On the mixed-unitary rank of quantum channels

Mark Girard[1,2]   Debbie Leung[1,3,4]   Jeremy Levick[1,5]   Chi-Kwong Li[1,6]

Vern Paulsen[1,7]   Yiu Tung Poon[8,9]   John Watrous[1,2,10]

[1]*Institute for Quantum Computing, University of Waterloo*
[2]*School of Computer Science, University of Waterloo*
[3]*Department of Combinatorics & Optimization, University of Waterloo*
[4]*Perimeter Institute for Theoretical Physics, Waterloo*
[5]*Department of Mathematics & Statistics, University of Guelph*
[6]*Department of Mathematics, College of William and Mary*
[7]*Department of Pure Mathematics, University of Waterloo*
[8]*Department of Mathematics, Iowa State University*
[9]*Center for Quantum Computing, Peng Cheng Laboratory*
[10]*Canadian Institute for Advanced Research, Toronto*

March 31, 2020

Abstract

In the theory of quantum information, the *mixed-unitary quantum channels*, for any positive integer dimension n, are those linear maps that can be expressed as a convex combination of conjugations by $n \times n$ complex unitary matrices. We consider the *mixed-unitary rank* of any such channel, which is the minimum number of distinct unitary conjugations required for an expression of this form. We identify several new relationships between the mixed-unitary rank N and the Choi rank r of mixed-unitary channels, the Choi rank being equal to the minimum number of nonzero terms required for a Kraus representation of that channel. Most notably, we prove that the inequality $N \leq r^2 - r + 1$ is satisfied for every mixed-unitary channel (as is the equality $N = 2$ when $r = 2$), and we exhibit the first known examples of mixed-unitary channels for which $N > r$. Specifically, we prove that there exist mixed-unitary channels having Choi rank $d + 1$ and mixed-unitary rank $2d$ for infinitely many positive integers d, including every prime power d. We also examine the mixed-unitary ranks of the mixed-unitary Werner–Holevo channels.

1. Introduction

The theory of quantum information posits that discrete-time changes in quantum-mechanical systems that store quantum information are represented by *quantum channels* (or just *channels* for short), which are completely positive and trace-preserving linear maps from square matrices to square matrices having complex number entries. Hereafter we shall write $\mathcal{M}_{n,m}$ to denote the space of $n \times m$ complex matrices, and we also write $\mathcal{M}_n = \mathcal{M}_{n,n}$.

One standard way of describing any given channel $\Phi : \mathcal{M}_n \to \mathcal{M}_m$ is to choose a positive integer r along with matrices $A_1, \ldots, A_r \in M_{m,n}$, and then take

$$\Phi(X) = \sum_{k=1}^{r} A_k X A_k^* \tag{1}$$

for all $X \in \mathcal{M}_n$. Such a description is known as a *Kraus representation* of Φ, and the existence of such a description is equivalent to Φ being completely positive [Cho75]. A map Φ described in this way preserves trace if and only if

$$\sum_{k=1}^{r} A_k^* A_k = \mathbb{1}_n, \tag{2}$$

where $\mathbb{1}_n \in \mathcal{M}_n$ is the identity matrix. The minimum value of r for which such a description exists is called the *Choi rank* of Φ, this number being so-named because it is equal to the rank of the *Choi representation* (or *Choi matrix*) $J(\Phi)$ associated with Φ:

$$J(\Phi) = \sum_{1 \le j,k \le n} \Phi(E_{j,k}) \otimes E_{j,k}, \tag{3}$$

where $E_{j,k} \in \mathcal{M}_n$ denotes the matrix having a 1 in entry (j,k) and 0 in all other entries. As the Choi representation is an $nm \times nm$ matrix, it follows that the Choi rank of Φ is always at most nm.

In this paper we consider a restricted class of channels called mixed-unitary channels. Writing $\mathcal{U}_n$ to denote the set of all $n \times n$ complex unitary matrices, we say that a channel $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ is a *unitary channel* if there exists a unitary matrix $U \in \mathcal{U}_n$ for which

$$\Phi(X) = UXU^* \tag{4}$$

for all $X \in \mathcal{M}_n$, and we say that a channel is a *mixed-unitary channel* if it can be expressed as a convex combination of unitary channels. That is, a channel $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ is mixed unitary if and only if there exists a positive integer N, a probability vector $(p_1, \ldots, p_N)$, and unitary matrices $U_1, \ldots, U_N \in \mathcal{U}_n$ such that

$$\Phi(X) = \sum_{k=1}^{N} p_k U_k X U_k^* \tag{5}$$

for all $X \in \mathcal{M}_n$. We observe that the set of all mixed-unitary channels is compact, as it is the convex hull of a compact set (the set of unitary channels) in a finite-dimensional space. Thus, by Carathéodory's theorem, every element in the closed convex hull of the set of unitary channels can be represented as a (finite) convex combination of unitary channels.

Various properties of mixed-unitary channels may be observed. Of course, with respect to the general description of channels above, mixed-unitary channels are channels for which $m = n$, and it is evident that every mixed-unitary channel $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ is *unital*, meaning that $\Phi(\mathbb{1}_n) = \mathbb{1}_n$. It is known that in the case $n = 2$, a channel is mixed unitary if and only if it is unital, but when $n \ge 3$ there exist channels $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ that are unital but not mixed unitary [Tre86, LS93].

The importance of mixed-unitary channels in quantum information theory is multifarious. Many natural examples of noisy quantum channels (including the so-called *dephasing* and *depolarizing* channels) are mixed unitary. The general form of a mixed-unitary channel—which can be described as a classical source of randomness selecting a unitary transformation to be applied

to a system—is simple and intuitive, and arises naturally in algorithmic and cryptographic settings. For example, the most standard forms of encryption and decryption of quantum information using a private key induce mixed-unitary channels on the data from the viewpoint of an eavesdropper [AMTdW00, HLSW04]. *Quantum expanders, twirling operations,* and *unitary t-designs* are specific types of mixed-unitary channels that have been studied extensively in quantum information and computation [BASTS08, BDSW96, DLT01, DCEL09]. Mixed-unitary channels are also known to correspond precisely to those channels for which an ideal form of environment-assisted error correction is possible [GW03]. Despite the fact that mixed-unitary channels have a simple form, they do nevertheless inherit many interesting properties of general channels [Ros08].

Mixed-unitary channels also have important uses, as an analytic tool, in quantum information theory. For example, *majorization* for Hermitian matrices [AU82] is typically defined in terms of mixed-unitary channels: a Hermitian matrix H is said to majorize a Hermitian matrix K if there exists a mixed-unitary channel Φ such that $\Phi(H) = K$. This notion has found many applications in quantum information, perhaps most notably in Nielsen's theorem [Nie99], which provides a perfect characterization of the bipartite pure state transformations that can be realized through local quantum operations and classical communication. Another example is that the monotonicity of quantum relative entropy under the action of mixed-unitary channels, which follows directly from the joint convexity of quantum relative entropy, offers a convenient stepping stone to monotonicity for all channels. (Recent proofs of the monotonicity of quantum relative entropy under the action of all channels, and indeed all positive and trace-preserving maps [MHR17], do however offer an alternative path.)

Mixed-unitary channels are also interesting mathematical objects in their own right, and have inspired fruitful lines of research. For example, the *asymptotic quantum Birkhoff conjecture* [SVW05], which was eventually refuted [HM11], was concerned with the approximation of tensor powers of unital channels by mixed-unitary channels. Through the *channel–state correspondence*, which essentially identifies a channel with the state obtained by normalizing its Choi representation, mixed-unitary channels also offer an interesting twist on bipartite separability. That is, whereas a separable state is a convex mixture of *pure product states*, the states corresponding to mixed-unitary channels are convex mixtures of *maximally entangled states*. As it turns out, the two sets of states share some important common properties, including the fact that they have a nonempty interior [ŻHSL98, GB02, Wat09] and have NP-hard membership testing problems [Gur03, Ioa07, Gha10, LW19]. Additional properties of mixed-unitary channels can be found in [AS08] and [MW09].

In this paper we focus on the minimum number N, over all possible expressions of the form (5) that exist for a given mixed-unitary channel Φ, and we shall refer to this number as the *mixed-unitary rank* of Φ. It is immediate that $N \geq r$; the mixed-unitary rank is always at least the Choi rank. Buscemi [Bus06] proved the upper bound $N \leq r^2$, which was the strongest bound known prior to our work.[1] With respect to the lower bound $N \geq r$, to our knowledge no examples of mixed-unitary channels for which $N > r$ have previously been exhibited. The main contributions of our paper are as follows.

1. We prove that the mixed-unitary rank N of every mixed-unitary channel $\Phi : \mathcal{M}_n \to \mathcal{M}_n$

---

[1]See also Theorem 4.10 and Corollary 4.11 in [Wat18], which provides an alternative way to prove Buscemi's bound. We note, in addition, that one can obtain a very slight improvement to Buscemi's bound in the specific case $r = n^2$ by observing that the bound $N \leq n^4 - 2n^2 + 2$ follows in a straightforward fashion from Carathéodory's theorem, as is explained in Proposition 4.9 of [Wat18].

having Choi rank r satisfies

$$N \leq r^2 - s + 1, \tag{6}$$

where $s = \dim(\mathcal{S}_\Phi)$ is the dimension of the operator system associated with Φ. This operator system is given by

$$\mathcal{S}_\Phi = \mathrm{span}\{A_j^* A_k : 1 \leq j, k \leq r\}, \tag{7}$$

for any expression of Φ taking the form (1). By examining relations between the dimension of the operator system of a mixed-unitary channel and its Choi rank, we conclude that

$$N \leq r^2 - r + 1 \tag{8}$$

for all mixed-unitary channels. Furthermore, we prove that $N = r$ if either $r \leq 2$ or $s \leq 3$, and that $N \leq 6$ in the case when $r = 3$.

2. We provide a construction through which one may obtain examples of mixed-unitary channels having mixed-unitary ranks strictly larger than their Choi ranks. Specifically, the construction takes these channels to be the *direct sum* of a unitary channel with a mixed-unitary channel that can be expressed uniquely as a nontrivial convex combination of unitary channels. Through this construction we exhibit examples of mixed-unitary channels of the form $\Phi : \mathcal{M}_{d+1} \to \mathcal{M}_{d+1}$ having Choi rank $d + 1$ and mixed-unitary rank $2d$ for every odd prime d, as well as mixed-unitary Schur channels of the form $\Phi : \mathcal{M}_{d^2+1} \to \mathcal{M}_{d^2+1}$ having Choi rank $d + 1$ and mixed-unitary rank $2d$ for every positive integer d for which $d + 1$ mutually unbiased bases for the space $\mathbb{C}^d$ exist (which includes every prime power d).

3. We observe that the mixed-unitary rank is not multiplicative with respect to tensor products. In particular, there exist mixed-unitary channels Φ and Ψ having mixed-unitary ranks 4 and 2, respectively, such that the mixed-unitary rank of $\Phi \otimes \Psi$ is 6.

4. Finally, we examine the mixed-unitary ranks of the Werner–Holevo channels, which are an important class of channels in quantum information theory defined for every dimension $n \geq 2$ by the formulas

$$\Phi_0(X) = \frac{\mathrm{Tr}(X)\mathbb{1}_n + X}{n+1} \qquad \text{and} \qquad \Phi_1(X) = \frac{\mathrm{Tr}(X)\mathbb{1}_n - X}{n-1} \tag{9}$$

for all $X \in \mathcal{M}_n$. The channel Φ_0 is mixed unitary for all such n, while Φ_1 is mixed-unitary if and only if n is even. We prove the following facts concerning the mixed-unitary ranks of these channels.

- For all even $n \geq 2$, the Choi rank and the mixed-unitary rank are in agreement for both Φ_0 and Φ_1: we have $N = r = \binom{n+1}{2}$ for Φ_0 and $N = r = \binom{n}{2}$ for Φ_1.
- The mixed-unitary rank of Φ_0 in every odd dimension n is at most $n(n+3)/2$, and the mixed-unitary rank of Φ_0 for the case $n = 3$ is $N = r = 6$.

Numerical evidence suggests that the mixed-unitary rank of Φ_0 for a few other small odd values of n satisfies $N = r = \binom{n+1}{2}$, but we leave open the problem of determining whether or not this formula holds in general.

4

2. Preliminaries

In this section we summarize known facts and results concerning quantum channels, including a few results specific to mixed-unitary channels, that will be used later in the paper. Further information on quantum channels, and the role they play in the theory of quantum information, can be found in texts on the subject, including [NC00, Wil17, Wat18].

Linear algebra notations and conventions

Given any matrix $A \in \mathcal{M}_{m,n}$, we denote by A^T, $\overline{A}$, and A^* the transpose, entry-wise conjugate, and adjoint (or conjugate transpose) of A, respectively. A square matrix $H \in \mathcal{M}_n$ is *Hermitian* if $H = H^*$, a square matrix $U \in \mathcal{M}_n$ is *unitary* if $U^*U = UU^* = \mathbb{1}_n$, and a matrix $A \in \mathcal{M}_{m,n}$ is an *isometry* if $A^*A = \mathbb{1}_n$. This last condition requires that $m \geq n$, and in the case $m = n$ the condition that A is an isometry is equivalent to A being unitary.

The vectorization mapping $\mathrm{vec} : \mathcal{M}_{m,n} \to \mathbb{C}^{nm}$ converts a given matrix to a column vector by transposing its rows into columns and stacking them on top of one another from top to bottom. In more precise terms, this mapping is defined as

$$\mathrm{vec}(A) = \sum_{j=1}^{m}\sum_{k=1}^{n} A(j,k)\, e_j \otimes e_k \tag{10}$$

for every $A \in \mathcal{M}_{m,n}$, where $e_j \in \mathbb{C}^m$ and $e_k \in \mathbb{C}^n$ denote the elementary unit vectors having a 1 in entry j or k, respectively, and 0 in all other entries. We define the inner product of two matrices $A, B \in \mathcal{M}_{m,n}$ as $\langle A, B \rangle = \mathrm{Tr}(A^*B)$, which is equivalent to the ordinary inner product (conjugate linear in the first argument) of A and B viewed as vectors: $\langle A, B \rangle = \langle \mathrm{vec}(A), \mathrm{vec}(B) \rangle$.

