



HAL
open science

Operator algebra generalization of a theorem of Watrous and mixed unitary quantum channels

David Kribs, Jeremy Levick, Rajesh Pereira, Mizanur Rahaman

► **To cite this version:**

David Kribs, Jeremy Levick, Rajesh Pereira, Mizanur Rahaman. Operator algebra generalization of a theorem of Watrous and mixed unitary quantum channels. *Journal of Physics A: Mathematical and Theoretical*, 2024, 57, pp.115303. 10.1088/1751-8121/ad2cb0 . hal-04390457

HAL Id: hal-04390457

<https://hal.science/hal-04390457v1>

Submitted on 22 Oct 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

PAPER • OPEN ACCESS

Operator algebra generalization of a theorem of Watrous and mixed unitary quantum channels

To cite this article: David W Kribs *et al* 2024 *J. Phys. A: Math. Theor.* **57** 115303

View the [article online](#) for updates and enhancements.

You may also like

- [On the uniqueness of the steady-state solution of the Lindblad–Gorini–Kossakowski–Sudarshan equation](#)
Davide Nigro
- [Conformal field theory, tensor categories and operator algebras](#)
Yasuyuki Kawahigashi
- [A quantum extended Kalman filter](#)
Muhammad F Emzir, Matthew J Woolley and Ian R Petersen

Operator algebra generalization of a theorem of Watrous and mixed unitary quantum channels

David W Kribs^{1,*} , Jeremy Levick¹, Rajesh Pereira¹ 
and Mizanur Rahaman² 

¹ Department of Mathematics & Statistics, University of Guelph, Guelph N1G 2W1, ON, Canada

² Univ Lyon, ENS Lyon, UCBL, CNRS, Inria, LIP, F-69342 Lyon Cedex 07, France

E-mail: dkribs@uoguelph.ca, jerlevick@gmail.com, pereirar@uoguelph.ca and mizanur.rahaman@ens-lyon.fr

Received 11 November 2023; revised 5 February 2024

Accepted for publication 23 February 2024

Published 7 March 2024



CrossMark

Abstract

We establish an operator algebra generalization of Watrous' theorem (Watrous 2009 *Quantum Inf. Comput.* **9** 403–413) on mixing unital quantum channels (completely positive trace-preserving maps) with the completely depolarizing channel, wherein the more general objects of focus become (finite-dimensional) von Neumann algebras, the unique trace preserving conditional expectation onto the algebra, the group of unitary operators in the commutant of the algebra, and the fixed point algebra of the channel. As an application, we obtain a result on the asymptotic theory of quantum channels, showing that all unital channels are eventually mixed unitary. We also discuss the special case of the diagonal algebra in detail, and draw connections to the theory of correlation matrices and Schur product maps.

Keywords: quantum channel, mixed unitary channel, von Neumann algebra, conditional expectation, unital quantum channel, fixed point set, commutant

* Author to whom any correspondence should be addressed.



Original Content from this work may be used under the terms of the [Creative Commons Attribution 4.0 licence](https://creativecommons.org/licenses/by/4.0/). Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

1. Introduction

Quantum channels, which are mathematically described by completely positive trace-preserving maps, are central objects of study in quantum information theory [16, 27, 29, 37]. The class of unital (or doubly bistochastic) channels is a class of particular interest, and amongst such channels the subclass of mixed unitary channels arise in almost every area of quantum information theory (see [3, 11, 12, 17, 21, 24] as entrance points into the corresponding literature). Hence a basic topic in the theory of quantum channels and their applications is the determination of when or how close a unital channel is to being mixed unitary. A fundamental result in this direction is a theorem of Watrous [36], which shows that any unital channel that is properly averaged with the ‘completely depolarizing channel’, the map that sends all quantum states to the maximally mixed state, can be written as a mixed unitary channel.

In this paper, we obtain a generalization of Watrous’ Theorem to the setting of operator algebras. The more general objects of focus become (finite-dimensional) von Neumann algebras, the unique trace preserving conditional expectation onto the algebra, the group of unitary operators in the commutant of the algebra, and the fixed point algebra of the channel. The original theorem is recovered when applied to the special case of the (trivial) scalar algebra, wherein the completely depolarizing channel is viewed as the conditional expectation onto the algebra. Our proof is necessarily more intricate, requiring a number of supporting results that may be of independent interest. As an application, we obtain a result on the asymptotic theory of quantum channels, and we show that all unital channels are eventually mixed unitary. We first show this for primitive unital channels using the Watrous theorem, and then we prove the general result following some preparatory work on irreducible unital channels and their peripheral eigenvalue algebras before applying the theorem. Finally, the case of the diagonal algebra yields a connection with correlation matrices and Schur product maps, and we conclude by considering this case in more detail, interpreting the results in that setting and providing alternative viewpoints of the main theorem.

