthogonal in the trace inner product for any $k \neq \ell$, where $\{E_i\}_{i=1}^r$ are Kraus operators of Φ. Moreover, if C is a quantum code for Φ, then Lemma 3.1 also implies that $\alpha(\Phi) \geq \dim C$, and hence

$$\alpha(\Phi) \geq \max\{\dim C : C \text{ is a quantum code for } \Phi\}.$$

In what follows we will use $\beta(\Phi)$ to denote the right-hand-side of the above inequality. The following simple example shows that the equality does not hold in general.

EXAMPLE 3.1. Let $\Phi : M_{2\times 2}(\mathbb{C}) \to M_{2\times 2}(\mathbb{C})$ be a quantum channel with Kraus operators $E_1 = e_1 \otimes e_1$ and $E_2 = e_2 \otimes e_2$. Then $\Phi(e_1 \otimes e_1) \perp \Phi(e_2 \otimes e_2)$, and hence $\alpha(\Phi) = 2$. However, $\mathbb{C}^2$ is not a correctable quantum code for Φ since condition (ii) in Lemma 3.1 is not satisfied. Thus $\beta(\Phi) = 1$.

On the other hand there are plenty of quantum channels when the equality holds.

Example 3.2. Let $\Phi : B(H) \to B(H \oplus H)$ be a quantum channel with Kraus operators E_1, E_2 defined by $E_1 x = \frac{1}{\sqrt{2}}(x \oplus 0)$ and $E_2 x = \frac{1}{\sqrt{2}}(0 \oplus x)$ for any $x \in H$. Then $E_1^* E_1 = E_2^* E_2 = \frac{1}{2} I_H$, and $E_i^* E_j = 0$ if $i \neq j$. Thus H is a quantum code for Φ, and hence $\alpha(\Phi) = \beta(\Phi) = \dim H$.

It is natural to explore necessary and/or sufficient conditions under which the equality holds. We will prove that the equality holds for a twirling channel Φ_π if and only if π is unitarily equivalent to $m\sigma$ for some irreducible representation σ and $m \in \mathbb{N}$. We first show that $\alpha(\Phi_\pi) = \sum_{i=1}^d m_i$.

Theorem 3.1. *Suppose that $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ is a unitary representation of G on a Hilbert space H, where each π_i is irreducible and π_i, π_j are inequivalent for $\forall 1 \leq i \neq j \leq d$. Then $\alpha(\Phi_\pi) = \sum_{i=1}^d m_i$.*

Proof: Let $\mathcal{A}_\pi$ be the C*-algebra generated by $\pi(G)$. Then

$$\mathcal{A}_\pi = (I_{m_1} \otimes B(H_1)) \oplus \cdots \oplus (I_{m_d} \otimes B(H_d)),$$

where I_{m_i} is the identity matrix on $\mathbb{C}^{m_i}$. Let $\{e_{ij}\}_{j=1}^{m_i}$ be the canonical orthonormal basis for $\mathbb{C}^{m_i}$ and pick a unit vector $x_i \in H_i$. Set $x_{ij} = e_{ij} \otimes x_i$ viewing it as a vector in H by considering $\mathbb{C}^{m_i} \otimes H_i$ as a subspace of H. Then it is obvious that $\langle x_{ij}, Ax_{k\ell}\rangle = 0$ for all $(i, j) \neq (k, \ell)$ and all $A \in \mathcal{A}_\pi$. This implies that $\alpha(\Phi_\pi) \geq \sum_{i=1}^d m_i$.

Conversely, suppose $x_1, \ldots, x_N$ is a collection of nonzero vectors in H such that $\langle x_i, Ax_k\rangle = 0$ for all $i \neq k$ and for all $A \in \mathcal{A}_\pi$. Let $M_i = \mathcal{A}_\pi x_i$. Then we have that $M_i \perp M_j$ for all $i \neq j$ and each M_i is π-invariant. Let σ_i be the restriction of π to M_i. Then each σ_i is a unitary representation and $\sigma_1 \oplus \cdots \oplus \sigma_N$ is a subrepresentation of π. Since π is the direct sum of only $m_1 + \cdots + m_d$ number of irreducible subrepresentations, we get that $N \leq \sum_{i=1}^d m_i$ which implies that $\alpha(\Phi_\pi) \leq \sum_{i=1}^d m_i$. Thus we proved the claim that $\alpha(\Phi_\pi) = \sum_{i=1}^d m_i$. □

To prove $\beta(\Phi_\pi) = \max\{m_1, \ldots, m_d\}$ we first consider the following special case.

Lemma 3.2. *If $\pi = m\sigma = I_m \otimes \sigma$ acting on $\mathbb{C}^m \otimes K$ such that $\sigma : G \to U(K)$ is irreducible, then $\alpha(\Phi_\pi) = \beta(\Phi_\pi) = m$.*

Proof: First, by Theorem 3.1, we know that $\alpha(\Phi_\pi) = m$. Now fix a unit vector $x \in K$ and let $x_i = e_i \otimes x$, where $\{e_i\}_{i=1}^m$ is the canonical orthonormal basis for $\mathbb{C}^m$. Let $C = \operatorname{span}\{x_i\}_{i=1}^m = \mathbb{C}^m \otimes x$. It is enough to show that C is a quantum code for Φ. For any $u = \mathbf{c} \otimes x, v = \mathbf{d} \otimes x \in C$ such that $u \perp v$, we have that $\mathbf{c} \perp \mathbf{d}$. Since $\mathcal{A}_\pi = I_m \otimes B(K)$, we get

$$\langle u, Av\rangle = \langle \mathbf{c}, \mathbf{d}\rangle \cdot \langle x, Tx\rangle = 0$$

for any $A = I_m \otimes T \in \mathcal{A}_\pi$, which implies by Lemma 3.1 that C is a quantum code. Thus we obtain $\alpha(\Phi_\pi) = \beta(\Phi_\pi)$. □