Finally, the adjoint of a linear map $\Phi : \mathcal{M}_n \to \mathcal{M}_m$ is the unique linear map $\Phi^* : \mathcal{M}_m \to \mathcal{M}_n$ that satisfies $\langle Y, \Phi(X) \rangle = \langle \Phi^*(Y), X \rangle$ for all $X \in \mathcal{M}_n$ and $Y \in \mathcal{M}_m$. The condition that Φ is *trace-preserving* is equivalent to Φ^* being unital.

Choi and Kraus representations of channels

We have already defined the Choi representation and the notion of a Kraus representation of a completely positive linear map $\Phi : \mathcal{M}_n \to \mathcal{M}_m$ in the introduction, but it will be helpful to note two additional facts concerning them. First, if Φ is a completely positive map having the Kraus representation (1), then its Choi representation is given by

$$J(\Phi) = \sum_{k=1}^{r} \mathrm{vec}(A_k)\, \mathrm{vec}(A_k)^*. \tag{11}$$

Second, although Kraus representations are not unique, any two Kraus representations of a given completely positive map are related in the following way: if $\Phi : \mathcal{M}_n \to \mathcal{M}_m$ has the Kraus representation (1), and

$$\Phi(X) = \sum_{k=1}^{N} B_k X B_k^* \tag{12}$$

is a Kraus representation of Φ for which $N \geq r$, then there must exist an isometry $V \in \mathcal{M}_{N,r}$ such that

$$B_k = \sum_{j=1}^{r} V(k,j) A_j \tag{13}$$

for every $k \in \{1, \ldots, N\}$.

Complementary channels

Suppose that $\Phi : \mathcal{M}_n \to \mathcal{M}_m$ is a channel (i.e., a completely positive and trace-preserving linear map) having Kraus representation

$$\Phi(X) = \sum_{k=1}^{r} A_k X A_k^*. \tag{14}$$

The linear map $\Psi : \mathcal{M}_n \to \mathcal{M}_r$ defined by

$$\Psi(X) = \sum_{j,k=1}^{r} \langle A_k^* A_j, X \rangle E_{j,k} \tag{15}$$

for all $X \in \mathcal{M}_n$ is then also necessarily a channel, and is said to be *complementary* to Φ. (The notion of a complementary channel is more commonly defined through the Stinespring representation of channels, which we have no need to discuss, but the definitions are equivalent.)

If it is the case that $r = \operatorname{rank}(J(\Phi))$ and $\Psi : \mathcal{M}_n \to \mathcal{M}_r$ is complementary to Φ, then any other given channel $\Xi : \mathcal{M}_n \to \mathcal{M}_N$ is also complementary to Φ if and only if there exists an isometry $V \in \mathcal{M}_{N,r}$ such that $\Xi(X) = V\Psi(X)V^*$ for every $X \in \mathcal{M}_n$.

The operator system of a channel

Let n be a positive integer. A linear subspace $\mathcal{S} \subseteq \mathcal{M}_n$ is an *operator system* if $\mathbb{1}_n \in \mathcal{S}$ and if $A^* \in \mathcal{S}$ for each $A \in \mathcal{S}$. Every operator system is spanned by its Hermitian elements. In particular, if $s = \dim(\mathcal{S})$ is the dimension of this subspace, there exist Hermitian matrices $H_1, \ldots, H_{s-1}$ such that

$$\mathcal{S} = \operatorname{span}\{\mathbb{1}_n, H_1, \ldots, H_{s-1}\}. \tag{16}$$

Further information on the topic of operator systems can be found in [Pau86], [Con99], and [Pau03].

An operator system $\mathcal{S}_\Phi$ is associated with every channel $\Phi : \mathcal{M}_n \to \mathcal{M}_m$ in the following manner:

$$\mathcal{S}_\Phi = \{A : \operatorname{vec}(A) \in \operatorname{im}(J(\Phi^*\Phi))\}. \tag{17}$$

Equivalently, given any Kraus representation

$$\Phi(X) = \sum_{k=1}^{r} A_k X A_k^* \tag{18}$$

of a channel Φ, the operator system $\mathcal{S}_\Phi$ may be expressed as

$$\mathcal{S}_\Phi = \operatorname{span}\{A_k^* A_j : 1 \leq j, k \leq r\}, \tag{19}$$

which is evident from the observation that

$$J(\Phi^*\Phi) = \sum_{j,k=1}^{r} \operatorname{vec}(A_k^* A_j) \operatorname{vec}(A_k^* A_j)^*. \tag{20}$$

The fact that $\mathcal{S}_\Phi$ is closed under adjoints is immediate, while the condition $\mathbb{1}_n \in \mathcal{S}_\Phi$ follows from the assumption that Φ preserves trace, and therefore satisfies

$$\sum_{k=1}^{r} A_k^* A_k = \mathbb{1}_n. \tag{21}$$

The operator system $\mathcal{S}_\Phi$ of the channel Φ has also been referred to as the *non-commutative graph* of Φ in the context of quantum zero-error information theory [DSW13].

If $\Phi : \mathcal{M}_n \to \mathcal{M}_m$ is a channel with Choi rank r, then the dimension $s = \dim(S_\Phi)$ of the operator system of Φ necessarily satisfies $s \leq r^2$. One also has that $s = r^2$ if and only if Φ is an extreme point in the convex set of all channels from $\mathcal{M}_n$ to $\mathcal{M}_m$ [Cho75]. In addition, if Φ is a mixed-unitary channel with mixed-unitary rank N, it further holds that $s \leq N^2 - N + 1$, as each unitary operator U_k in the Kraus representation (1) satisfies $U_k^* U_k = \mathbb{1}_n$.

Direct sums of channels

Let n and m be positive integers and let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ and $\Psi : \mathcal{M}_m \to \mathcal{M}_m$ be linear mappings. The *direct sum* of the mappings Φ and Ψ is the linear map $\Phi \oplus \Psi : \mathcal{M}_{n+m} \to \mathcal{M}_{n+m}$ defined as

$$(\Phi \oplus \Psi) \begin{pmatrix} X & \cdot \\ \cdot & Y \end{pmatrix} = \begin{pmatrix} \Phi(X) & 0 \\ 0 & \Psi(Y) \end{pmatrix} \tag{22}$$

for every $X \in \mathcal{M}_n$ and $Y \in \mathcal{M}_m$ (where the dots indicate arbitrary matrices of the appropriate size that have no influence on the output of the map). If Φ and Ψ are channels, then $\Phi \oplus \Psi$ is a channel as well. It is always the case that

$$\operatorname{rank}(J(\Phi \oplus \Psi)) = \operatorname{rank}(J(\Phi)) + \operatorname{rank}(J(\Psi)). \tag{23}$$

Using any Kraus representations of Φ and Ψ, we can express $\Phi \oplus \Psi$ as

$$(\Phi \oplus \Psi) \begin{pmatrix} X & \cdot \\ \cdot & Y \end{pmatrix} = \sum_{k=1}^{N} \begin{pmatrix} A_k & 0 \\ 0 & B_k \end{pmatrix} \begin{pmatrix} X & \cdot \\ \cdot & Y \end{pmatrix} \begin{pmatrix} A_k & 0 \\ 0 & B_k \end{pmatrix}^* \tag{24}$$

for some choice of matrices $A_1, \ldots, A_N \in \mathcal{M}_n$ and $B_1, \ldots, B_N \in \mathcal{M}_m$ and for some positive integer N. Furthermore, following the relation between different Kraus representations given by (13) every Kraus representation of $\Phi \oplus \Psi$ must have the form similar to the above.

Unique mixed-unitary decompositions

Let n be a positive integer, let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a mixed-unitary channel, and let N be the mixed-unitary rank of Φ. Let us also introduce the following notation: for two unitary matrices $U, V \in \mathcal{U}_n$, we write $U \sim V$ if there exists a complex number $\alpha \in \mathbb{C}$ with $|\alpha| = 1$ such that $U = \alpha V$. That is, $U \sim V$ if and only if U and V describe the same unitary channel through conjugation. A decomposition

$$\Phi(X) = \sum_{k=1}^{N} p_k U_k X U_k^* \tag{25}$$

of Φ is said to be a *unique mixed-unitary decomposition* for Φ if the following statement is true. For every mixed-unitary decomposition

$$\Phi(X) = \sum_{j=1}^{t} q_j V_j X V_j^* \tag{26}$$

of Φ, there must exist a partition $\{1,\ldots,t\} = T_1 \cup \cdots \cup T_N$ so that these two conditions hold for every $k \in \{1,\ldots,N\}$:

1. $V_j \sim U_k$ for every $j \in T_k$.

2. $p_k = \sum_{j \in T_k} q_j$.

Condition for a channel to be mixed unitary

Finally, we require a characterization of mixed-unitary channels, expressed by the following theorem and corollary. The theorem is based on a characterization of mixed-unitary channels due to Audenaert and Scheel [AS08]; a proof is included below because we require a slight refinement of their characterization.

A square matrix $X \in \mathcal{M}_n$ is said to be *traceless* if $\mathrm{Tr}(X) = 0$ and is said to have *vanishing diagonal* if all of its diagonal entries are equal to 0. We remark that the set of traceless $n \times n$ matrices is equal to the set $\mathbb{1}_n^\perp$.

Theorem 1. *Let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a channel having Choi rank r. For every positive integer $N \geq r$, the following statements are equivalent:*

1. *Φ is mixed unitary with mixed-unitary rank at most N.*

2. *There is a channel $\Psi : \mathcal{M}_n \to \mathcal{M}_N$ complementary to Φ such that $\Psi(X)$ has vanishing diagonal for every traceless matrix X.*

Proof. Suppose first that $\Psi : \mathcal{M}_n \to \mathcal{M}_N$ is a channel complementary to Φ such that $\Psi(X)$ has vanishing diagonal for every traceless matrix X. Let $A_1,\ldots,A_N \in \mathcal{M}_n$ be matrices satisfying

$$\Phi(X) = \sum_{k=1}^{N} A_k X A_k^* \qquad \text{and} \qquad \langle A_k^* A_j, X \rangle E_{j,k} \tag{27}$$

for each $X \in \mathcal{M}_n$. For each index $k \in \{1,\ldots,N\}$, one has that

$$\langle A_k^* A_k, X \rangle = \langle E_{k,k}, \Psi(X) \rangle = 0 \tag{28}$$

for each matrix $X \in \mathbb{1}_n^\perp$, as the diagonal entries of $\Psi(X)$ are equal to zero by assumption for each traceless matrix X. It must therefore hold that $A_k^* A_k \in \mathrm{span}\{\mathbb{1}_n\}$ and thus $A_k = \alpha_k U_k$ for some choice of a complex number α_k and a unitary matrix $U_k \in \mathcal{U}_n$, for every index $k \in \{1,\ldots,N\}$. It follows that

$$\Phi(X) = \sum_{k=1}^{N} A_k X A_k^* = \sum_{k=1}^{N} |\alpha_k|^2 U_k X U_k^* = \sum_{k=1}^{N} p_k U_k X U_k^* \tag{29}$$

for each $X \in \mathcal{M}_n$, where $(p_1,\ldots,p_N)$ is the probability vector defined as $p_k = |\alpha_k|^2$ for each $k \in \{1,\ldots,N\}$, and thus Φ is mixed unitary with mixed-unitary rank at most N.

To prove the reverse implication, suppose that there exist unitary matrices $U_1, \ldots, U_N \in \mathcal{U}_n$ and a probability vector $(p_1, \ldots, p_N)$ satisfying

$$\Phi(X) = \sum_{k=1}^{N} p_k U_k X U_k^* \tag{30}$$

for each $X \in \mathcal{M}_n$, and define a channel $\Psi : \mathcal{M}_n \to \mathcal{M}_N$ complementary to Φ as

$$\Psi(X) = \sum_{j,k=1}^{N} \sqrt{p_j p_k} \langle U_k^* U_j, X \rangle E_{j,k} \tag{31}$$

for each $X \in \mathcal{M}_n$. For each traceless matrix X, one has

$$\langle E_{k,k}, \Psi(X) \rangle = p_k \langle U_k^* U_k, X \rangle = p_k \operatorname{Tr}(X) = 0 \tag{32}$$

for each $k \in \{1, \ldots, N\}$, and therefore the diagonal entries of $\Psi(X)$ are equal to zero. $\square$

Corollary 2. *Let n be a positive integer, let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a channel, let r be the Choi rank of Φ, and let $\Psi : \mathcal{M}_n \to \mathcal{M}_r$ be a channel that is complementary to Φ. For every integer $N \geq r$, the channel Φ is mixed unitary with mixed-unitary rank at most N if and only if there exists an isometry $V \in \mathcal{M}_{N,r}$ such that $V\Psi(X)V^*$ has vanishing diagonal for each traceless matrix X.*

Proof. This follows from Theorem 1 and the observation that another channel $\Xi : \mathcal{M}_n \to \mathcal{M}_N$ is complementary to $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ if and only if there exists an isometry $V \in \mathcal{M}_{N,r}$ satisfying $\Xi(X) = V\Psi(X)V^*$ for each $X \in \mathcal{M}_n$. $\square$

Corollary 2 suggests a useful method for approximating the mixed-unitary rank of a channel. Given a channel $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ with Choi rank r and a candidate integer $N \geq r$ for the mixed-unitary rank of Φ, one can use the following procedure to determine if Φ can be decomposed as a convex combination of N unitary channels:

1. Choose any channel $\Psi : \mathcal{M}_n \to \mathcal{M}_r$ that is complementary to Φ.

2. Define a subspace of matrices $\mathcal{B} \subseteq \mathcal{M}_r$ as $\mathcal{B} = \{\Psi(X) : X \in \mathbb{1}_n^{\perp}\}$ and choose matrices $B_1, \ldots, B_N \in \mathcal{B}$ such that $\mathcal{B} = \operatorname{span}\{B_1, \ldots, B_N\}$.