This paper is organized as follows. The next section includes requisite preliminary notions, and we motivate and formulate the main theorem statement. Section 3 includes the proof of the theorem, section 4 derives the application discussed above, and section 5 gives the detailed treatment of the diagonal algebra case.

2. Background

We begin by recalling basic preliminary notions, and then we formulate our main theorem.

2.1. Preliminaries

Given a positive integer $d \geq 1$, we let M_d denote the set of $d \times d$ complex matrices. The matrix units E_{ij} , for $1 \leq i, j \leq d$, are the elements of M_d with a 1 in the i, j entry and 0’s elsewhere. The (Hilbert-Schmidt) trace inner product on M_d is given by $\langle A, B \rangle = \text{Tr}(B^*A)$. The tensor product algebra $M_d \otimes M_d$ is naturally identified with M_{d^2} and has matrix units $E_{ij} \otimes E_{kl}$. We will make use of the linear map $\text{vec} : M_d \rightarrow \mathbb{C}^d \otimes \mathbb{C}^d$ defined by $\text{vec}(E_{ij}) = e_i \otimes e_j$, where $\{e_1, \dots, e_d\}$ is the standard basis for \mathbb{C}^d .

We will be interested in completely positive maps $\Phi : M_d \rightarrow M_d$ [29], which can always be represented in operator-sum form $\Phi(X) = \sum_i K_i X K_i^*$ for some set of ‘Kraus’ operators $K_i \in M_d$ [19]. Each map defines a dual map via the trace inner product, wherein the roles of the operators K_i and K_i^* are reversed in the operator-sum form. The map Φ is unital if $\Phi(I) = I$,

where I is the identity matrix. If it is trace-preserving, which occurs exactly when $\sum_i K_i^* K_i = I$, then the map is called a *quantum channel* [16, 27, 37]. The class of unital (quantum) channels are pervasive in quantum information, and we define an important subclass below. Note that a channel is unital if and only its dual map is a unital channel as well.

The ‘Choi matrix’ [8] for Φ is the matrix $J(\Phi) \in M_d \otimes M_d$ given by,

$$J(\Phi) = \sum_{i,j=1}^d E_{ij} \otimes \Phi(E_{ij}). \tag{1}$$

It is a positive semi-definite matrix if and only if Φ is a completely positive map. The map $J(\cdot)$ is linear, and we note that $J(\Phi) = \sum_i \text{vec}(K_i) \text{vec}(K_i)^*$ when the K_i are Kraus operators for Φ [37].

In this paper, by an *operator algebra* we will mean a von Neumann algebra (or C^* -algebra) on finite-dimensional Hilbert space, which, up to unitarily equivalence [9], is a set of matrices contained inside some M_d of the form:

$$\mathcal{A} = \oplus_k (I_{m_k} \otimes M_{n_k}), \tag{2}$$

for some unique choice of positive integers m_k, n_k . The algebras we consider will typically be the fixed point sets of unital channels, and so necessarily will be unital ($I \in \mathcal{A}$), which means that $\sum_k m_k n_k = d$. The commutant \mathcal{A}' of \mathcal{A} , which is the set of all matrices in M_d that commute with every element of \mathcal{A} , has a corresponding form up to unitary equivalence given by $\mathcal{A}' = \oplus_k (M_{m_k} \otimes I_{n_k})$.

Given an algebra $\mathcal{A} \subseteq M_d$, we can consider *conditional expectations* onto the algebra, which are maps $\mathcal{E} : M_d \rightarrow \mathcal{A}$ such that: (1) $\mathcal{E}(A) = A$ for all $A \in \mathcal{A}$; (2) $\mathcal{E}(A_1 X A_2) = A_1 \mathcal{E}(X) A_2$ for all $A_1, A_2 \in \mathcal{A}$ and $X \in M_d$; and, (3) if $X \in M_d$ is positive semi-definite, then so is $\mathcal{E}(X)$. Every conditional expectation of M_d onto \mathcal{A} is completely positive (and is a unital map when the algebra is unital), and amongst all possible conditional expectations onto \mathcal{A} , there is a unique map that is also trace-preserving [30] (in fact, it is exactly the orthogonal projection of M_d onto \mathcal{A} in the trace inner product). So given a unital algebra $\mathcal{A} \subseteq M_d$, we shall denote the trace preserving conditional expectation onto \mathcal{A} by $\mathcal{E}_{\mathcal{A}} : M_d \rightarrow \mathcal{A}$.