THEOREM 3.2. *Suppose that $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ is a unitary representation of G on a Hilbert space H, where π_i is irreducible and π_i, π_j are inequivalent for $\forall 1 \le i \ne j \le d$. Then $\beta(\Phi_\pi) = \max\{m_1, \dots, m_d\}$.*

Proof: Let C be a quantum code of dimension N for Φ_π. Let $\{u_j\}_{i=1}^N$ be an orthonormal basis for C, and P_i be the orthogonal projection onto the subspace $\mathbb{C}^{m_i} \otimes H_i$. Since $P_1 + \cdots + P_d = I$, there exists an i such that $P_i u_1 \ne 0$. For any fixed index $j \ge 2$, $u_1 + u_j, u_1 - u_j$ are two orthogonal vectors in C. Since C is a quantum code, we get that $u_1 \perp \mathcal{A}_\pi u_j$ and $u_1 + u_j \perp \mathcal{A}_\pi(u_1 - u_j)$. In particular, since $P_i \in \mathcal{A}_\pi$ we have

$$\langle u_j, P_i u_1\rangle = 0 \quad \text{and} \quad \langle u_1 + u_j, P_i(u_1 - u_j)\rangle = 0.$$

The above two combined imply that $Pu_j \perp Pu_1$ and $\|P_i u_j\| = \|P_i u_1\|$. With the same argument by replacing u_1 by u_j, and j by another index j', we clearly get that $\{P_i u_j\}_{j=1}^N$ is an orthogonal set of nonzero vectors in $\mathbb{C}^{m_i} \otimes H_i$ such that $P_i u_j \perp \mathcal{A}_{m_i\pi_i} P_i u_{j'}$ for any $j \ne j'$. Thus $N \le \alpha(\Phi_{m_i\pi}) = m_i$, and therefore $\beta(\Phi_\pi) \le \max\{m_i : 1 \le i \le d\}$.

On the other hand, without losing the generality we can assume that $m_1 = \max\{m_i : i = 1, \dots, d\}$. By Lemma 3.2, there is an m_1-dimensional quantum code C_1 in $\mathbb{C}^{m_1} \otimes H_1$ for $\Phi_{m_1\pi_1}$. Clearly $C = C_1 \oplus 0 \oplus \cdots \oplus 0$ is a quantum code of Φ_π. Thus we have $\beta(\Phi_\pi) \ge \dim C = m_1$, and consequently we have proved $\beta(\Phi_\pi) = \max\{m_1, \dots, m_d\}$. □

COROLLARY 3.1. *Let $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ be a unitary representation of G on a Hilbert space H, where π_i is irreducible and π_i, π_j are inequivalent for $\forall 1 \le i \ne j \le d$. Then $\alpha(\Phi_\pi) = \beta(\Phi_\pi)$ if and only if $d = 1$.*

Proof: If $d = 1$, then $\alpha(\Phi_\pi) = \beta(\Phi_\pi)$ follows from Lemma 3.2. Conversely, since $\alpha(\Phi_\pi) = m_1 + \cdots + m_d$ and $\beta(\Phi_\pi) = \max\{m_1, \dots, m_d\}$, we immediately get $d = 1$ if $\alpha(\Phi_\pi) = \beta(\Phi_\pi)$. □

Let G be a group and $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ be a unitary representation of G onto a finite-dimensional Hilbert space H. Let $G^n = \{\mathbf{g} = (g_1, \dots, g_n) : g_i \in G\}$ be the product group and $\pi_\pi^{\otimes n}$ be the unitary presentation of G on $H^{\otimes n}$ defined by

$$\pi_\pi^{\otimes n}(\mathbf{g}) = \pi(g_1) \otimes \cdots \otimes \pi(g_n), \quad \forall \mathbf{g} \in G^n.$$

THEOREM 3.3. *Let $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ be a unitary representation of G on a Hilbert space H, where π_i is irreducible and π_i, π_j are inequivalent for $\forall 1 \le i \ne j \le d$. Then*

$$C_0(\Phi_\pi) = \log\Big(\sum_{i=1}^d m_i\Big).$$

Proof: Write $[d]^n = \{(k_1, \dots, k_n) : k_i \in [d]\}$. The $\pi_\pi^{\otimes n}$ has the decomposition of the form

$$\pi_\pi^{\otimes n} = \sum_{(k_1,\dots,k_n)\in[d]^n}^{\oplus} m_{k_1} \cdots m_{k_n} (\pi_{k_1} \otimes \cdots \otimes \pi_{k_n})$$