3. Use numerical methods to search for an isometry $V \in \mathcal{M}_{N,r}$ such that $\langle E_{j,j}, V B_k V^* \rangle = 0$ for each pair of indices $j \in \{1, \ldots, N\}$ and $k \in \{1, \ldots, r\}$.

The last step cannot be performed efficiently (unless $P = NP$), but we have found that this procedure is useful for computing the mixed-unitary ranks of interesting channels for small choices of the dimension n.

3. Upper bounds on mixed-unitary rank

In this section we prove upper bounds on the mixed-unitary rank of mixed-unitary channels. We begin with the following general theorem.

Theorem 3. *Let n be a positive integer, let* $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ *be a mixed-unitary channel having Choi rank r and mixed-unitary rank N, and let* $s = \dim(\mathcal{S}_\Phi)$ *be the dimension of the operator system of* Φ. *It is the case that*

$$N \leq r^2 - s + 1. \tag{33}$$

Proof. Let $A_1, \ldots, A_r \in \mathcal{M}_n$ be matrices offering a Kraus representation of Φ:

$$\Phi(X) = \sum_{k=1}^{r} A_k X A_k^* \tag{34}$$

for all $X \in \mathcal{M}_n$. Also define $\Psi : \mathcal{M}_n \to \mathcal{M}_r$ as

$$\Psi(X) = \sum_{j,k=1}^{r} \langle A_k^* A_j, X \rangle E_{j,k} \tag{35}$$

for all $X \in \mathcal{M}_n$, so that Ψ is a channel complementary to Φ. It is the case that $\text{im}(\Psi^*) = \mathcal{S}_\Phi$ and therefore $s = \dim(\text{im}(\Psi^*))$. By the rank-nullity theorem we have that

$$\dim(\ker(\Psi^*)) + \dim(\text{im}(\Psi^*)) = \dim(\mathcal{M}_r) = r^2, \tag{36}$$

and so the theorem will follow from a demonstration that $N \leq \dim(\ker(\Psi^*)) + 1$. Toward this goal, suppose $U_1, \ldots, U_N \in \mathcal{U}_n$ are unitary matrices and $(p_1, \ldots, p_N)$ is a probability vector such that

$$\Phi(X) = \sum_{k=1}^{N} p_k U_k X U_k^* \tag{37}$$

for each $X \in \mathcal{M}_n$, and let us observe that each p_k must be nonzero by the assumption that N is the mixed-unitary rank of Φ.

At this point we have two Kraus representations of Φ, which must be related as was discussed in the previous section: there must exist an isometry $V \in \mathcal{M}_{N,r}$ such that

$$\sqrt{p_k} U_k = \sum_{j=1}^{r} V(k,j) A_j \tag{38}$$

for every $k \in \{1, \ldots, N\}$. Define $u_k \in \mathbb{C}^r$ as $u_k = V^{\mathsf{T}} e_k$ for each $k \in \{1, \ldots, N\}$ and define a matrix $A \in \mathcal{M}_{n^2, r}$ as

$$A = \sum_{j=1}^{r} \text{vec}(A_j) e_j^*. \tag{39}$$

Observe that

$$\sqrt{p_k} \, \text{vec}(U_k) = AV^{\mathsf{T}} e_k = Au_k \tag{40}$$

for each $k \in \{1, \ldots, N\}$.

Next, consider the collection

$$\{\text{vec}(U_1) \, \text{vec}(U_1)^*, \, \ldots, \, \text{vec}(U_N) \, \text{vec}(U_N)^*\}, \tag{41}$$

which we claim must be linearly independent. To verify this claim, suppose to the contrary that $\alpha_1, \ldots, \alpha_N \in \mathbb{C}$ are not all zero and satisfy

$$\alpha_1 \, \text{vec}(U_1) \, \text{vec}(U_1)^* + \cdots + \alpha_N \, \text{vec}(U_N) \, \text{vec}(U_N)^* = 0. \tag{42}$$

10

By taking the trace of both sides of this equation, we find that $\alpha_1 + \cdots + \alpha_N = 0$, and therefore

$$\sum_{k=2}^{N} \alpha_k \left(\text{vec}(U_k) \text{vec}(U_k)^* - \text{vec}(U_1) \text{vec}(U_1)^* \right) = 0. \tag{43}$$

As $\alpha_1 + \cdots + \alpha_N = 0$, it cannot be that $\alpha_2, \ldots, \alpha_N$ are all zero, so the collection

$$\left\{ \text{vec}(U_2) \text{vec}(U_2)^* - \text{vec}(U_1) \text{vec}(U_1)^*, \ldots, \text{vec}(U_N) \text{vec}(U_N)^* - \text{vec}(U_1) \text{vec}(U_1)^* \right\} \tag{44}$$

is linearly dependent, implying that the collection (41) generates an affine subspace of dimension strictly less than $N - 1$. This, however, contradicts the assumption that the mixed-unitary rank of Φ is N through Carathéodory's theorem.

Given that the collection (41) is linearly independent and each p_k is nonzero, it follows that the collection

$$\left\{ A u_k u_k^* A^*, \ldots, A u_N u_N^* A^* \right\} = \left\{ p_1 \text{vec}(U_1) \text{vec}(U_1)^*, \ldots, p_N \text{vec}(U_N) \text{vec}(U_N)^* \right\} \tag{45}$$

is also linearly independent. This implies that the collection $\mathcal{B} \subseteq \mathcal{M}_r$ defined as

$$\mathcal{B} = \left\{ u_1 u_1^*, \ldots, u_N u_N^* \right\} \tag{46}$$

is linearly independent as well: $\dim(\text{span}(\mathcal{B})) = N$. For each index $k \in \{1, \ldots, N\}$ we see that

$$\Psi^*(u_k u_k^*) = \sum_{i,j=1}^{r} \langle E_{i,j}, V^{\mathsf{T}} E_{k,k} \overline{V} \rangle A_j^* A_i = \sum_{i,j=1}^{r} V(k,i) \overline{V(k,j)} A_j^* A_i = p_k U_k^* U_k = p_k \mathbb{1}_n, \tag{47}$$

and therefore $\Psi^*(\text{span}(\mathcal{B})) = \text{span}\{\mathbb{1}_n\}$. It follows that $\dim(\ker(\Psi^*) \cap \text{span}(\mathcal{B})) = N - 1$ which implies that $\dim(\ker(\Psi^*)) \geq N - 1$, completing the proof. $\square$

Corollary 4. *Let n be a positive integer, let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a mixed-unitary channel with mixed-unitary rank equal to N and Choi rank equal to r. It is the case that*

$$N \leq r^2 - r + 1. \tag{48}$$

Proof. By Theorem 3, it will suffice to show that $r \leq \dim(\mathcal{S}_\Phi)$. Let $U_1, \ldots, U_N \in \mathcal{U}_n$ be unitary matrices and let $(p_1, \ldots, p_N)$ be a probability vector for which

$$\Phi(X) = \sum_{k=1}^{N} p_k U_k X U_k^* \tag{49}$$

for each $X \in \mathcal{M}_n$, and consider the collection of matrices $\{U_1^* U_1, \ldots, U_1^* U_N\} \subset \mathcal{S}_\Phi$. As U_1 is invertible, one has that

$$\dim(\{U_1^* U_1, \ldots, U_1^* U_N\}) = \dim(\{U_1, \ldots, U_N\}) = \text{rank}(J(\Phi)) = r \tag{50}$$

from which it follows that $\dim(\mathcal{S}_\Phi) \geq r$. $\square$

Next we will prove that any channel $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ having an operator system of dimension 3 or less must be mixed unitary, and indeed must have mixed-unitary rank in agreement with its Choi rank. By combining this theorem with the previous one, we obtain the upper bound $\max\{r, r^2 - 3\}$ on the mixed-unitary rank of any mixed-unitary channel having Choi rank r. In the proof of the theorem to follow, we will use the fact that every traceless square matrix is unitarily equivalent to one having a vanishing diagonal. This is a well-known fact that follows from the Toeplitz–Hausdorff theorem. (See, for instance, Theorem 1.3.4 of [HJ94].)

Theorem 5. *Let n be a positive integer, let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a channel, and suppose that $\dim(\mathcal{S}_\Phi) \leq 3$. The channel Φ is mixed unitary with mixed-unitary rank equal to its Choi rank.*

Proof. Let $r = \mathrm{rank}(J(\Phi))$ be the Choi rank of Φ, let $\Psi : \mathcal{M}_n \to \mathcal{M}_r$ be any channel complementary to Φ, and observe that $\mathcal{S}_\Phi = \mathrm{im}(\Psi^*)$. Define a subspace of matrices $\mathcal{A} \subseteq \mathcal{M}_r$ as

$$\mathcal{A} = \{\Psi(X) \,:\, X \in \mathbb{1}_n^\perp\}. \tag{51}$$

As $\mathcal{A}$ is the image of all traceless matrices under the action of Ψ, by Corollary 2 it will suffice to show the existence of a unitary matrix $U \in \mathcal{U}_r$ such that $U\mathcal{A}U^*$ contains only matrices with vanishing diagonal. By the assumption $\dim(\mathcal{S}_\Phi) \leq 3$, together with the observation that $\mathbb{1}_n \in \mathcal{S}_\Phi$, we conclude that there must exist traceless Hermitian matrices $H, K \in \mathbb{1}_n^\perp$ such that

$$\mathcal{S}_\Phi = \mathrm{span}\{\mathbb{1}_n, H, K\}. \tag{52}$$

As $\mathrm{im}(\Psi^*) = \ker(\Psi)^\perp$, one therefore has that $\mathrm{im}(\Psi) = \Psi(\mathcal{S}_\Phi)$ from which we may conclude that $\mathcal{A} = \mathrm{span}\{\Psi(H), \Psi(K)\}$. Note that $\mathrm{Tr}(A) = 0$ for each $A \in \mathcal{A}$, as Ψ is trace preserving, and in particular

$$\mathrm{Tr}(\Psi(H + iK)) = 0. \tag{53}$$

There must therefore exist a unitary matrix $U \in \mathcal{U}_n$ such that $U\Psi(H + iK)U^*$ has vanishing diagonal. Because both H and K are Hermitian, each of the Hermitian matrices $U\Psi(H)U^*$ and $U\Psi(H)U^*$ must therefore also have vanishing diagonal. It follows that $U\mathcal{A}U^*$ has vanishing diagonal for every $A \in \mathcal{A}$, and therefore Φ is mixed unitary with mixed-unitary rank equal to r by Corollary 2. $\square$

We may also use Theorem 5 to show that every channel with Choi rank equal to 2 is either extremal or a convex combination of two unitary channels.

Corollary 6. *Let n be a positive integer and let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a channel with Choi rank equal to 2. If Φ is not an extreme point in the set of all channels, then Φ is mixed unitary with mixed-unitary rank equal to 2.*

Proof. The channel Φ is an extreme point in the convex set of all channels if and only if $\dim(\mathcal{S}_\Phi) = \mathrm{rank}(J(\Phi))^2$. Therefore, under the assumption that Φ is not extremal, it follows that $\dim(\mathcal{S}_\Phi) \leq 3$ by the assumption that Φ has Choi rank 2. The channel Φ is therefore mixed unitary with mixed-unitary rank equal to 2 by Theorem 5. $\square$

Finally, we may combine the results of Theorem 3 and Theorem 5 to improve the upper bound on the mixed-unitary rank of mixed-unitary channels with Choi rank equal to 3.

Corollary 7. *Let n be a positive integer, let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a mixed-unitary channel with Choi rank equal to 3 and mixed-unitary rank equal to N. It is the case that $N \leq 6$.*

Proof. If $s = \dim(\mathcal{S}_\Phi) \leq 3$, then $N = 3$ by Theorem 5; if $s \geq 4$, then $N \leq 6$ by Theorem 3. $\square$

12

4. A construction for non-trivial mixed-unitary rank

Next we present a construction to obtain mixed-unitary channels with mixed-unitary ranks strictly larger than their Choi ranks. The construction makes use of two concepts that were discussed in the preliminaries section: the direct-sum of two channels and the notion of a unique mixed-unitary decomposition of a mixed-unitary channel.

Theorem 8. *Let n and m be positive integers, let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a mixed-unitary channel having Choi rank equal to r, mixed-unitary rank equal to r, and a unique mixed-unitary decomposition. For every unitary channel $\Psi : \mathcal{M}_m \to \mathcal{M}_m$, the direct sum channel $\Phi \oplus \Psi$ has Choi rank $r + 1$ and mixed-unitary rank $2r$.*

Proof. We begin by noting that there is no loss of generality in assuming Ψ is the identity channel on $\mathcal{M}_m$, which we shall do for the remainder of the proof. The Choi rank of $\Phi \oplus \Psi$ can simply be calculated:

$$\operatorname{rank}(J(\Phi \oplus \Psi)) = \operatorname{rank}(J(\Phi)) + \operatorname{rank}(J(\Psi)) = r + 1. \tag{54}$$

It therefore remains to prove that the mixed-unitary rank of $\Phi \oplus \Psi$ is equal to $2r$. For the purpose of doing this, we let

$$\Phi(X) = \sum_{k=1}^{r} p_k U_k X U_k^* \tag{55}$$

be a unique mixed-unitary decomposition of Φ, the existence of which has been assumed by the theorem. We also observe that

$$(\Phi \oplus \Psi)(Z) = \frac{1}{2} \sum_{k=1}^{r} p_k \begin{pmatrix} U_k & 0 \\ 0 & \mathbb{1}_m \end{pmatrix} Z \begin{pmatrix} U_k & 0 \\ 0 & \mathbb{1}_m \end{pmatrix}^* + \frac{1}{2} \sum_{k=1}^{r} p_k \begin{pmatrix} U_k & 0 \\ 0 & -\mathbb{1}_m \end{pmatrix} Z \begin{pmatrix} U_k & 0 \\ 0 & -\mathbb{1}_m \end{pmatrix}^* \tag{56}$$

is a mixed-unitary decomposition of $\Phi \oplus \Psi$, establishing that its mixed-unitary rank is no greater than $2r$.