The fixed point set $\text{Fix}(\Phi) = \{X \in M_d \mid \Phi(X) = X\}$ will also play a key role in our analysis. For a unital map Φ , it is easily seen that $\text{Fix}(\Phi)$ contains the commutant of the Kraus operators, and further, for a unital channel these two sets coincide $\text{Fix}(\Phi) = \{K_i\}'$, and this statement is true for any choice of Kraus operators for the channel [20]. In particular, this means the fixed point set, which in general is just an operator subspace, in the case of unital channels is an operator algebra. (Note that this really is a feature of unital channels, as even the fixed point set of a unital completely positive map need not be an algebra [5, 20].)

We shall focus on the following class of unital channels, which are important in several areas of quantum information [3, 11, 12, 17, 21, 24].

Definition 1. A completely positive linear map $\Phi : M_d \rightarrow M_d$ is called a *mixed unitary channel* if there exists a set of $d \times d$ unitary matrices $\{U_i\}_{i=1}^r$ and a set of nonnegative numbers $\{\lambda_i\}_{i=1}^r$ with $\sum_{i=1}^r \lambda_i = 1$ such that $\Phi(X) = \sum_{i=1}^r \lambda_i U_i X U_i^*$.

It is known that every single-qubit unital channel is mixed unitary, but this is not the case for higher dimensions. We note that since M_d is finite dimensional, the Minkowski–Caratheodory convexity theorem [35] implies that a completely positive linear map $\Phi : M_d \rightarrow M_d$ is mixed unitary if and only if Φ is in the convex hull of the unitary transformation maps $X \rightarrow U X U^*$.

2.2. Formulation of the conjecture

We shall establish a generalization of the following theorem of Watrous [36] to the setting of operator algebras.

Theorem 2. *Let $\Phi : M_d \rightarrow M_d$ be a unital quantum channel. Then for $0 \leq p \leq 1/(d^2 - 1)$, the convex combination of maps given by*

$$p\Phi(X) + (1-p)\frac{\text{Tr}(X)}{d}I_d \tag{3}$$

is a mixed unitary channel.

The *completely depolarizing channel* $\delta_d : M_d \rightarrow M_d$ is defined as: $\delta_d(X) = d^{-1}\text{Tr}(X)I_d$. As it is also a mixed unitary channel (implemented by any set of (uniformly scaled) unitary operators that form an orthogonal basis in the trace inner product on M_d), and the set of mixed unitary channels is convex, the theorem is proved by explicitly proving the case $p = 1/(d^2 - 1)$. That is, theorem 2 is equivalent to the statement that the convex combination $p\Phi + (1-p)\delta_d$ is mixed unitary for $p = \frac{1}{d^2-1}$.

Some initial investigation shows that a naive generalization of theorem 2 does not hold. Consider the following example, which illustrates this point.

Example 3. We have the identity map $\text{id} : M_3 \rightarrow M_3$, $\text{id}(X) = X$, and the Werner–Holevo channel [38] on M_3 given by,

$$W_3^-(X) = \frac{1}{2}[\text{Tr}(X)I_3 - X^t],$$

where X^t is the transpose of X . Now consider the channel $\Phi_p : M_3 \rightarrow M_3$ for $0 < p \leq 1$ given by,

$$\Psi_p(X) = pX + (1-p)W_3^-(X).$$

We claim that this channel is not mixed-unitary for any p . Indeed, first note that any operator-sum representation of Ψ_p will have Kraus operators of the form $K = \alpha I + A$, where A is an anti-symmetric matrix, I is the identity matrix and α is a constant. (To see this, observe that Ψ_p has a representation of this form, and then note this implies any representation has this form.) As A is a 3×3 anti-symmetric matrix, the eigenvalues are $\lambda, -\lambda, 0$. So the eigenvalues of K are $\alpha + \lambda, \alpha - \lambda, \alpha$. Now if K is a multiple of a unitary, then these eigenvalues must lie on a circle. However, these three numbers are co-linear. Hence $\lambda = 0$ and so $A = 0$. This is true for all Kraus operators and thus it follows that $p = 1$.