Note that $\pi_{k_1} \otimes \cdots \otimes \pi_{k_n}$ is irreducible, and $\pi_{k_1} \otimes \cdots \otimes \pi_{k_n}$, $\pi_{k_1'} \otimes \cdots \otimes \pi_{k_n'}$ are inequivalent whenever $(k_1, \ldots, k_n) \neq (k_1', \ldots, k_n')$ (This can be easily checked by comparing their characters). Thus, by Theorem 3.1, we get

$$\alpha(\Phi_\pi^{\otimes n}) = \alpha(\Phi_{\pi^{\otimes n}}) = \sum_{(k_1,\ldots,k_n)\in[d]^n} m_{k_1} m_{k_2} \cdots m_{k_n} = (m_1 + \cdots + m_d)^n,$$

and hence $C_0(\Phi_\pi) = \lim_{n\to\infty} \frac{1}{n} \log \alpha(\Phi_\pi^{\otimes n}) = \log(\sum_{i=1}^d m_i)$. □

4. Orthogonality index of Φ_π

Recall that the orthogonality index of a quantum channel Φ, denoted by $\gamma(\Phi)$, is the largest number N such that there exists $\{x_i\}_{i=1}^N$ such that $\Phi(x_i \otimes x_j) = 0$ for any $i \neq j$. This is a concept related to strongly disjoint frames that plays extremely important roles in frame theory and in establishing a Balian-Low type of duality principle for group representation frames cf. [1, 16, 24, 25]. Let $\{x_i\}_{i=1}^N$ be a sequence in a Hilbert space H and $\{y_i\}_{i=1}^N$ be a sequence in a Hilbert space K. We say that $\{x_i\}_{i=1}^N$ $\{y_i\}_{i=1}^N$ are *strongly disjoint* if $\sum_{i=1}^N \langle x, x_i\rangle y_i = 0$ for all $x \in H$, or equivalently, $\sum_{i=1}^N y_i \otimes x_i = 0$. Consequently, $\Phi_\pi(x \otimes y) = 0$ if and only if $\{\pi(g)x\}_{g\in G}$ and $\{\pi(g)y\}_{g\in G}$ are strongly disjoint. In this case we also say that x and y are *π-orthogonal* [16].

LEMMA 4.1. *Let $\pi : G \to U(H)$ be a unitary representation and $x, y \in H$. Then $\Phi_\pi(x \otimes y) = 0$ if and only if $x \perp \mathcal{A}_\pi' y$.*

Proof: Recall that $\mathcal{A}_\pi' = \text{range}(\Phi)$ and $\Phi = \Phi^*$. Thus we have

$$\langle T, \Phi(x \otimes y)\rangle = \langle \Phi(T), x \otimes y\rangle = \langle \Phi(T)x, y\rangle$$

which implies that $\Phi(x \otimes y) = 0$ if and only if $x \perp \Phi(T)y$ for every $T \in B(H)$. Thus we get that x and y are π-orthogonal if and only if $x \perp \mathcal{A}_\pi' y$. □

We remark that since $\mathcal{A}_\pi'$ is a C*-algebra, we have that $\mathcal{A}_\pi' x \perp \mathcal{A}_\pi' y$ if and only if $x \perp \mathcal{A}_\pi' y$.

LEMMA 4.2. *If $\pi = m\sigma : G \to U(H)$ acting on $H = \mathbb{C}^m \otimes K$ such that $\sigma : G \to U(K)$ is irreducible, then $\gamma(\Phi_\pi) = \dim K$.*

Proof: If $\Phi_\pi(x \otimes y) = 0$ for some $x, y \in H = \mathbb{C}^m \otimes K$, then by Lemma 4.1 we have $\mathcal{A}_\pi' x \perp \mathcal{A}_\pi' y$, where $\mathcal{A}_\pi' = M_m(\mathbb{C}) \otimes I$. Note that we can always write x, y in the form of $x = \sum_{i=1}^m e_i \otimes x_i$ and $y = \sum_{i=1}^m e_i \otimes y_i$ for some $x_i, y_i \in K$, where $\{e_i\}_{i=1}^m$ is the canonical orthonormal basis for $\mathbb{C}^m$. Let $E_{ii} = e_i \otimes e_i \in M_m(\mathbb{C})$. Since $E_{ii} \otimes I \in \mathcal{A}_\pi'$, we get

$$\langle x_i, y_j\rangle = \langle (E_{ii} \otimes I)x, (E_{jj} \otimes I)y\rangle = 0$$

for all $i, j \in [m]$.

Now, let $\{u_i\}_{j=1}^N$ be an orthonormal set in H such that $\Phi_\pi(u_i \otimes u_j) = 0$ for any $i \neq j$. Write $u_i = \sum_{j=1}^m e_i \otimes u_{ij}$, where $u_{ij} \in K$. For each i, pick an index n_i such that $u_{in_i} \neq 0$. Then by the above argument we get that $\{u_{in_i}\}_{i=1}^N$ is an orthogonal set of nonzero vectors in K. This implies that $N \leq \dim K$, and hence $\gamma(\Phi_\pi) \leq \dim K$.

On the other hand, let $\{u_i\}_{i=1}^n$ be an orthonormal basis for K and let $x_i = e_1 \otimes u_i \in H$ for $i \in [n]$. Then clearly we have $\mathcal{A}'_\pi x_i \perp \mathcal{A}'_\pi x_j$ for any $i \neq j$. Thus $\gamma(\Phi_\pi) \geq \dim K$, which completes the proof. □

Now we prove for the general case.