To complete the proof, we must establish that every mixed-unitary decomposition of $\Phi \oplus \Psi$ has at least $2r$ terms. With this task in mind, and recalling from the discussion on direct sums of channels that each Kraus operator of $\Phi \oplus \Psi$ is necessarily a direct sum of matrices, consider any mixed-unitary decomposition

$$(\Phi \oplus \Psi)(Z) = \sum_{j=1}^{t} q_j \begin{pmatrix} V_j & 0 \\ 0 & W_j \end{pmatrix} Z \begin{pmatrix} V_j & 0 \\ 0 & W_j \end{pmatrix}^*. \tag{57}$$

We note that the decomposition (57) implies that

$$\Phi(X) = \sum_{j=1}^{t} q_j V_j X V_j^* \quad \text{and} \quad \Psi(Y) = \sum_{j=1}^{t} q_j W_j Y W_j^* \tag{58}$$

for all $X \in \mathcal{M}_n$ and $Y \in \mathcal{M}_m$. Because Ψ is the identity channel on $\mathcal{M}_m$, it must therefore be the case that $W_j \sim \mathbb{1}_m$ for all $j \in \{1, \ldots, t\}$. That is, there exist complex units $\alpha_1, \ldots, \alpha_t$ such that $W_j = \alpha_j \mathbb{1}_m$ for all $j \in \{1, \ldots, t\}$. Moreover, by the assumption that (55) is a unique mixed-unitary decomposition, there must therefore exist a partition $\{1, \ldots, t\} = T_1 \cup \cdots \cup T_r$ such that for every

13

$k \in \{1, \dots, r\}$ we have $V_j \sim U_k$ for every $j \in T_k$ and $p_k = \sum_{j \in T_k} q_j$. Let us choose complex units $\beta_{j,k}$ for all $j \in T_k$ so that $V_j = \beta_{j,k} U_k$. Finally, we observe that the decomposition (57) implies that

$$(\Phi \oplus \Psi) \begin{pmatrix} 0 & Z \\ 0 & 0 \end{pmatrix} = \sum_{j=1}^{t} q_j \begin{pmatrix} 0 & V_j Z W_j^* \\ 0 & 0 \end{pmatrix} = \sum_{j=1}^{t} q_j \begin{pmatrix} 0 & \overline{\alpha_j} V_j Z \\ 0 & 0 \end{pmatrix} \tag{59}$$

for all $Z \in \mathcal{M}_{n,m}$. The direct sum of two channels must zero-out the off-diagonal blocks of its input, and therefore we conclude that

$$\sum_{j=1}^{t} q_j \overline{\alpha_j} V_j = 0. \tag{60}$$

By splitting this sum according to the partition $T_1 \cup \cdots \cup T_r$, we find that

$$0 = \sum_{k=1}^{r} \sum_{j \in T_k} q_j \overline{\alpha_j} V_j = \sum_{k=1}^{r} \left(\sum_{j \in T_k} q_j \overline{\alpha_j} \beta_{j,k} \right) U_k. \tag{61}$$

The matrices $U_1, \dots, U_r$ are linearly independent by the assumption that Φ has Choi rank r. It is therefore the case that

$$\sum_{j \in T_k} q_j \overline{\alpha_j} \beta_{j,k} = 0 \tag{62}$$

for every $k \in \{1, \dots, r\}$. Note that it cannot be that there is any choice of k such that $q_j = 0$ for every $j \in T_k$, for then we would have $p_k = \sum_{j \in T_k} q_j = 0$, which violates the assumption that Φ has Choi rank r. Each of the sums (62) is therefore a positive linear combination of complex units, and consequently $|T_k| \geq 2$ for ever $k \in \{1, \dots, r\}$. This implies $t = |T_1| + \cdots + |T_r| \geq 2r$, as required. $\qquad \square$

Naturally, in order to use the previous theorem to obtain examples of mixed-unitary channels whose mixed-unitary ranks are greater than their Choi ranks, one must address the following question: Under what conditions must a mixed-unitary channel Φ have a unique mixed-unitary decomposition? The following theorem provides one suitable condition: if the dimension s of the operator system of a mixed-unitary channel Φ satisfies $s = r^2 - r + 1$, for r being the Choi rank of Φ, then the mixed-unitary rank of Φ must also be r, and moreover Φ possesses a unique mixed-unitary decomposition.

Theorem 9. *Let n be a positive integer and let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a mixed-unitary channel having Choi rank r. If the dimension s of the operator system of Φ is given by $s = r^2 - r + 1$, then Φ has mixed-unitary rank equal to r and has a unique mixed-unitary decomposition.*

Proof. Suppose Φ has mixed-unitary rank equal to N. By Theorem 3 we have $N \leq r^2 - s + 1 = r$, and therefore $N = r$. There must therefore exist distinct unitary matrices $U_1, \dots, U_r \in \mathcal{U}_n$ and a probability vector $(p_1, \dots, p_r)$ so that

$$\Phi(X) = \sum_{k=1}^{r} p_k U_k X U_k^* \tag{63}$$

14

for every $X \in \mathcal{M}_n$. It remains to prove that (63) is a unique mixed-unitary decomposition of Φ. Toward this goal we define a map $\Psi : \mathcal{M}_n \to \mathcal{M}_r$ as

$$\Psi(X) = \sum_{j,k=1}^{r} \sqrt{p_j p_k} \langle U_k^* U_j, X \rangle E_{j,k} \tag{64}$$

for all $X \in \mathcal{M}_n$, so that Ψ is a complementary channel to Φ. For convenience we note that

$$\Psi^*(Y) = \sum_{j,k=1}^{r} \sqrt{p_j p_k} \, Y(j,k) \, U_k^* U_j \tag{65}$$

for all $Y \in \mathcal{M}_r$.

We now observe that $\Psi^*(Y) \in \operatorname{span}\{\mathbb{1}_n\}$ if and only if $Y \in \mathcal{M}_r$ is a diagonal matrix. Indeed, from (65), for every diagonal matrix Y, $\Psi^*(Y) \in \operatorname{span}\{\mathbb{1}_n\}$. On the other hand, by the rank nullity theorem we have

$$\dim(\ker(\Psi^*)) = r^2 - \dim(\operatorname{im}(\Psi^*)) = r^2 - s = r - 1, \tag{66}$$

so the subspace containing all matrices Y satisfying $\Psi^*(Y) \in \operatorname{span}\{\mathbb{1}_n\}$ can have dimension no larger than r. Thus, there can be no matrices Y outside of the r dimensional subspace of diagonal matrices in $\mathcal{M}_r$ that satisfy $\Psi^*(Y) \in \operatorname{span}\{\mathbb{1}_n\}$.

Now suppose that $V_1, \ldots, V_t \in \mathcal{U}_n$ are unitary matrices and $(q_1, \ldots, q_t)$ is a probability vector with each q_k being positive such that

$$\Phi(X) = \sum_{k=1}^{t} q_k V_k X V_k^* \tag{67}$$

for all $X \in \mathcal{M}_n$. It follows that there must exist an isometry $W \in \mathcal{M}_{t,r}$ satisfying

$$\sqrt{q_k} V_k = \sum_{j=1}^{r} W(k,j) \sqrt{p_j} \, U_j \tag{68}$$

for each $k \in \{1, \ldots, t\}$, from which we conclude that

$$\Psi^* \big(\overline{W} E_{k,k} W^\mathsf{T} \big) = \sum_{i,j=1}^{r} \sqrt{p_i p_j} \, W(k,i) \, \overline{W(k,j)} \, U_j^* U_i = q_k V_k^* V_k = q_k \mathbb{1}_n. \tag{69}$$

It is therefore the case that $D_k = \overline{W} E_{k,k} W^\mathsf{T}$ is diagonal for every $k \in \{1, \ldots, t\}$. We conclude that

$$q_k V_k X V_k^* = \sum_{i,j=1}^{r} \sqrt{p_i p_j} D_k(j,i) U_i X U_j^* = \sum_{j=1}^{r} p_j D_k(j,j) U_j X U_j^* \tag{70}$$

for every $X \in \mathcal{M}_n$ and $k \in \{1, \ldots, t\}$. As $U_1, \ldots, U_r$ are linearly independent, it follows that for every index $k \in \{1, \ldots, t\}$, the matrix entry $D_k(j,j)$ is nonzero for precisely one choice of an index $j \in \{1, \ldots, r\}$, and for this unique index j it is necessarily the case that $V_k \sim U_j$. Letting $T_1 \cup \cdots \cup T_r = \{1, \ldots, t\}$ be the partition defined by

$$T_j = \{k \in \{1, \ldots, t\} : D_k(j,j) \neq 0\}, \tag{71}$$

15

we find that $V_k \sim U_j$ for every $k \in T_j$ and

$$p_j = \sum_{k \in T_j} q_k. \tag{72}$$

The channel Φ therefore has a unique mixed-unitary decomposition. $\qquad\square$

We may now use Theorem 8 to construct mixed-unitary channels in dimension $n = p+1$ having mixed-unitary rank strictly greater than their Choi rank for any odd prime p. The channels constructed in this manner will be shown to have Choi rank $p+1$ but mixed-unitary rank $2p$, yielding an increasingly large separation between mixed-unitary rank and Choi rank as p increases. Moreover, the channels constructed in this manner are not unitary equivalent to a Schur map (see Appendix A). This construction makes use of the discrete Weyl matrices.

Example 10. Let p be an odd prime integer. Define $\zeta = \exp(2\pi i/p)$ and define unitary matrices $U, V \in \mathcal{U}_p$ as

$$U = \sum_{a \in \mathbb{Z}_p} E_{a+1,a} \qquad \text{and} \qquad V = \sum_{a \in \mathbb{Z}_p} \zeta^a E_{a,a}, \tag{73}$$

where one takes $\{e_a : a \in \mathbb{Z}_p\}$ as the standard basis of $\mathbb{C}^p$, and define a mixed-unitary channel $\Phi : \mathcal{M}_p \to \mathcal{M}_p$ as

$$\Phi(X) = \frac{1}{p} \sum_{a \in \mathbb{Z}_p} \left(U^a V^{a^2} \right) X \left(U^a V^{a^2} \right)^* \tag{74}$$

for each $X \in \mathcal{M}_p$. The collection of unitary matrices $\{U^a V^b : a, b \in \mathbb{Z}_p\}$ form an orthogonal basis of $\mathcal{M}_p$, and these matrices satisfy

$$(U^a V^b)^* (U^c V^d) \sim U^{c-a} V^{d-b} \tag{75}$$

for each $a, b, c, d \in \mathbb{Z}_p$. It is evident that the collection $\{U^a V^{a^2} : a \in \mathbb{Z}_p\}$ is linearly independent, and thus Φ has Choi rank and mixed-unitary rank both equal to p. We will show that the dimension of the operator system of Φ satisfies $\dim(\mathcal{S}_\Phi) = p^2 - p + 1$. To prove this claim, we will show that, for any $a, b, c, d \in \mathbb{Z}_p$, the matrices

$$\left(U^b V^{b^2} \right)^* \left(U^a V^{a^2} \right) \qquad \text{and} \qquad \left(U^d V^{d^2} \right)^* \left(U^c V^{c^2} \right) \tag{76}$$

are orthogonal unless at least one of $(a, b) = (c, d)$ or $(a, c) = (b, d)$ holds. Indeed, note that

$$\left| \left\langle \left(U^b V^{b^2} \right)^* \left(U^a V^{a^2} \right), \left(U^d V^{d^2} \right)^* \left(U^c V^{c^2} \right) \right\rangle \right| = \left| \left\langle U^{a-b} V^{a^2-b^2}, U^{c-d} V^{c^2-d^2} \right\rangle \right|$$

$$= \begin{cases} p & \text{if } a - b = c - d \text{ and } a^2 - b^2 = c^2 - d^2 \\ 0 & \text{otherwise,} \end{cases} \tag{77}$$

where the equalities are taken to be equivalences modulo p. Suppose now that the pair of matrices in (76) are not orthogonal and suppose further that $a \neq b$. As it must be the case that

$$a - b = c - d \qquad \text{and} \qquad a^2 - b^2 = c^2 - d^2, \tag{78}$$

where $a - b \neq 0$, we may divided the second equality by the first to find that

$$a - b = c - d \qquad \text{and} \qquad a + b = c + d. \tag{79}$$

16

Taking both the sum and difference of these two resulting equalities, we find that

$$2a = 2c \qquad \text{and} \qquad 2b = 2d. \tag{80}$$

As these equalities are taken to be equivalences modulo p (where p is an odd prime), we may conclude that $a = c$ and $b = d$. This completes the proof of the claim that $\dim(\mathcal{S}_\Phi) = p^2 - p + 1$. It follows that Φ has a unique mixed-unitary decomposition by Theorem 9.

Now let $\Psi : \mathcal{M}_1 \to \mathcal{M}_1$ be the (rather trivial) channel defined as $\Psi(\alpha) = \alpha$ for every $\alpha \in \mathbb{C}$. By Theorem 8, the channel $\Phi \oplus \Psi : \mathcal{M}_{p+1} \to \mathcal{M}_{p+1}$ is mixed unitary with Choi rank equal to $p + 1$ but mixed-unitary rank equal to $2p$.

Remark. We remark that the channel in (74) appears in [AS04] in the context of approximate quantum encryption schemes.