One might expect a naive generalization of the original Watrous Theorem to find that $t\text{id} + (1-t)\Phi$ is mixed unitary for some t , simply replacing δ_3 with the identity map id . But in fact, W_3^- is a channel for which $t\text{id} + (1-t)W_3^-$ is not mixed unitary for any $t < 1$. So, simply replacing the depolarizing channel by another unital channel immediately yields that there are channels for which no non-trivial convex combination is mixed unitary.

After some more thought, we were led to view theorem 2 as a special case of a more general phenomena in the context of operator algebras. In particular, in seeking to generalize the theorem, we make the following observations:

- δ_d is the (unique) trace preserving conditional expectation onto the trivial scalar algebra $\mathcal{A} = \mathbb{C}I_d$.
- Every unital channel Φ contains the trivial algebra in its fixed point algebra; $\text{Fix}(\mathcal{A}) \supseteq \mathbb{C}I_d$.
- The unitary group $\mathcal{U}(d)$ inside M_d is the group of unitaries contained in the commutant of the trivial algebra; $(\mathbb{C}I_d)' = M_d$.

Following further investigation, we replace the trivial algebra $\mathbb{C}I_d$ with an arbitrary unital operator algebra \mathcal{A} , and then we formulated a conjecture on the generalization, which we state and prove as the following result.

Theorem 4. *Let \mathcal{A} be any unital operator algebra inside M_d . Let $\mathcal{E}_{\mathcal{A}}$ be the trace preserving conditional expectation onto \mathcal{A} , and let $\mathcal{U}_{\mathcal{A}'}$ be the group of unitaries contained in the commutant of \mathcal{A} . Then for any unital channel Φ whose fixed point algebra contains \mathcal{A} , there exists a $p \in (0, 1)$ depending only on the algebra \mathcal{A} such that the convex combination*

$$p\Phi + (1 - p)\mathcal{E}_{\mathcal{A}} \tag{4}$$

is in the convex hull of channels of the form $\Phi_U(X) = UXU^*$ where $U \in \mathcal{U}_{\mathcal{A}'}$.

Returning to the example above, the point is, in order to generalize properly, one must restrict the set of channels, Φ , to only those that fix the algebra onto which the conditional expectation projects. In the example, id is the conditional expectation onto the full matrix algebra, M_3 , and in fact there are no non-trivial channels that fix this algebra. It is also the case that the fixed point algebra of $W_3^-(X)$ is just the trivial algebra, consisting of scalar multiples of the identity matrix. Thus, there is no unital channel other than δ_3 for which we should expect a Watrous-type theorem to hold for W_3^- .

3. Proof of main result

In this section we shall prove theorem 4. The proof requires a number of supporting results that may be of independent interest. We begin by establishing notation.

Let $d = \sum_{k=1}^r m_k n_k$ for some positive integers m_k, n_k , and let $D = \sum_{k=1}^r n_k^2$. For the purposes of the proof, here we will assume the algebra \mathcal{A} is given by,

$$\mathcal{A} = \bigoplus_{k=1}^r M_{m_k} \otimes I_{n_k},$$

so that

$$\mathcal{A}' = \bigoplus_{k=1}^r I_{m_k} \otimes M_{n_k},$$

and note this means the vector space dimension of the commutant is $D = \dim(\mathcal{A}')$.

Let $\{K_i\}_{i=1}^n$ be a fixed set of Kraus operators for Φ . Then by assumption we have $\mathcal{A} \subseteq \text{Fix}(\Phi) = \{K_i\}'$, so that the K_i belong to \mathcal{A}' and hence each $K_i = \bigoplus_{k=1}^r I_{m_k} \otimes K_{ik}$ for some $K_{ik} \in M_{n_k}$. Define Φ_k , for each k , to be the map on M_{n_k} with Kraus operators $\{K_{ik}\}_{i=1}^n$, and define $\widehat{\Phi}_k$ to be the map on M_d whose Kraus operators \widehat{K}_{ik} have $I_{m_k} \otimes K_{ik}$ on the k th block and zeroes on the other blocks. Note that Φ_k is a unital channel as Φ is.