Theorem 4.1. *Suppose that $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ is a unitary representation of G on a Hilbert space H, where each π_i is an irreducible representation on H_i and π_i, π_j are inequivalent for $\forall 1 \leq i \neq j \leq d$. Then $\gamma(\Phi_\pi) = \sum_{i=1}^k n_i$, where $n_i = \dim H_i$.*

Proof: Since $\mathcal{A}_\pi = (I_{m_1} \otimes B(H_1)) \oplus \cdots \oplus (I_{m_d} \otimes B(H_d))$, we get that

$$\mathcal{A}'_\pi = (M_{m_1}(\mathbb{C}) \otimes I_{H_1}) \oplus \cdots \oplus (M_{m_d}(\mathbb{C}) \otimes I_{H_d}).$$

By Lemma 4.2, there is an orthonormal basis $\{x_{ij}\}_{j=1}^{n_i}$ for $\mathbb{C}^{m_i} \otimes H_i$ that

$$x_{ij} \perp (M_{m_i}(\mathbb{C}) \otimes I_{H_i})x_{ik}$$

for $1 \leq j \neq k \leq m_i$. This implies that

$$x_{ij} \perp \mathcal{A}'_\pi x_{k\ell}$$

whenever $(i, j) \neq (k, \ell)$. Thus, $\Phi_\pi(x_{ij} \otimes x_{k\ell}) = 0$ for all $(i, j) \neq (k, \ell)$, which implies that $\gamma(\Phi_\pi) \geq \sum_{i=1}^d n_i$.

For the other direction of the inequality, let $N = \gamma(\Phi_\pi)$. Then there exists an orthonormal set $\{x_j\}_{j=1}^N$ for H such that $x_j \perp \mathcal{A}'_\pi x_k$ for all $j \neq k$. Let P_i be the orthogonal projection onto the subspace $\mathbb{C}^{m_i} \otimes H_i$. Then $P_i \in \mathcal{A}'_\pi$. This implies that $P_i x_j \perp \mathcal{A}'_{m_i\pi_i} P_i x_k$ for all $k \neq \ell$ and every i. In particular, we have $P_i x_j \perp P_i x_k$ for all $j \neq k$. Define subsets $\Lambda_1, \ldots, \Lambda_d$ of $\{1, \ldots, N\}$ inductively by

$$\Lambda_1 = \{j \in [N] : P_1 x_j \neq 0\}$$

and

$$\Lambda_i = \{j \notin \Lambda_{i-1} : P_i x_j \neq 0\}$$

for $2 \leq i \leq d$. Then $[N] = \cup_{i=1}^d \Lambda_i$. Let $y_j = P_1 x_j$ for $j \in \Lambda_1$. Then $\{y_j\}_{j\in\Lambda_1}$ is a collection of nonzero orthogonal vectors such that $y_j \perp \mathcal{A}'_{m_i\pi_i} y_k$ for all $k \neq \ell$ in Λ_1. Thus, by Lemma 4.2, we have $|\Lambda_1| \leq n_1$. With the same arguments we also have $|\Lambda_i| \leq n_i$ for $i = 2, \ldots, d$. Therefore we get $\gamma(\Phi_\pi) = N = \sum_{i=1}^d |\Lambda_i| \leq \sum_{i=1}^d n_i$, which completes the proof. □

Note that $\gamma(\Phi)$ can be considered as a “dual object" of $\alpha(\Phi)$. Similarly it is natural to consider a “dual version" of $\beta(\Phi)$. For this let us define $\tau(\Phi)$ to be the largest integer L such that there exists an L-dimensional subspace M with the property that $\Phi(x \otimes y) = 0$ whenever $x \perp y$ and $x, y \in M$. We have the following dual theorem of Theorem 3.2.

THEOREM 4.2. *Suppose that* $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ *is a unitary representation of* G *on a Hilbert space* $H = (\mathbb{C}^{m_1} \otimes H_1) \oplus \cdots \oplus (\mathbb{C}^{m_d} \otimes H_d)$, *where* π_i, π_j *are inequivalent irreducible representations for* $\forall 1 \leq i \neq j \leq d$. *Then* $\tau(\Phi_\pi) = \max\{n_1, \ldots, n_d\}$, *where* $n_i = \dim H_i$ *for each* $i \in [d]$.

Proof: We first show that $\tau(\Phi_\pi) \geq n_i$ for every $i \in [d]$. It suffices to check that $\tau(\Phi_\pi) \geq n_1$. Let $M = e_1 \otimes H_1$. Then two vectors $x = e_1 \otimes u$, $y = e_1 \otimes v \in M$ are orthogonal if and only if u and v are orthogonal vectors in H_1 Thus for any $B = (B_1 \otimes I_{H_1}) \oplus \cdots \oplus (B_d \otimes I_{H_d}) \in \mathcal{A}'_\pi$ we get $\langle x, By\rangle = \langle e_1, B_1e_1\rangle \cdot \langle u, v\rangle = 0$, which implies by Lemma 4.1 that $\Phi_\pi(x \otimes y) = 0$. Thus $\tau(\Phi_\pi) \geq n_1$, and therefore we get $\tau(\Phi_\pi) \geq \max\{n_1, \ldots, n_d\}$.