Example 11. In order to provide a concrete example, we now explicitly present the mixed unitary channel from Example 10 in the case when $p = 3$, where $\zeta = \exp(2\pi i/3)$. The matrices in (73) are

$$U = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \end{pmatrix}, \tag{81}$$

and the channel $\Phi : \mathcal{M}_3 \to \mathcal{M}_3$ as defined in (74) is given by

$$\Phi(X) = \frac{1}{3}\left(W_0 X W_0^* + W_1 X W_1^* + W_2 X W_2^*\right), \tag{82}$$

where one defines the unitary matrices $W_a = U^a V^{a^2}$ for each $a \in \{0,1,2\}$. Explicitly,

$$W_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad W_1 = \begin{pmatrix} 0 & 0 & \zeta^2 \\ 1 & 0 & 0 \\ 0 & \zeta & 0 \end{pmatrix}, \quad \text{and} \quad W_2 = \begin{pmatrix} 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \\ 1 & 0 & 0 \end{pmatrix}. \tag{83}$$

The Choi rank of Φ is $\text{rank}(J(\Phi)) = 3$ and Φ has mixed-unitary rank equal to 3. The operator system $\mathcal{S}_\Phi$ is spanned by the seven linearly independent matrices:

$$W_0^* W_1 = \begin{pmatrix} 0 & 0 & \zeta^2 \\ 1 & 0 & 0 \\ 0 & \zeta & 0 \end{pmatrix}, \quad W_0^* W_2 = \begin{pmatrix} 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \\ 1 & 0 & 0 \end{pmatrix} \quad W_1^* W_0 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \zeta^2 \\ \zeta & 0 & 0 \end{pmatrix},$$

$$W_1^* W_2 = \begin{pmatrix} 0 & 0 & \zeta^2 \\ \zeta^2 & 0 & 0 \\ 0 & \zeta^2 & 0 \end{pmatrix}, \quad W_2^* W_0 = \begin{pmatrix} 0 & 0 & 1 \\ \zeta^2 & 0 & 0 \\ 0 & \zeta & 0 \end{pmatrix}, \quad W_2^* W_1 = \begin{pmatrix} 0 & \zeta & 0 \\ 0 & 0 & \zeta \\ \zeta & 0 & 0 \end{pmatrix}, \tag{84}$$

$$W_0^* W_0 = W_1^* W_1 = W_2^* W_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and thus $\dim(\mathcal{S}_\Phi) = 7$. It follows from Theorem 9 that Φ has a unique mixed-unitary decomposition. Defining the trivial channel $\Psi : \mathcal{M}_1 \to \mathcal{M}_1$ as $\Psi(\alpha) = \alpha$ for every $\alpha \in \mathbb{C}$, it follows from

Theorem 8 that the channel $\Phi \oplus \Psi : \mathcal{M}_4 \to \mathcal{M}_4$ is mixed unitary with Choi rank equal to 4 but mixed-unitary rank equal to 6. Explicitly, this channel is given by

$$(\Phi \oplus \Psi)(X) = \frac{1}{6} \sum_{k=1}^{6} A_k X A_k^*, \tag{85}$$

where $A_1, \ldots, A_6 \in \mathcal{U}_4$ are the unitary matrices defined as

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & \zeta^2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 0 & 0 & \zeta^2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad A_5 = \begin{pmatrix} 0 & \zeta & 0 & 0 \\ 0 & 0 & \zeta^2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_6 = \begin{pmatrix} 0 & \zeta & 0 & 0 \\ 0 & 0 & \zeta^2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{86}$$

5. Further examples based on Schur channels

Further examples illustrating properties of the mixed-unitary rank are presented in this section. These examples fall into the category of *Schur channels*, which are channels that can be expressed as

$$\Phi(X) = C \odot X \tag{87}$$

for every $X \in \mathcal{M}_n$, for some fixed choice of $C \in \mathcal{M}_n$, where $C \odot X$ denotes the *Schur product* (or entry-wise product) of the matrices C and X. Schur channels are sometimes alternatively called *diagonal channels*, owing to the fact that every Kraus representation of a Schur channel must make use of only diagonal Kraus matrices. The Choi rank of the Schur channel (87) is given by $\mathrm{rank}(J(\Phi)) = \mathrm{rank}(C)$, and it is well known that a map of this form is a channel if and only if C is a *correlation matrix*, which is a positive semidefinite matrix whose diagonal entries are all equal to 1. Every Schur channel is necessarily unital; meanwhile, for $n \geq 4$, there are examples of Schur channels that are not mixed unitary [Tre86, LS93].

Before proceeding to the examples promised, it will be helpful to note various properties of Schur channels, and mixed-unitary Schur channels in particular. First, we observe that the dimension of the operator system of any Schur channel can be calculated directly from the formula

$$\dim(\mathcal{S}_\Phi) = \mathrm{rank}(\overline{C} \odot C), \tag{88}$$

which follows from the fact that $(\Phi^*\Phi)(X) = (\overline{C} \odot C) \odot X$ for every $X \in \mathcal{M}_n$. We also note that the operator system of every Schur channel contains only diagonal matrices.

Second, we observe that the mixed-unitary rank of a mixed-unitary Schur channel can alternatively be characterized directly in terms of what we call the *toroidal rank* of the matrix C. To be precise, let us introduce the notation

$$\mathbb{T} = \{\alpha \in \mathbb{C} : |\alpha| = 1\}. \tag{89}$$

18

It is evident that a correlation matrix $C \in \mathcal{M}_n$ has rank equal to 1 if and only if $C = uu^*$ for some choice of a vector $u \in \mathbb{T}^n$. We shall say that a correlation matrix C is *toroidal* if it can be expressed as a convex combination of rank-one correlation matrices. That is, $C \in \mathcal{M}_n$ is toroidal if there exists a positive integer N, vectors $u_1, \ldots, u_N \in \mathbb{T}^n$, and a probability vector $(p_1, \ldots, p_n)$ such that

$$C = \sum_{k=1}^{N} p_k u_k u_k^*. \tag{90}$$

The *toroidal rank* of C is the smallest positive integer N for which such an expression exists. The observation that the mixed-unitary rank of the Schur channel (87) coincides with the toroidal rank of C is expressed by the following proposition.

Proposition 12. *Let n and N be positive integers, let $C \in \mathcal{M}_n$ be a correlation matrix, and let Φ be the Schur channel defined as $\Phi(X) = C \odot X$ for every $X \in \mathcal{M}_n$. The following two statements are equivalent:*

1. *Φ is mixed unitary and has mixed-unitary rank equal to N.*

2. *C is toroidal and has toroidal rank equal to N.*

For all dimensions $n \geq 4$ there exist correlation matrices in $\mathcal{M}_n$ that are not toroidal [LT94]. However, it is the case that every correlation matrix in $\mathcal{M}_2$ and $\mathcal{M}_3$ is toroidal. Indeed, it follows from Theorem 5 that all correlation matrices in $\mathcal{M}_2$ and $\mathcal{M}_3$ have toroidal ranks equal to their ranks.

Proposition 13. *Let $n \in \{2, 3\}$. Every correlation matrix $C \in \mathcal{M}_n$ is toroidal and has toroidal rank equal to $\mathrm{rank}(C)$. Equivalently, the channel $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ defined as $\Phi(X) = C \odot X$ for each $X \in \mathcal{M}_n$ is mixed unitary and has mixed-unitary rank equal to its Choi rank.*

Proof. The operator system $\mathcal{S}_\Phi \subseteq \mathcal{M}_n$ consists of only diagonal matrices and thus $\dim(\mathcal{S}) \leq n$. The result now follows from Theorem 5, as $\mathrm{rank}(J(\Phi)) = \mathrm{rank}(C)$ and we have assumed that $n \leq 3$. $\square$

Theorem 3 implies the following upper bound on the toroidal rank of any correlation matrix.

Corollary 14. *Let n be a positive integer and let $C \in \mathcal{M}_n$ be a toroidal correlation matrix having toroidal rank N. It is the case that*

$$N \leq r^2 - s + 1, \tag{91}$$

where $r = \mathrm{rank}(C)$ and $s = \mathrm{rank}(\overline{C} \odot C)$.

Now we are prepared to proceed to the examples suggested previously. The following lemma will be used for the first example.

Lemma 15. *Let $C \in \mathcal{M}_3$ be a correlation matrix with $\mathrm{rank}(C) = 2$, and assume that none of the off-diagonal entries of C is contained in $\mathbb{T}$. It must then be the case that $\mathrm{rank}(\overline{C} \odot C) = 3$.*

Proof. Note first that C is a toroidal correlation matrix, as every 3×3 correlation matrix is toroidal. By Proposition 13, the toroidal rank of C must be equal to 2, so there must exist vectors $u_0, u_1 \in \mathbb{T}^3$ such that $C \in \mathrm{conv}\{u_0 u_0^*, u_1 u_1^*\}$. It may be assumed without loss of generality that

$$u_0 = \begin{pmatrix} 1 \\ \alpha_0 \\ \beta_0 \end{pmatrix} \quad \text{and} \quad u_1 = \begin{pmatrix} 1 \\ \alpha_1 \\ \beta_1 \end{pmatrix} \tag{92}$$

19

for some choice of complex units $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{T}$. By the assumption that none of the off-diagonal entries of C lies in $\mathbb{T}$, we have

$$\alpha_0 \neq \alpha_1, \quad \beta_0 \neq \beta_1, \quad \text{and} \quad \overline{\alpha_0}\beta_0 \neq \overline{\alpha_1}\beta_1. \tag{93}$$

Define the complex units $\alpha, \beta \in \mathbb{T}$ as $\alpha = \alpha_0\overline{\alpha_1}$ and $\beta = \beta_0\overline{\beta_1}$, and observe that $1 \notin \{\alpha, \beta, \overline{\alpha}\beta\}$. It is the case that

$$\text{im}(\overline{C} \odot C) = \text{span}\{u_0 \odot \overline{u_0}, u_0 \odot \overline{u_1}, u_1 \odot \overline{u_0}, u_1 \odot \overline{u_1}\}$$
$$= \text{span}\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix}, \begin{pmatrix} 1 \\ \overline{\alpha} \\ \overline{\beta} \end{pmatrix} \right\}. \tag{94}$$

Now define a matrix $A \in \mathcal{M}_3$ as

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \overline{\alpha} \\ 1 & \beta & \overline{\beta} \end{pmatrix}, \tag{95}$$

for which it may be verified (using the fact that $\alpha, \beta \in \mathbb{T}$) that

$$\det(A^*A) = -(2 - \alpha - \overline{\alpha})(2 - \beta - \overline{\beta})(2 - \alpha\overline{\beta} - \overline{\alpha}\beta)$$
$$= 8\,\text{Re}(\alpha - 1)\,\text{Re}(\beta - 1)\,\text{Re}(\overline{\alpha}\beta - 1). \tag{96}$$

As $\alpha, \beta, \overline{\alpha}\beta \in \mathbb{T}$ but none of α, β, and $\overline{\alpha}\beta$ is equal to 1, it follows that $\det(A^*A) \neq 0$ and therefore A is nonsingular. This implies that the columns of A are linearly independent, and therefore we have $\dim(\text{im}(\overline{C} \odot C)) = 3$, as required. $\qquad\square$

Example 16. Define the (necessarily toroidal) correlation matrix $B \in \mathcal{M}_3$ as

$$B = \begin{pmatrix} 1 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 1 \end{pmatrix}. \tag{97}$$

Note that $\text{rank}(B) = 2$ and that none of its off-diagonal entries lies in $\mathbb{T}$. It follows from Lemma 15 that $\text{rank}(\overline{B} \odot B) = 3$. The channel defined as $\Phi(X) = B \odot X$ for all $X \in \mathcal{M}_3$ therefore has Choi rank $r = 2$ and an operator system of dimension $s = 3$. By Theorem 9, it follows that Φ has mixed-unitary rank equal to $r = 2$ and has a unique mixed-unitary decomposition. Equivalently, B has toroidal rank 2 and has a unique toroidal decomposition. The fact that B has toroidal rank 2 may also be observed directly from the toroidal decomposition

$$B = \frac{1}{2}uu^* + \frac{1}{2}vv^* \tag{98}$$

for the choice of toroidal vectors $u, v \in \mathbb{T}^3$ given by

$$u = \begin{pmatrix} 1 \\ \frac{1+i}{\sqrt{2}} \\ \frac{1-i}{\sqrt{2}} \end{pmatrix} \quad \text{and} \quad v = \begin{pmatrix} 1 \\ \frac{1-i}{\sqrt{2}} \\ \frac{1+i}{\sqrt{2}} \end{pmatrix}. \tag{99}$$

Now consider the channel $\Phi \oplus \Psi$, where $\Psi : \mathcal{M}_n \to \mathcal{M}_n$ is the identity channel for any choice of a dimension $n \geq 1$. By Theorem 8, this channel has Choi rank 3 and mixed-unitary rank 4. This direct sum channel is also a Schur channel, owing to the fact that the identity channel is a Schur channel corresponding to the all 1s matrix. In particular, for $n = 1$ we find that the correlation matrix $C \in \mathcal{M}_4$ defined as

$$C = \begin{pmatrix} 1 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 1 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{100}$$

has $\mathrm{rank}(C) = 3$ and toroidal rank equal to 4.

For the next example we will require the notion of *mutually unbiased bases*, which is as follows. Let d be a positive integer and let $\mathcal{A}_1, \ldots, \mathcal{A}_N \subset \mathbb{C}^d$ be orthonormal bases of $\mathbb{C}^d$ given as

$$\mathcal{A}_k = \{u_{k,1}, \ldots, u_{k,d}\} \tag{101}$$

for each $k \in \{1, \ldots, N\}$. This collection of bases $\{\mathcal{A}_1, \ldots, \mathcal{A}_N\}$ is said to be *mutually unbiased* if, for all choices of distinct indices $i \neq j \in \{1, \ldots, N\}$, it is the case that

$$|\langle u, v \rangle| = \frac{1}{\sqrt{d}} \tag{102}$$

for all $u \in \mathcal{A}_i$ and $v \in \mathcal{A}_j$. An upper bound to the maximal size N of a collection of mutually unbiased bases that may exist in $\mathbb{C}^d$ is $N \leq d + 1$. It is known that this bound is achieved in the case when d is a prime power (see, e.g., [Ivo81]), while it is a major open question to determine if this maximum value can be achieved for non-prime-powers. More information on mutually unbiased bases can be found in [WF89] and [DEBŻ10].