Now let M be a subspace such that $\Phi_\pi(x \otimes y) = 0$ whenever $x, y \in M$ are orthogonal vectors. Let $\{u_j\}_{i=1}^N$ be an orthonormal basis for M, and P_i be the orthogonal projection onto the subspace $\mathbb{C}^{m_i} \otimes H_i$. Since $u_1 \neq 0$ and $P_1 + \cdots + P_d = I$, there exists an index i such that $P_iu_1 \neq 0$. For any fixed index $j \geq 2$, $u_1 + u_j, u_1 - u_j$ are two orthogonal vectors in M. Thus $u_1 \perp \mathcal{A}'_\pi u_j$ and $u_1 + u_j \perp \mathcal{A}'_\pi(u_1 - u_j)$. Since $P_i \in \mathcal{A}'_\pi$ we get

$$\langle u_j, P_iu_1\rangle = 0 \quad \text{and} \quad \langle u_1 + u_j, P_i(u_1 - u_j)\rangle = 0.$$

The above two combined to imply that $Pu_i \perp Pu_1$ and $\|P_iu_j\| = \|P_iu_1\|$. With the same argument by replacing u_1 by u_j, and j by another index j', we clearly get that $\{P_iu_j\}_{j=1}^N$ is an orthogonal set of nonzero vectors in $\mathbb{C}^{m_i} \otimes H_i$ such that $P_iu_j \perp \mathcal{A}'_{m_i\pi_i}P_iu_{j'}$ for any $j \neq j'$. Thus $N \leq \gamma(\Phi_{m_i\pi})$, and hence it follows from Theorem 4.1 that $N \leq n_i$. Therefore we get $N \leq \max\{n_i : 1 \leq i \leq d\}$ and hence $\tau(\Phi_\pi) \leq \max\{n_i : 1 \leq i \leq d\}$, which completes the proof. □

5. Phase-retrievability of Φ_π

We first point out the following and provide its proof for self-completeness.

LEMMA 5.1. *[29] Let* $\Phi : B(H) \to B(K)$ *be a quantum channel and* M *be a subspace of* H. *The the following are equivalent:*

(i) *There exists a POVM* $\{F_j\}_{j=1}^N$ *such that* $\{\langle x, \Phi^*(F_j)x\rangle\}_{j=1}^N$ *uniquely determines* $x \otimes x$ *for every* $x \in M$ *(In this case we say that* Φ *is phase retrievable on* M*).*
(ii) $x \otimes x = y \otimes y$ *whenever* $\Phi(x \otimes x) = \Phi(y \otimes y)$ *and* $x, y \in M$ *(In this case we say that* Φ *is pure state injective on* M*).*

Proof: (i) $\Rightarrow$ (ii): Let $\{F_j\}_{j\in\mathbb{J}}$ be a POVM in $B(K)$ such that $\{\langle x, \Phi^*(F_j)x\rangle\}_{j=1}^N$ uniquely determines $x \otimes x$ for every $x \in M$. If $\Phi(x \otimes x) = \Phi(y \otimes y)$ with $x, y \in M$, then we have

$$\langle x \otimes x, \Phi^*(F_j)\rangle = \langle \Phi(x \otimes x), F_j\rangle = \langle \Phi(y \otimes y), F_j\rangle = \langle y \otimes y, \Phi^*(F_j)\rangle$$

for all $j \in \mathbb{J}$, and hence $x \otimes x = y \otimes y$. Therefore Φ is pure-state injective.

(ii) $\Rightarrow$ (i): Assume that Φ is pure-state injective on M. Let $\{F_j\}_{j\in\mathbb{J}}$ be a POVM such that $\mathrm{span}\{F_j : j \in \mathbb{J}\}$ coincides with the space of all self-adjoint operators of $B(K)$. Then $\langle x\otimes x, \Phi^*(F_j)\rangle = \langle y\otimes y, \Phi^*(F_j)\rangle$, where $x, y \in M$, implies $\mathrm{tr}(\Phi(x\otimes x)F_j) = \mathrm{tr}(\Phi(y\otimes y)F_j)$ for all j, which implies that $\Phi(x\otimes x) = \Phi(y\otimes y)$. Therefore $x\otimes x = y\otimes y$ and hence we get (i). □

Recall that $\mathrm{pr}(\Phi_\pi)$ is the largest integer k such that there exits a k-dimensional subspace $M \subset H$ such that M is phase retrievable under Φ.

LEMMA 5.2. *Suppose that $\pi = m_1\pi_1 \oplus\cdots\oplus m_d\pi_d$ is a unitary representation of G on a Hilbert space H, where each π_i is an irreducible representation on H_i, and π_i, π_j are inequivalent for $\forall 1 \le i \ne j \le d$. Then* $\mathrm{pr}(\Phi_\pi) \ge \max\{m_1,\ldots,m_d\} = \beta(\Phi_\pi)$.

Proof: It suffices to show that $\mathrm{pr}(\Phi_\pi) \ge m_1$. Fix a unit vector $u \in H_1$ and let $M = \mathbb{C}^{m_1}\otimes u$. Then for any $x = \mathbf{a}\otimes u$, we can write the rank-one operator $x\otimes x$ in the matrix form

$$x\otimes x = [a_i x\otimes a_j x]_{m_1\times m_1},$$

where $\mathbf{a} = (a_1,\ldots,a_{m_1})$. Thus $\Phi_\pi(x\otimes x) = [\Phi_{\pi_1}(a_i u\otimes a_j u)]_{m_1\times m_1}$. Since π_1 is irreducible, we know that $\Phi_{\pi_1}(T) = \frac{1}{n_1}\mathrm{tr}(T)I_{H_1}$, where $n_1 = \dim H_1$. Therefore we get that

$$\Phi_\pi(x\otimes x) = [\Phi_{\pi_1}(a_i u\otimes a_j u)]_{m_1\times m_1} = [\frac{1}{n_1}a_i\bar{a}_j I_{H_1}]_{m_1\times m_1}.$$

Now, if $\Phi_\pi(x\otimes x) = \Phi_\pi(y\otimes y)$ for two vectors $x = \mathbf{a}\otimes u, y = \mathbf{b}\otimes u \in M$, then we have $a_i\bar{a}_j = b_i\bar{b}_j$ for all $i, j = 1,\ldots,m$, which implies that $x\otimes x = y\otimes y$. Therefore $\mathrm{pr}(\Phi_\pi) \ge m_1$. □

PROPOSITION 5.1. $\mathrm{pr}(\Phi_\pi) = 1$ *if either (i) π is irreducible or (ii) $\pi = \pi_1\oplus\pi_2$ such that π_1 and π_2 are inequivalent representations on one-dimensional Hilbert spaces.*

Proof: (i) follows from the fact that $\Phi_\pi(x\otimes x) = \Phi_\pi(x\otimes x)$ whenever $\|x\| = \|y\|$. Thus any subspace of dimension greater than 1 cannot be phase retrievable for Φ.

For (ii), it is sufficient to point out that Φ_π is not pure state injective on $H = H_1\oplus H_2$. Pick two unit vectors $x_1 \in H_1, x_2 \in H_2$. Let $x = x_1\oplus x_2$ and $y = x_1\oplus(-x_2)$. Then $\Phi_\pi(x\otimes x) = I_{H_1}\otimes I_{H_2} = \Phi_\pi(y\otimes y)$. However, $x\otimes x \ne y\otimes y$. Thus Φ_π is not pure state injective on H. □

Our goal is to get a reasonable estimate for $\mathrm{pr}(\Phi_\pi)$. For this purpose we present the following characterization of phase retrievable subspaces for representations of multiplicity one, i.e. $m_1 = \cdots = m_d = 1$.

PROPOSITION 5.2. *Let $\pi = \pi_1\oplus\cdots\oplus\pi_d$ be a unitary representation of G acting on $H = H_1\oplus\cdots\oplus H_d$ such that π_i and π_j are inequivalent irreducible representations for all $i \ne j$, and let M be a k-dimensional subspace of H. Then the following are equivalent:*

(i) *M is phase retrievable for Φ_π,*
(ii) *$M=$ range(T) for some linear map $T=(T_1,\dots,T_d):\mathbb{C}^k\to H$ such that $\{T_i^*T_i\}_{i=1}^d$ does phase retrieval for $\mathbb{C}^k$, where $T\xi=T_1\xi\oplus\cdots\oplus T_d\xi$ for all $\xi\in\mathbb{C}^k$.*

Proof: (i) $\Rightarrow$ (ii): Let P_i be the orthogonal projection from H to H_i for $i=1,\dots,d$, and $U:\mathbb{C}^k\to M$ be a unitary map. Define $T_i=P_iU$ and $T=(T_1,\dots,T_d)$. Then

$$T\xi=T_1U\xi\oplus\cdots\oplus T_d\xi=P_1U\xi\oplus\cdots\oplus P_dU\xi=(P_1\oplus\cdots\oplus P_d)U\xi=U\xi.$$

Thus range$(T)=M$. Suppose that $\xi,\eta\in\mathbb{C}^k$ such that

$$\langle\xi\otimes\xi,T_i^*T_i\rangle=\langle\eta\otimes\eta,T_i^*T_i\rangle,\quad\text{i.e.}\quad\|T_i\xi\|^2=\|T_i\eta\|^2$$

for every $i\in[d]$. Since $\pi_1,\dots,\pi_d$ are inequivalent irreducible representations we get that

$$\Phi_{\pi_i,\pi_j}(T_i\xi\otimes T_j\xi)=0$$

if $i\neq j$ and $\Phi_{\pi_i}(T_i\xi\otimes T_i\xi)=\frac{1}{\dim H_i}\|T_i\xi\|^2I_{H_i}$. Thus we get

$$\Phi_\pi(T\xi\otimes T\xi)=[\Phi_{\pi_i,\pi_j}(T_i\xi\otimes T_j\xi)]_{d\times d}=[\Phi_{\pi_i,\pi_j}(T_i\eta\otimes T_j\eta)]_{d\times d}=\Phi_\pi(T\eta\otimes T\eta).$$

Since $T\xi,T\eta\in M$ and Φ_π is pure state injective on M, we get that $T\xi\otimes T\xi=T\eta\otimes T\eta$, which implies that $\xi\otimes\xi=\eta\otimes\eta$. Therefore $\{T_i^*T_i\}_{i=1}^d$ does phase retrieval for $\mathbb{C}^k$.

(ii) $\Rightarrow$ (i): Let $x=T\xi,y=T\eta\in M$ be such that $\Phi_\pi(x\otimes x)=\Phi_\pi(y\otimes y)$. Then we get $\Phi_{\pi_i,\pi_j}(T_i\xi\otimes T_j\xi)=\Phi_{\pi_i,\pi_j}(T_i\eta\otimes T_j\eta)$ for all $i,j\in[d]$, which implies that

$$\|T_i\xi\|^2=\|T_j\eta\|^2,\quad\text{i.e.}\quad\langle x,T_i^*T_ix\rangle=\langle y,T_i^*T_iy\rangle$$

for every $i\in[d]$. Since $\{T_i^*T_i\}_{i=1}^d$ does phase retrieval for $\mathbb{C}^k$, we get that $\xi\otimes\xi=\eta\otimes\eta$ which in turn implies that $x\otimes x=y\otimes y$. Therefore M is phase retrievable for Φ_π. □

COROLLARY 5.1. *Let $\pi=\pi_1\oplus\cdots\oplus\pi_d$ be a unitary representation of G acting on $H=H_1\oplus\cdots\oplus H_d$ such that π_i and π_j are inequivalent irreducible representtaions for all $i\neq j$. Then* $\mathrm{pr}(\Phi_\pi)\geq\lfloor\frac{d}{4}+1\rfloor$.