In the following example we will show how to construct correlation matrices with rank $d + 1$ and toroidal rank equal to $2d$ for any d for which $d + 1$ mutually unbiased bases of $\mathbb{C}^d$ exist.

Example 17. Let d be a positive integer and suppose that there exist $d + 1$ mutually unbiased bases $\mathcal{A}_1, \ldots, \mathcal{A}_{d+1} \subset \mathbb{C}^d$ given as $\mathcal{A}_t = \{u_{t,1}, \ldots, u_{t,d}\}$ for each $t \in \{1, \ldots, d+1\}$. Define a matrix $A \in \mathcal{M}_{d^2, d}$ as

$$A = \sum_{k,j=1}^{d} (e_k \otimes e_j) u_{k,j}^* \tag{103}$$

and define $C \in \mathcal{M}_{d^2}$ as $C = AA^*$. It is evident that $\mathrm{rank}(C) = d$ and that C is a correlation matrix.

Let us first verify that C is toroidal, with toroidal rank equal to d. Define $v_1, \ldots, v_d \in \mathbb{C}^d \otimes \mathbb{C}^d$ as

$$v_k = \sqrt{d} \sum_{i,j}^{d} \langle u_{i,j}, u_{d+1,k} \rangle e_i \otimes e_j \tag{104}$$

for each $k \in \{1, \ldots, d\}$, and observe that

$$|v_k(i,j)| = \sqrt{d}\,|\langle u_{i,j}, u_{d+1,k} \rangle| = 1 \tag{105}$$

21

for all $i, j, k \in \{1, \ldots, d\}$. By defining a unitary matrix $U \in \mathcal{U}_d$ as

$$U = \sum_{k=1}^{d} u_{d+1,k} e_k^*, \tag{106}$$

one may verify that

$$\frac{1}{d} \sum_{k=1}^{d} v_k v_k^* = A U U^* A = A A^* = C. \tag{107}$$

Now let us compute $\overline{C} \odot C$. For each choice of indices $i, j, k, \ell \in \{1, \ldots, d\}$, we may express the corresponding entry of $\overline{C} \odot C$ as follows:

$$\left(\overline{C} \odot C\right)\left((k,i), (\ell,j)\right) = \begin{cases} 1 & \text{if } k = \ell \text{ and } i = j \\ 0 & \text{if } k = \ell \text{ and } i \neq j \\ \frac{1}{d} & \text{if } k \neq \ell. \end{cases} \tag{108}$$

As a block matrix, $\overline{C} \odot C$ takes this form:

$$\overline{C} \odot C = \begin{pmatrix} \mathbb{1}_d & \frac{1}{d} J_d & \cdots & \frac{1}{d} J_d \\ \frac{1}{d} J_d & \mathbb{1}_d & \ddots & \vdots \\ \vdots & \ddots & \ddots & \frac{1}{d} J_d \\ \frac{1}{d} J_d & \cdots & \frac{1}{d} J_d & \mathbb{1}_d \end{pmatrix}, \tag{109}$$

where J_d denotes the $d \times d$ matrix having a 1 in every entry. Equivalently,

$$\overline{C} \odot C = \frac{1}{d} J_d \otimes J_d + \mathbb{1}_d \otimes \left(\mathbb{1}_d - \frac{1}{d} J_d\right). \tag{110}$$

As $\mathbb{1}_d - J_d/d$ and J_d/d are orthogonal projection matrices of rank $d - 1$ and 1, respectively, we conclude that

$$\mathrm{rank}\left(\overline{C} \odot C\right) = 1 + d(d-1) = d^2 - d + 1. \tag{111}$$

Through a similar argument to the previous example, we conclude that if $\Phi : \mathcal{M}_{d^2} \to \mathcal{M}_{d^2}$ is the Schur channel defined as

$$\Phi(X) = C \odot X \tag{112}$$

for all $X \in \mathcal{M}_{d^2}$ and Ψ is a unitary channel of any dimension, then the channel $\Phi \oplus \Psi$ is a mixed-unitary channel having Choi rank $d + 1$ and mixed-unitary rank $2d$.

Our final example reveals that the mixed-unitary rank is not multiplicative with respect to tensor products.

Example 18. Let $C \in \mathcal{M}_4$ be the correlation matrix as defined in (100). This correlation matrix has $\mathrm{rank}(C) = 3$ and toroidal rank equal to 4. However, the correlation matrix $C \otimes \mathbb{1}_2$ satisfies $\mathrm{rank}(C \otimes \mathbb{1}_2) = 6$ and has toroidal rank also equal to 6.

To see this, one may construct a toroidal decomposition of $C \otimes \mathbb{1}_2$ as follows. Define a 6×8 matrix A as

$$A = \begin{pmatrix} 0 & 3 & -3 & 0 & 0 & 3 & -3 & 0 \\ 0 & -3 & 3 & 12 & 12 & 9 & -9 & 0 \\ 8 & 11 & 5 & -8 & 0 & 3 & -3 & -8 \\ 0 & 3 & -3 & -8 & 8 & 11 & 5 & -8 \\ 0 & -3 & 3 & -4 & 4 & 1 & 7 & 8 \\ 4 & 1 & 7 & 8 & 0 & -3 & 3 & -4 \end{pmatrix} \tag{113}$$

and define vectors $u_1, \ldots, u_6 \in \mathbb{T}^8$ as

$$u_j(k) = \exp(2\pi i A(j,k)/24) \tag{114}$$

for each $j \in \{1, \ldots, 6\}$ and $k \in \{1, \ldots, 8\}$. It may be verified (most easily with the help of a computer) that

$$C \otimes \mathbb{1}_2 = \frac{1}{6} \sum_{j=1}^{6} u_j u_j^*. \tag{115}$$

Thus, by taking $\Phi \in \mathcal{M}_4 \to \mathcal{M}_4$ to be the Schur channel defined by $\Phi(X) = C \odot X$ for each $X \in \mathcal{M}_4$, and letting $\Delta : \mathcal{M}_2 \to \mathcal{M}_2$ be the *completely dephasing channel*, which is the Schur channel given by

$$\Delta(Y) = \mathbb{1}_2 \odot Y \tag{116}$$

for all $Y \in \mathcal{M}_2$, one finds that the mixed-unitary rank of $\Phi \otimes \Delta$ is 6, despite the fact that the mixed-unitary ranks of Φ and Δ are 4 and 2, respectively.

6. Mixed-unitary rank of Werner–Holevo channels

The *Werner–Holevo channels* are interesting examples of unital channels defined as

$$\Phi_0(X) = \frac{\text{Tr}(X)\mathbb{1}_n + X^\mathsf{T}}{n+1} \qquad \text{and} \qquad \Phi_1(X) = \frac{\text{Tr}(X)\mathbb{1}_n - X^\mathsf{T}}{n-1} \tag{117}$$

for each $X \in \mathcal{M}_n$. We will call Φ_0 the *symmetric* Werner–Holevo channel and Φ_1 the *anti-symmetric* Werner–Holevo channel. For these channels, one has

$$J(\Phi_0) = \frac{2}{n+1}\Pi_0 \qquad \text{and} \qquad J(\Phi_1) = \frac{2}{n-1}\Pi_1 \tag{118}$$

where Π_0 and Π_1 are the projection matrices onto the symmetric and anti-symmetric subspaces of $\mathbb{C}^n \otimes \mathbb{C}^n$ respectively. The Werner–Holevo channels have Choi ranks equal to

$$\text{rank}(J(\Phi_0)) = \binom{n+1}{2} = \frac{n(n+1)}{2} \qquad \text{and} \qquad \text{rank}(J(\Phi_1)) = \binom{n}{2} = \frac{n(n-1)}{2} \tag{119}$$

respectively. It is known that Φ_1 is not mixed unitary for any odd n. It is perhaps known that Φ_0 is mixed unitary for all n and that Φ_1 is mixed unitary for all even n. In this section we will present mixed-unitary decompositions showing that both Φ_0 and Φ_1 have minimal mixed-unitary

rank for all even n. For $n = 3$, the symmetric Werner–Holevo channel Φ_0 also has minimal mixed-unitary rank and we conjecture based on numerical evidence that Φ_0 has minimal mixed-unitary rank for all odd n as well.

Before proceeding with the presentation of the mixed-unitary decompositions of the Werner–Holevo channels, allow us to first remark on the relationship between the Werner–Holevo channels and the spaces of symmetric and skew-symmetric matrices. Denote the spaces of symmetric matrices $S_n \subset \mathcal{M}_n$ and skew-symmetric matrices $K_n \subset \mathcal{M}_n$ as

$$S_n = \{A \in \mathcal{M}_n \,:\, A^{\mathsf{T}} = A\} \qquad \text{and} \qquad K_n = \{A \in \mathcal{M}_n \,:\, A^{\mathsf{T}} = -A\}. \tag{120}$$

These spaces have dimensions $\dim(S_n) = \binom{n+1}{2}$ and $\dim(K_n) = \binom{n}{2}$ respectively. The subspaces of $\mathbb{C}^n \otimes \mathbb{C}^n$ onto which the symmetric projection matrix Π_0 and anti-symmetric projection matrix Π_1 project are precisely

$$\mathrm{im}(\Pi_0) = \{\mathrm{vec}(A) \,:\, A \in S_n\} \qquad \text{and} \qquad \mathrm{im}(\Pi_1) = \{\mathrm{vec}(A) \,:\, A \in K_n\}. \tag{121}$$

Moreover, if $\Pi \in \mathcal{M}_m$ is any projection matrix with $\mathrm{rank}(\Pi) = r$ and $x_1, \ldots, x_r \in \mathbb{C}^m$ are any vectors, it holds that $\Pi = \sum_{k=1}^r x_k x_k^*$ if and only if $\{x_1, \ldots, x_r\}$ is an orthonormal basis for $\mathrm{im}(\Pi)$. This allows us to make the following observation.

Theorem 19. *Let n be a positive integer. The following statements hold.*

1. *The symmetric Werner–Holevo channel Φ_0 has mixed-unitary rank equal to $\binom{n+1}{2}$ if and only if there exists an orthogonal basis of S_n consisting of only unitary matrices.*

2. *Suppose n is even. The anti-symmetric Werner–Holevo channel Φ_1 has mixed-unitary rank equal to $\binom{n}{2}$ if and only if there exists an orthogonal basis of K_n consisting of only unitary matrices.*

Proof. We prove statement (1). The proof of statement (2) is analogous. Suppose there exist unitary matrices $U_1, \ldots, U_{n(n+1)/2} \subset \mathcal{U}_n$ and a probability vector $(p_1, \ldots, p_{n(n+1)/2})$ satisfying

$$\Phi_0(X) = \sum_{k=1}^{\frac{n(n+1)}{2}} p_k U_k X U_k^* \tag{122}$$

for each $X \in \mathcal{M}_n$. It holds that

$$\Pi_0 = \frac{n+1}{2} J(\Phi_0) = \sum_{k=1}^{\frac{n(n+1)}{2}} \frac{n+1}{2} p_k \, \mathrm{vec}(U_k) \, \mathrm{vec}(U_k)^*. \tag{123}$$

It follows that $p_k = 2/n(n+1)$ for each $k \in \{1, \ldots, n(n+1)/2\}$ and that the collection of unitary matrices $\{U_1, \ldots, U_{n(n+1)/2}\} \subset \mathcal{U}_n$ is an orthogonal basis for S_n. The reverse implication is immediate. $\qquad\square$

The remainder of this section is dedicated to constructing mixed-unitary decompositions of the Werner–Holevo channels. We will introduce the following notation. For each positive integer n, the space of matrices $\mathcal{M}_n$ is spanned by the collection of Hermitian matrices

$$\{H_{j,k} \,:\, j, k \in \{1, \ldots, n\}\} \tag{124}$$

24

defined by

$$H_{j,k} = \begin{cases} E_{j,j} & \text{if } j = k \\ \frac{1}{\sqrt{2}}(E_{j,k} + E_{k,j}) & \text{if } j < k \\ \frac{1}{\sqrt{2}}(iE_{j,k} - iE_{k,j}) & \text{if } j > k \end{cases} \qquad (125)$$

for each pair of indices $j, k \in \{1, \ldots, n\}$. It may be easily verified that the action of the Werner–Holevo channels can be given by

$$\Phi_0(X) = \frac{2}{n+1} \sum_{1 \leq j \leq k \leq n} H_{j,k} X H_{j,k} \qquad \text{and} \qquad \Phi_1(X) = \frac{2}{n-1} \sum_{1 \leq k < j \leq n} H_{j,k} X H_{j,k} \qquad (126)$$

for each $X \in \mathcal{M}_n$. The construction of the mixed-unitary decompositions of the Werner–Holevo channels presented in the following will make use of the fact that the complete graph on n vertices can be partitioned into $n-1$ disjoint perfect matchings for all even integers n (see [HR85]).

Mixed-unitary rank of anti-symmetric Werner–Holevo channel

For odd integers n, the anti-symmetric Werner–Holevo channel Φ_1 is not mixed unitary. Here we show that, for even integers n, the anti-symmetric Werner–Holevo channel has mixed-unitary rank equal to its Choi rank.

Theorem 20. *For each even positive integer n, the anti-symmetric Werner–Holevo channel Φ_1 is mixed unitary with mixed-unitary rank equal to* $\text{rank}(J(\Phi_1)) = n(n-1)/2$.