Proof: Let $k=\lfloor\frac{d}{4}+1\rfloor$. Then $d\geq 4k-4$, and hence by Proposition 2.1 there exists a phase retrievable frame $\{\xi_i\}_{i=1}^d$ for $\mathbb{C}^k$. Since $\{S\xi_i\}_{i=1}^d$ is also a phase retrievable frame for any invertible matrix $S\in M_{k\times k}(\mathbb{C})$, we can assume that $\xi_i=e_i$ for $i\in[k]$, where $\{e_1,\dots,e_k\}$ is the canonical orthonormal basis for $\mathbb{C}^k$. Pick unit vectors $x_i\in H_i$ for $i\in[d]$, and let $T_i=x_i\otimes\xi_i:\mathbb{C}^k\to H_i$ be the rank-one operator defined by $T_i\xi=\langle\xi,\xi_i\rangle x_i$ $(\forall\xi\in\mathbb{C}^k)$. We claim that $T=(T_1,\dots,T_d):\mathbb{C}^k\to H$ is a rank-k linear operator. Clearly it is enough to show that $Te_1,\dots,Te_k$ are linearly independent. Suppose that $\sum_{i=1}^k c_iTe_i=0$ for some scalars $c_i\in\mathbb{C}$. Note that

$$\begin{aligned}\sum_{i=1}^k c_iTe_i&=\sum_{i=1}^k c_i\langle e_i,\xi_1\rangle x_1\oplus\cdots\oplus\sum_{i=1}^k c_i\langle e_i,\xi_d\rangle x_d\\&=c_1x_1\oplus\cdots\oplus c_kx_k\oplus\sum_{i=1}^k c_i\langle e_i,\xi_{k+1}\rangle x_{k+1}\cdots\oplus\sum_{i=1}^k c_i\langle e_i,\xi_d\rangle x_d.\end{aligned}$$

Thus we get $c_1 = \cdots = c_k = 0$, and hence $Te_1, \ldots, Te_k$ are linearly independent. Now let $M = \mathrm{range}(T)$. Then M is a k-dimensional subspace of H. Since $T_i^*T_i = \xi_i \otimes \xi_i$ and $\{\xi_i\}_{i=1}^d$ is a phase retrievable frame for $\mathbb{C}^k$, we immediately get from Proposition 5.2 that M is phase retrievable for Φ_π, and therefore $\mathrm{pr}(\Phi_\pi) \geq k \geq \lfloor \frac{d}{4} + 1 \rfloor$. □

Since it is easy to see by definition that $\mathrm{pr}(\Phi_\pi) \geq \mathrm{pr}(\Phi_\sigma)$ if σ is a subrepresentation of π, we get the following lower bound of $\mathrm{pr}(\Phi_\pi)$ from Lemma 5.2 and Corollary 5.1.

Theorem 5.1. *Let $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ be a unitary representation of G such that π_i and π_j are inequivalent irreducible representations for all $i \neq j$. Then*

$$\mathrm{pr}(\Phi_\pi) \geq \max\{\beta(\Phi_\pi), \lfloor \frac{d}{4} + 1 \rfloor\}.$$

Recall that $\mathcal{I}_k$ is the smallest integer such that there is a phase retrievable frame of $\mathcal{I}_k$ vectors for $\mathbb{C}^k$. Now consider the case when $\pi = \pi_1 \oplus \cdots \oplus \pi_d$ such that π_i and π_j are inequivalent one-dimensional irreducible representations for all $i \neq j$. We claim that if $\mathcal{I}_k \leq d < \mathcal{I}_{k+1}$, then $\mathrm{pr}(\Phi_\pi) = k = \max\{\beta(\Phi_\pi), k\}$ (Note $\beta(\Phi_\pi) = 1$ in this case).

Indeed, by replacing d with $\mathcal{I}_k$ in the proof of Corollary 5.1, we get $\mathrm{pr}(\Phi_\pi) \geq k$. Therefore we only need to show that $\mathrm{pr}(\Phi_\pi) \leq k$. Let M be an L-dimensional subspace of H such that Φ_π is pure state injective on M. Then by Proposition 5.2, there exists a linear operator $T = (T_1, \ldots, T_d) : \mathbb{C}^L \to H$ such that $\mathrm{range}(T) = M$ and $\{T_i^*T_i\}_{i=1}^d$ does phase retrieval for $\mathbb{C}^L$. Since H_i is one-dimensional, we know that T_i is rank-one operator. Write $T_i = x_i \otimes \xi_i$ for some $x_i \in H_i$ and $\xi_i \in \mathbb{C}^L$. Then $T_i^*T_i = \|x_i\|^2\xi_i \otimes \xi_i$. This implies that $\{\xi_i\}_{i=1}^d$ is a phase retrievable frame for $\mathbb{C}^L$, and thus $d \geq \mathcal{I}_L$. If $L \geq k+1$, then $\mathcal{I}_L \geq \mathcal{I}_{k+1}$ and this would have implied that $d \geq \mathcal{I}_{k+1}$, which is a contradiction. Thus $L \leq k$, which implies that $\mathrm{pr}(\Phi_\pi) \leq k$. Therefore $\mathrm{pr}(\Phi_\pi) = k = \max\{\beta(\Phi_\pi), k\}$ for this case. We make the following conjecture.

Conjecture. *Let $\pi = m_1\pi_1 \oplus \cdots \oplus m_d\pi_d$ be a unitary representation of G such that π_i and π_j are inequivalent irreducible representations for all $i \neq j$ and $\mathcal{I}_k \leq d < \mathcal{I}_{k+1}$. Then* $\mathrm{pr}(\Phi_\pi) = \max\{\beta(\Phi_\pi), k\}$.

Acknowledgements

The authors thank the referees very much for several constructive comments and suggestions that helped improve the presentation of this paper. Deguang Han acknowledges the partial support by the National Science Foundation grant DMS-2105038.

REFERENCES

[1] E. Balan, D. Dutkay, D. Han, D. Larson and F. Luef: *J. Fourier Anal. Appl.* **26**, 1 (2020).
[2] C. Bennett, D. DiVincenzo, J. Smolin and W. Wootters: *Phys. Rev. A,* **54**, 3824(1996).
[3] S. Braunstein, D. Kribs, M. Patra: *IEEE International Symposium on Information Theory*, 104(2011).

[4] J. Chen, S. Grogan, N. Johnston, C. Kwong and S. Plosker: *Phys. Rev. A* **94**, 042313 (2016).
[5] D. Kribs: *Proc. Edin. Math. Soc.* **46**, 421 (2003).
[6] D. Kribs: *Lin. Alg. Appl.* **400**, 147 (2005).
[7] D. Kribs, C. Mintah, M. Nathanson, R. Pereira: *J. Math. Phys.,* **60**, 032202 (2019).
[8] M. Girard and J. Levick: *Lin. Alg. Appl.* **615**, 207(2021).
[9] E. Chang, J. Kim, H. Kwak, H. Lee and S. Youn: *Rev. Math. Phys.* **34**, 2250021 (2022).
[10] M. D. Choi: *Lin. Alg. Appl.* **10**, 285(1975).
[11] D. DiVincenzo, D. Leung, and B. Terhal: *IEEE Trans. Inf. Theory* **48**, 580(2002).
[12] M. D. Choi: *Lin. Alg. Appl.* **12**, 95(1975).
[13] G.M. d'Ariano, P. Perinotti, and M. F. Sacchi: *J. Opt., B Quantum and semiclass. opt.* **6**, S487(2004).
[14] N. Datta, M. Fukuda and A.S. Holevo: *Quantum Inf. Process* **5**, 79(2006).
[15] R. Duan, S. Severini, and A. Winter: *IEEE Trans. Info. Theory* **59**, 1164(2013).
[16] D. Dutkay, D. Han and D. Larson: *J. Funct. Anal.* **257**, 1133(2009).
[17] V. Gupta, P. Mandayam and V.S. Sunder, *The Functional Analysis of Quantum Information Theory*, A Collection of Notes Based on Lectures by Gilles Pisier, K. R. Parthasarathy, Vern Paulsen and Andreas Winter, Lecture Notes in Physics 902, Springer, 2015.
[18] M. Gschwendtner, A. Bluhm and A. Winter: *Quantum* **5**, 488(2021).
[19] E. Haapasalo: *Quantum Stud. Math.* **8**, 251(2021).
[20] E. Haapasalo: *Annales Henri Poincaré* **20**, 3163(2019).
[21] E. Haapasalo and J. Pellonpää: *J. Phys. A Math. Theor.* **54**, 155304 (2021).
[22] D. Han, T. Juste, Y. Li and W. Sun: *J. Fourier Anal. Appl.* **25**, 3154 (2019).
[23] D. Han and T. Juste: *Lin. Alg. Appl.* **579**, 148(2019).
[24] D. Han and D. Larson: *Memoirs Amer. Math. Soc.* **697** (2000).
[25] D. Han and D. Larson: *Bull. London Math. Soc.* **40**, 685(2008).
[26] T. Heinosaari and T. Miyadera: *J. Phys. A Math. Theor.* **50**, 135302 (2017).
[27] A. Jamiołkowski: *Rep. Math. Phys.* **3**, 275(1972).
[28] K. Liu, C. Cheng and D. Han: *Lin. Alg. Appl.* **668**, 28(2023).
[29] K. Liu and D. Han: Phase retrievability of frames and quantum channels, preprint 2023.
[30] M. Mozrzymas, M. Studzin'ski and N. Datta: *J. Math. Phys.* **58**, 052204 (2017).
[31] M. A. Naimark and A. I. Stern: *Theory of Group Representations*, Springer-Verlag, New York, 1982.
[32] M. Nuwairan: *SU(2)-Irreducibly Covariant Quantum Channels and Some Applications*, Ph. D dissertation, University of Ottawa, 2015.
[33] Y. Ouyang: *Quantum Inf. Comput.* **14**, 917(2014).
[34] J. Renes, R. Blume-Kohout, A. J. Scott and C. Caves: *J. Math. Phys.* **45**, 2171(2004).
[35] S. Singh, N. Datta and I. Nechita: Ergodic theory of diagonal orthogonal covariant quantum channels, 2022 (arXiv:2206.01145).
[36] R. Tumulka: *POVM (Positive Operator Value Measure)*, Book chapter: Compendium of Quantum Physics: 480 (2009).
[37] K. Vollbrecht and R. Werner: *Phys. Rev. A* **64**, 062307 (2001).