Proof. Consider the complete graph of n vertices with vertices labelled $\{1, \ldots, n\}$. The edge set of this graph may be identified with the set

$$\mathcal{E} = \{H_{j,k} : j, k \in \{1, \ldots, n\} \text{ with } k < j\}, \qquad (127)$$

where, for each $j, k \in \{1, \ldots, n\}$ with $k < j$, the matrix $H_{j,k}$ represents the edge connecting vertices j and k. The edge set of this graph may be partitioned into $n-1$ disjoint perfect matchings $\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}$ such that

$$\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \cdots \cup \mathcal{E}_{n-1}. \qquad (128)$$

For each $\ell \in \{1, \ldots, n-1\}$, we may label the $n/2$ elements of the perfect matching $\mathcal{E}_\ell$ as

$$\mathcal{E}_\ell = \{F_{\ell,1}, \ldots, F_{\ell,n/2}\} \qquad (129)$$

such that the matrix $F_{\ell,1} + \cdots + F_{\ell,n/2}$ has exactly one nonzero entry in each row and column. Setting $\zeta = \exp(2\pi i / n)$, we may define the matrices

$$U_{\ell,a} = \sqrt{2} \sum_{b=1}^{\frac{n}{2}} \zeta^{2ab} F_{\ell,b} \qquad (130)$$

for each pair of indices $\ell \in \{1, \ldots, n-1\}$ and $a \in \{1, \ldots, n/2\}$. It may be verified that each of the matrices $U_{\ell,a}$ is unitary, as each such matrix has exactly one nonzero entry in each row and

25

column where each nonzero entry has modulus 1. Now, for each $X \in \mathcal{M}_n$ one has

$$
\begin{aligned}
\frac{2}{n(n-1)} \sum_{\ell=1}^{n-1} \sum_{a=1}^{\frac{n}{2}} U_{\ell,a} X U_{\ell,a}^* &= \frac{2}{n(n-1)} \sum_{\ell=1}^{n-1} \sum_{a=1}^{\frac{n}{2}} \sum_{b,c=1}^{\frac{n}{2}} 2 \zeta^{2a(b-c)} F_{\ell,b} X F_{\ell,c}^* \\
&= \frac{2}{n-1} \sum_{\ell=1}^{n-1} \sum_{b=1}^{\frac{n}{2}} F_{\ell,b} X F_{\ell,b}^* \\
&= \frac{2}{n-1} \sum_{1 \le k < j \le n} H_{j,k} X H_{j,k} = \Phi_1(X),
\end{aligned}
\tag{131}
$$

and thus Φ_1 can be expressed as the average of $\mathrm{rank}(\Phi_1) = n(n-1)/2$ unitary channels. It follows that Φ_1 is mixed unitary with mixed-unitary rank equal to $n(n-1)/2$. $\qquad\square$

Mixed-unitary rank of symmetric Werner–Holevo channel

Symmetric Werner–Holevo channel for even n

For even integers n, the proof that the symmetric Werner–Holevo channel Φ_0 has minimal mixed-unitary rank is analogous to the proof for the anti-symmetric version.

Theorem 21. *For each positive even integer n, the symmetric Werner–Holevo channel Φ_0 is mixed unitary with mixed-unitary rank equal to* $\mathrm{rank}(J(\Phi_0)) = n(n+1)/2$.

Proof. The proof is similar to the proof of Theorem 20. As before, consider the complete graph of n vertices with vertices labelled $\{1, \ldots, n\}$, but here we identify the edge set of the graph with the collection of matrices

$$
\mathcal{E} = \{H_{j,k} : j, k \in \{1, \ldots, n\} \text{ with } j < k\},
\tag{132}
$$

where, for each $j, k \in \{1, \ldots, n\}$ with $j < k$, the matrix $H_{j,k}$ represents the edge connecting vertices k and j. The edge set of this graph may be partitioned into $n-1$ disjoint perfect matchings $\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}$ such that $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \cdots \cup \mathcal{E}_{n-1}$. For each $\ell \in \{1, \ldots, n-1\}$, we may label the $n/2$ elements of the perfect matching $\mathcal{E}_\ell$ as $\mathcal{E}_\ell = \{F_{\ell,1}, \ldots, F_{\ell,n/2}\}$. Setting $\zeta = \exp(2\pi i/n)$, we may define the matrices

$$
U_{\ell,a} = \sqrt{2} \sum_{b=1}^{\frac{n}{2}} \zeta^{2ab} F_{\ell,b}
\tag{133}
$$

for each pair of indices $\ell \in \{1, \ldots, n-1\}$ and $a \in \{1, \ldots, n/2\}$, and define the matrices

$$
V_j = \sum_{k=1}^{n} \zeta^{jk} H_{k,k}
\tag{134}
$$

for each $j \in \{1, \ldots, n\}$. It may be verified that each of the matrices $U_{\ell,a}$ and V_j is unitary. Analo-

gous to the proof of Theorem 20, for each $X \in \mathcal{M}_n$ it holds that

$$\frac{2}{n(n+1)} \sum_{\ell=1}^{n-1} \sum_{a=1}^{\frac{n}{2}} U_{\ell,a} X U_{\ell,a}^* = \frac{2}{n(n+1)} \sum_{\ell=1}^{n-1} \sum_{a=1}^{\frac{n}{2}} \sum_{b,c=1}^{\frac{n}{2}} 2\, \zeta^{2a(b-c)} F_{\ell,b} X F_{\ell,c}^*$$

$$= \frac{2}{n+1} \sum_{\ell=1}^{n-1} \sum_{b=1}^{\frac{n}{2}} F_{\ell,b} X F_{\ell,b}^*$$

$$= \frac{2}{n+1} \sum_{1 \le k < j \le n} H_{j,k} X H_{j,k}. \tag{135}$$

One also has that

$$\frac{2}{n(n+1)} \sum_{j=1}^{n} V_j X V_j^* = \frac{2}{n(n+1)} \sum_{j,k,\ell=1}^{n} \zeta^{j(k-\ell)} H_{k,k} X H_{\ell,\ell}$$

$$= \frac{2}{n+1} \sum_{k=1}^{n} H_{k,k} X H_{k,k} \tag{136}$$

for each $X \in \mathcal{M}_n$. Putting together the results of (135) and (136), we see that

$$\frac{2}{n(n+1)} \left(\sum_{\ell=1}^{n-1} \sum_{a=1}^{\frac{n}{2}} U_{\ell,a} X U_{\ell,a}^* + \sum_{j=1}^{n} V_j X V_j^* \right) = \frac{2}{n+1} \sum_{1 \le j \le k \le n} H_{j,k} X H_{j,k} \tag{137}$$

$$= \Phi_0(X)$$

holds for each $X \in \mathcal{M}_n$. As Φ_0 is written as the average of $n(n+1)/2$ unitary channels, it follows that Φ_1 is mixed unitary with mixed-unitary rank equal to $n(n+1)/2$. □

Symmetric Werner–Holevo channel for odd n

For odd n, we will show that Φ_0 has mixed-unitary rank at most $n(n+3)/2$.

Theorem 22. *For each odd positive integer n, the symmetric Werner–Holevo channel Φ_0 has mixed-unitary rank at most $n(n+3)/2$.*

Proof. The proof is similar to the proofs of Theorems 20 and 21. Now however, consider the complete graph of $n+1$ vertices with vertices labelled $\{0, 1, \ldots, n\}$, and identify the edge set of this graph with the collection of matrices defined as

$$\mathcal{E} = \{H_{j,k} : j, k \in \{0, 1, \ldots, n\} \text{ with } j < k\}, \tag{138}$$

where we define $H_{0,k} = H_{k,k}/\sqrt{2}$ for each $k \in \{1, \ldots, n\}$. As before, this edge set may be partitioned into n disjoint perfect matchings $\mathcal{E}_1, \ldots, \mathcal{E}_n$ such that $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \cdots \cup \mathcal{E}_n$. For each $\ell \in \{1, \ldots, n\}$, we may label the $(n+1)/2$ elements of the perfect matching $\mathcal{E}_\ell$ as $\mathcal{E}_\ell = \{F_{\ell,1}, \ldots, F_{\ell,(n+1)/2}\}$. Setting $\zeta = \exp(2\pi i/(n+1))$, we may define the matrices

$$U_{\ell,a} = \sqrt{2} \sum_{b=1}^{\frac{n+1}{2}} \zeta^{2ab} F_{\ell,b} \tag{139}$$

27

for each pair of indices $\ell \in \{1, \ldots, n\}$ and $a \in \{1, \ldots, (n+1)/2\}$, and the matrices

$$V_j = \sum_{k=1}^{n} e^{i2\pi/n} H_{k,k} \tag{140}$$

for each index $j \in \{1, \ldots, n\}$. It may be verified that each of the matrices $U_{\ell,a}$ and V_j is unitary. Analogous to the proofs of Theorems 20 and 21, one has

$$\frac{1}{n+1} \sum_{\ell=1}^{n} \sum_{a=1}^{\frac{n+1}{2}} U_{\ell,a} X U_{\ell,a}^* = \frac{1}{n+1} \sum_{\ell=1}^{n} \sum_{a=1}^{\frac{n+1}{2}} \sum_{b,c=1}^{\frac{n+1}{2}} 2\, \zeta^{2a(b-c)} F_{\ell,b} X F_{\ell,c}^*$$

$$= \sum_{0 \leq j < k \leq n} H_{j,k} X H_{j,k}$$

$$= \sum_{1 \leq j < k \leq n} H_{j,k} X H_{j,k} + \frac{1}{2} \sum_{j=1}^{n} H_{j,j} X H_{j,j} \tag{141}$$

and

$$\frac{1}{2n} \sum_{j=1}^{n} V_j X V_j^* = \frac{1}{2} \sum_{j=1}^{n} H_{j,j} X H_{j,j} \tag{142}$$

for each $X \in \mathcal{M}_n$. Putting together the results of (141) and (142), we see that

$$\Phi_0(X) = \frac{2}{n+1} \left(\frac{1}{n+1} \sum_{\ell=1}^{n} \sum_{a=1}^{\frac{n+1}{2}} U_{\ell,a} X U_{\ell,a}^* + \frac{1}{2n} \sum_{j=1}^{n} V_j X V_j^* \right) \tag{143}$$

holds for each $X \in \mathcal{M}_n$ and thus Φ_0 can be expressed as a convex combination of $n(n+1)/2 + n = n(n+3)/2$ unitary channels. $\qquad \square$

While Theorems 20 and 21 indicate that the symmetric and anti-symmetric Werner–Holevo channels have minimal mixed-unitary rank for all even integers n, Theorem 22 only gives an upper bound on the mixed-unitary rank of the symmetric Werner–Holevo channel Φ_1 for odd n. As it must be the case that the mixed-unitary rank of a channel is at least equal to its rank, the mixed-unitary rank N of Φ_1 for odd n is therefore bounded by

$$\frac{n(n+1)}{2} \leq N \leq \frac{n(n+3)}{2}. \tag{144}$$

It would be interesting if it turned out that Φ_1 were to have minimal mixed-unitary rank for every positive integer n. As the Choi representation of the symmetric Werner–Holevo channel is proportional to the projection matrix onto the symmetric subspace of $\mathbb{C}^n \otimes \mathbb{C}^n$,

$$J(\Phi_0) = \frac{2}{n+1} \Pi_0, \tag{145}$$

finding a minimal mixed-unitary decomposition of Φ_0 for an integer n amounts to finding an orthogonal collection of $n(n+1)/2$ unitary matrices $\{U_1, \ldots, U_{n(n+1)/2}\} \subset \mathcal{U}_n$ such that each U_k is symmetric in the sense that $U_k^{\mathsf{T}} = U_k$. If such a collection could be found, it would satisfy

$$\Pi_0 = \frac{1}{n} \sum_{k=1}^{\frac{n(n+1)}{2}} \operatorname{vec} U_k \operatorname{vec}(U_k)^*, \tag{146}$$

as $\text{rank}(\Pi_0) = n(n+1)/2$. In the case when $n = 3$, it turns out that Φ_0 indeed has minimal mixed-unitary rank, as will be shown in Theorem 23 by explicitly constructing a mixed-unitary decomposition.

Theorem 23. *Let $\Phi_0 : \mathcal{M}_3 \to \mathcal{M}_3$ be the symmetric Werner–Holevo channel on $\mathcal{M}_3$. It holds that Φ_0 has mixed-unitary rank equal to 6 and thus has minimal mixed-unitary rank.*

Proof. It is evident that the Choi rank of Φ_0 is equal to $\text{rank}(J(\Phi_0)) = 6$. Define α and ζ as

$$\alpha = \frac{3}{8} + i\frac{\sqrt{15}}{8} \qquad \text{and} \qquad \zeta = \exp(2\pi i/3) \tag{147}$$

and define unitary matrices $U_1, U_2, U_3, U_4, U_5, U_6 \in \mathcal{U}_3$ as

$$U_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \end{pmatrix} \qquad U_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix} \qquad U_3 = \begin{pmatrix} \frac{1}{2} & -\alpha & -\alpha \\ -\alpha & \frac{1}{2} & -\alpha \\ -\alpha & -\alpha & \frac{1}{2} \end{pmatrix}$$

$$U_4 = \begin{pmatrix} \frac{1}{2} & \alpha & -\alpha \\ \alpha & \frac{1}{2} & \alpha \\ -\alpha & \alpha & \frac{1}{2} \end{pmatrix} \qquad U_5 = \begin{pmatrix} \frac{1}{2} & \alpha & \alpha \\ \alpha & \frac{1}{2} & -\alpha \\ \alpha & -\alpha & \frac{1}{2} \end{pmatrix} \qquad U_6 = \begin{pmatrix} \frac{1}{2} & -\alpha & \alpha \\ -\alpha & \frac{1}{2} & \alpha \\ \alpha & \alpha & \frac{1}{2} \end{pmatrix}. \tag{148}$$

It may be verified that the matrices $U_1, \dots, U_6$ are symmetric, unitary, and pairwise orthogonal. Hence, $\{U_1, \dots, U_6\}$ is an orthogonal collection of 6 symmetric unitary matrices in $\mathcal{U}_3$. Comparing this fact with the result of Theorem 19 completes the proof. $\square$

The construction for the mixed-unitary decomposition of Φ_0 for $n = 3$ presented in the proof of Theorem 23 does not appear to generalize for odd integers $n \geq 5$. Nevertheless, numerical evidence seems to suggest that a minimal mixed-unitary decomposition of Φ_0 might be found for every positive integer. A proof of the conjecture that Φ_0 has minimal mixed-unitary rank for every positive integer n would be interesting to pursue.

Acknowledgements

A. A characterization of Schur channels

Two channels $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ and $\Psi : \mathcal{M}_n \to \mathcal{M}_n$ are said to be *unitarily equivalent* if there exist unitary matrices $U, V \in \mathcal{U}_n$ satisfying

$$\Psi(X) = U\Phi(VXV^*)U^* \tag{149}$$

for each $X \in \mathcal{M}_n$. In this appendix we provide necessary and sufficient conditions that characterize when a channel is unitarily equivalent to a Schur channel in terms of the channel's operator system. We conclude from this characterization that the channels in Examples 10 and 11 are not equivalent to Schur channels.

It is known that a channel is a Schur map if and only if every Kraus representation for the channel consists of only diagonal matrices. The following lemma provides another useful characterization for Schur channels.

Lemma 24. *A channel* $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ *is a Schur map if and only if* $\Phi(D) = D$ *holds for each diagonal matrix* $D \in \mathcal{M}_n$.

Proof. If $\Phi(D) = D$ holds for each diagonal matrix $D \in \mathcal{M}_n$, then each Kraus matrix of Φ must commute with each diagonal matrix, and thus each Kraus matrix must itself be diagonal. On the other hand, if Φ is a Schur map then there is a correlation matrix $C \in \mathcal{M}_n$ satisfying $\Phi(X) = C \odot X$ for each $X \in \mathcal{M}_n$. As each diagonal entry of C must be equal to one, it holds that $\Phi(D) = D$ for each diagonal matrix $D \in \mathcal{M}_n$. $\square$

We now provide a necessary and sufficient condition for characterizing when a map is unitarily equivalent to a Schur map in terms of the operator system of the channel.

Theorem 25. *Let* $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ *be a channel. The following statements are equivalent.*

1. *The channel* Φ *is unitarily equivalent to a Schur map.*

2. *The operator system* $\mathcal{S}_\Phi$ *is a commuting family of matrices.*

Proof. Let $A_1, \ldots, A_N \in \mathcal{M}_n$ be linear matrices satisfying

$$\Phi(X) = \sum_{k=1}^{N} A_k X A_k^* \tag{150}$$

for each $X \in \mathcal{M}_n$. First suppose that Φ is unitarily equivalent to a Schur map. There exist unitary matrices $U, V \in \mathcal{U}_n$ such that the channel $\Psi : \mathcal{M}_n \to \mathcal{M}_n$ defined as $\Psi(X) = U\Phi(VXV^*)U^*$ is a Schur map. The channel Ψ has a Kraus representation of the form

$$\Psi(X) = \sum_{j=1}^{N} (UA_jV)X(UA_jV)^* \tag{151}$$

and thus UA_kV is a diagonal matrix for each $k \in \{1, \ldots, N\}$. Moreover, each of the matrices in the collection
$$V^*\mathcal{S}_\Phi V = \mathrm{span}\{V^*A_j^*U^*UA_kV : j,k \in \{1, \ldots, N\}\} \tag{152}$$
is also diagonal. It follows that $\mathcal{S}_\Phi$ is a commuting family of normal matrices in $\mathcal{M}_n$.

For the other direction, suppose that $\mathcal{S}_\Phi$ is a commuting family. As $\mathcal{S}_\Phi$ is self-adjoint, each matrix in $\mathcal{S}_\Phi$ is also normal. There exists a unitary matrix $V \in \mathcal{U}_n$ such that $V^*A_j^*A_kV$ is a diagonal matrix for each pair of indices $j, k \in \{1, \ldots, N\}$. For any two diagonal matrices $D_0, D_1 \in \mathcal{M}_n$, one

has that

$$\Phi(VD_0V^*)\Phi(VD_1V^*) = \sum_{j,k=1}^{N} A_j VD_0(V^*A_j^*A_kV)D_1V^*A_k^*$$

$$= \sum_{j,k=1}^{N} A_j VD_0D_1(V^*A_j^*A_kV)V^*A_k^* \qquad (153)$$

$$= \Phi(VD_0D_1V^*)\Phi(\mathbb{1}_n)$$

as each of the matrices in $\{V^*A_j^*A_kV : j,k \in \{1,\dots,N\}\}$ is diagonal and commutes with the diagonal matrices D_0 and D_1. Define matrices $P_1,\dots,P_n \in \mathcal{M}_n$ as

$$P_k = \Phi(VE_{k,k}V^*) \qquad (154)$$

for each $k \in \{1,\dots,n\}$. For indices $j,k \in \{1,\dots,n\}$ with $j \neq k$, one has that

$$P_jP_k = \Phi(VE_{j,j}E_{k,k}V^*)\Phi(\mathbb{1}_n) = 0 \qquad (155)$$

as $E_{j,j}E_{k,k} = 0$. Moreover, it holds that $\mathrm{Tr}(P_k) = \mathrm{Tr}(E_{k,k}) = 1$ and that P_k is positive for each $k \in \{1,\dots,n\}$ as Φ is a quantum channel. The collection $\{P_1,\dots,P_n\} \subset \mathcal{M}_n$ is therefore an orthogonal set of positive matrices each with trace equal to 1. Hence there must exist a unitary matrix $U \in \mathcal{U}_n$ such that $UP_jU^* = E_{j,j}$ for each $j \in \{1,\dots,n\}$. Define a channel $\Psi : \mathcal{M}_n \to \mathcal{M}_n$ as

$$\Psi(X) = U\Phi(VXV^*)U^* \qquad (156)$$

for each $X \in \mathcal{M}_n$. From the observations above, one finds that $\Psi(E_{k,k}) = E_{k,k}$ for each $k \in \{1,\dots,n\}$, and thus $\Psi(D) = D$ for each diagonal matrix $D \in \mathcal{M}_n$. It follows that Ψ is a Schur map by Lemma 24. This completes the proof. $\qquad\square$

Remark. Every unital quantum channel with Choi rank at most 2 is unitarily equivalent to a Schur map. This fact was proven in [LS93], but we remark that another proof of this fact can be found by making use of Theorem 25. Indeed, let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a unital quantum channel for some positive integer n such that $\mathrm{rank}(J(\Phi)) \leq 2$. There exist matrices $A_0, A_1 \in \mathcal{M}_n$ such that

$$\Phi(X) = A_0XA_0^* + A_1XA_1^* \qquad (157)$$

is a Kraus representation of Φ. As Φ is unital and trace preserving, these matrices must satisfy $A_0^*A_0 + A_1^*A_1 = \mathbb{1}_n$ and $A_0A_0^* + A_1A_1^* = \mathbb{1}_n$. The operator system of Φ may be given by $\mathcal{S}_\Phi = \mathrm{span}\{A_0^*A_0, A_0^*A_1, A_1^*A_0, A_1^*A_1\}$, and it is straightforward to verify that each of these matrices commute with one another:

$$\begin{aligned}
(A_0^*A_0)(A_0^*A_1) &= A_0^*(\mathbb{1} - A_1A_1^*)A_1 = A_0^*A_1(\mathbb{1} - A_1^*A_1) = (A_0^*A_1)(A_0^*A_0), \\
(A_0^*A_0)(A_1^*A_0) &= (\mathbb{1} - A_1^*A_1)A_1^*A_0 = A_1^*(\mathbb{1} - A_1A_1^*)A_0 = (A_1^*A_0)(A_0^*A_0), \\
(A_1^*A_1)(A_0^*A_1) &= (\mathbb{1} - A_0^*A_0)A_0^*A_1 = A_0^*(\mathbb{1} - A_0A_0^*)A_1 = A_0^*A_1A_1^*A_1, \\
(A_1^*A_1)(A_1^*A_0) &= A_1^*(\mathbb{1} - A_0A_0^*)A_0 = A_1^*A_0(\mathbb{1} - A_0^*A_0) = A_1^*A_0A_1^*A_1, \\
(A_0^*A_0)(A_1^*A_1) &= (\mathbb{1} - A_1^*A_1)(\mathbb{1} - A_0^*A_0) = \mathbb{1} - A_0^*A_0 - A_1^*A_1 + A_1^*A_1A_0^*A_0 \\
&= (A_1^*A_1)(A_0^*A_0), \\
(A_0^*A_1)(A_1^*A_0) &= A_0^*(\mathbb{1} - A_0A_0^*)A_0 = A_0^*A_0(\mathbb{1} - A_0^*A_0) = (\mathbb{1} - A_1^*A_1)A_1^*A_1 \\
&= A_1^*(\mathbb{1} - A_1A_1^*)A_1 = (A_1^*A_0)(A_0^*A_1).
\end{aligned} \qquad (158)$$

References

[AMTdW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[AS04] Andris Ambainis and Adam Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 249–260. Springer Berlin Heidelberg, 2004.

[AS08] Koenraad Audenaert and Stefan Scheel. On random unitary channels. *New Journal of Physics*, 10:1–11, 2008.

[AU82] Peter Alberti and Armin Uhlmann. *Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing*, volume 9 of *Mathematics and Its Applications*. D. Reidel Publishing Company, 1982.

[BASTS08] Avraham Ben-Aroya, Oded Schwartz, and Amnon Ta-Shma. Quantum expanders: Motivation and constructions. In *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity*, pages 292–303, 2008.

[BDSW96] Charles H. Bennett, David P. DiVincenzo, John Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996.

[Bus06] Francesco Buscemi. On the minimum number of unitaries needed to describe a random-unitary channel. *Physics Letters A*, 360(2):256–258, 2006.

[Cho75] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10(3):285–290, 1975.

[Con99] John Conway. *A Course in Operator Theory*, volume 21 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, Rhode Island, 1999.

[DCEL09] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80(1):012304, 2009.

[DEBŻ10] Thomas Durt, Berthold Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International Journal on Quantum Information*, 8(4):535–640, 2010.

[DLT01] David DiVincenzo, Debbie Leung, and Barbara Terhal. Data hiding with classical communication. *IEEE Transactions on Information Theory*, 48:580, 2001.

[DSW13] Runyao Duan, Simone Severini, and Andreas Winter. Zero-error communication via quantum channels, noncommutative graphs, and a quantum Lovász number. *IEEE Transactions on Information Theory*, 59(2):1164–1174, 2013.

[GB02]   Leonid Gurvits and Howard Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Physical Review A*, 66(6):062311, 2002.

[Gha10]   Sevag Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information & Computation*, 10(3):343–360, 2010.

[Gur03]   Leonid Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, pages 10–19. ACM, 2003.

[GW03]   Matteo Gregoratti and Reinhard Werner. Quantum lost and found. *Journal of Modern Optics*, 50(67):915–933, 2003.

[HJ94]   Roger Horn and Charles Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1994.

[HLSW04]   Patrick Hayden, Debbie Leung, Peter Shor, and Andreas Winter. Randomizing quantum states: constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004.

[HM11]   Uffe Haagerup and Magdalena Musat. Factorization and dilation problems for completely positive maps on von Neumann algebras. *Communications in Mathematical Physics*, 303(2):555–594, 2011.

[HR85]   Alan Hartman and Alexander Rosa. Cyclic one-factorization of the complete graph. *European Journal on Combinatorics*, 6(1):45–48, 1985.

[Ioa07]   Lawrence Ioannou. Computational complexity of the quantum separability problem. *Quantum Information & Computation*, 7(4):335–370, 2007.

[Ivo81]   I D Ivonovic. Geometrical description of quantal state determination. *Journal of Physics A*, 14(12):3241–3245, 1981.

[LS93]   Lawrence Landau and Raymond Streater. On Birkhoff's theorem for doubly stochastic completely positive maps of matrix algebras. *Linear Algebra and Its Applications*, 193(C):107–127, 1993.

[LT94]   Chi-Kwong Li and Bit-Shun Tam. A note on extreme correlation matrices. *SIAM Journal on Matrix Analysis and Applications*, 15(3):903–908, 1994.

[LW19]   Colin Lee and John Watrous. Detecting mixed-unitary quantum channels is NP-hard. Available from arXiv.org as e-Print 1902.03164, 2019.

[MHR17]   Alexander Müller-Hermes and David Reeb. Monotonicity of the quantum relative entropy under positive maps. *Annales Henri Poincaré*, 18(5):1777–1788, 2017.

[MW09]   Christian Mendl and Michael Wolf. Unital quantum channels – convex structure and revivals of Birkhoff's theorem. *Communications in Mathematical Physics*, 289(3):1057–1086, 2009.

[NC00]   Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Nie99]   Michael Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83(2):436–439, 1999.

[Pau86]   Vern Paulsen. *Completely Bounded Maps and Dilations*. Longman Scientific & Technical, Essex, 1986.

[Pau03]   Vern Paulsen. *Completely Bounded Maps and Operator Algebras*. Cambridge University Press, 2003.

[Ros08]   Bill Rosgen. Additivity and distinguishability of random unitary channels. *Journal of Mathematical Physics*, 49(10):102107, 2008.

[SVW05]   John Smolin, Frank Verstraete, and Andreas Winter. Entanglement of assistance and multipartite state distillation. *Physical Review A*, 72(5):052317, 2005.

[Tre86]   Semion Tregub. Bistochastic operators on finite-dimensional von Neumann algebras. *Izvestiya Vysshikh Uchebnykh Zavedenii. Matematika*, 30(3):75–55, 1986.

[Wat09]   John Watrous. Mixing doubly stochastic quantum channels with the completely depolarizing channel. *Quantum Information and Computation*, 9(5&6):403–413, 2009.

[Wat18]   John Watrous. *Theory of Quantum Information*. Cambridge University Press, 2018.

[WF89]   William Wootters and Brian Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.

[Wil17]   Mark Wilde. *Quantum Information Theory*. Cambridge University Press, second edition, 2017.

[ŻHSL98]   Karol Życzkowski, Paweł Horodecki, Anna Sanpera, and Maciej Lewenstein. Volume of the set of separable states. *Physical Review A*, 58(2):883–892, 1998.