We consider unitaries $U \in \mathcal{A}'$, which are of the form $U = \bigoplus_{k=1}^r I_{m_k} \otimes U_k$ with $U_k \in \mathcal{U}(n_k)$. For $A, B \in \mathcal{A}'$ define the inner product:

$$\langle A, B \rangle_{\mathcal{A}'} = \sum_{k=1}^r n_k \text{Tr}(A_k^* B_k),$$

where $A = \bigoplus_{k=1}^r I_{m_k} \otimes A_k$ and similarly for B . This is the inner product that arises from the left-regular representation of \mathcal{A}' [18, 30].

Further, let δ_{n_k} be the depolarizing map on M_{n_k} , and recall we have $\mathcal{E}_{\mathcal{A}}$ as the trace-preserving conditional expectation onto \mathcal{A} .

Given any unital channel $\Phi : M_d \rightarrow M_d$ with Kraus operators $K_i \in \mathcal{A}'$, define the following linear map on M_d :

$$L(\Phi)(X) = \sum_i \int_{U \in \mathcal{U}(\mathcal{A}')} UXU^* |\langle U, K_i \rangle_{\mathcal{A}'}|^2 d\mu(U) \quad \forall X \in M_d, \tag{5}$$

where $\mu(\cdot)$ is the Haar measure on the unitary group $\mathcal{U}(\mathcal{A}') = \mathcal{A}' \cap \mathcal{U}(d)$. Notice that $L(\Phi)$ is a positive combination of unitary adjunctions, so possibly after some normalizing, $L(\Phi)$ is a mixed-unitary map. We note that $L(\cdot)$ depends on the algebra \mathcal{A} , though we will suppress reference to it in the notation, and also observe that $L(\Phi + \Psi) = L(\Phi) + L(\Psi)$ for any unital channels with Kraus operators in \mathcal{A}' . Further, as will become clear in lemma 8, the definition of $L(\Phi)$ does not depend on the choice of Kraus operators that define it as above.

We collect the following known results (with short proofs for completeness) before analyzing the map $L(\Phi)$ in more detail.

Lemma 5. *For any positive integer d , we have*

$$\int_{U \in \mathcal{U}(d)} \text{vec}(U) \text{vec}(U)^* d\mu(U) = \frac{1}{d} I_d \otimes I_d. \tag{6}$$

Proof. For $\Phi(X) = UXU^*$, the Choi matrix is $J(\Phi) = \text{vec}(U) \text{vec}(U)^*$. Hence, the above integral is simply the Choi matrix of the channel

$$\delta_d(X) = \int_{U \in \mathcal{U}(d)} UXU^* d\mu(U) = \frac{1}{d} \text{Tr}(X) I_d,$$

and it is clear that $\frac{1}{d} I_d \otimes I_d$ is the correct Choi matrix. □

Since $U \otimes U^*$ has the same entries as $\text{vec}(U) \text{vec}(U)^*$, up to the permutation that maps $E_{ij} \otimes E_{lk} \mapsto E_{ik} \otimes E_{jl}$, and since this same permutation maps $\frac{1}{d} I_d \otimes I_d \mapsto \frac{1}{d} \sum_{i,j} E_{ij} \otimes E_{ji}$, we also have the following.

Corollary 6. *For any positive integer d , we have*

$$\int_{U \in \mathcal{U}(d)} U \otimes U^* d\mu(U) = \frac{1}{d} \sum_{i,j=1}^d E_{ij} \otimes E_{ji}. \tag{7}$$

This in turn, gives us another Corollary that will be useful.

Corollary 7. For any $X \in M_d(\mathbb{C})$, we have

$$\int_{U \in \mathcal{U}(d)} U \text{Tr}(U^* X) d\mu(U) = \frac{1}{d} X \tag{8}$$

$$\int_{U \in \mathcal{U}(d)} |\text{Tr}(UX^*)|^2 d\mu(U) = \frac{1}{d} \text{Tr}(X^* X). \tag{9}$$

Proof. This follows from the fact that the two integrals can be expressed as $(\text{id} \otimes \text{Tr})(P(I_d \otimes X))$, and $\text{Tr}(P(X^* \otimes X))$ respectively, where $P = \int_{U \in \mathcal{U}(d)} U \otimes U^* d\mu(U)$. By equation (7) this is just $\frac{1}{d} \sum_{i,j} E_{ij} \otimes E_{ji}$, and so we get, respectively,

$$\frac{1}{d} \sum_{i,j} \text{Tr}(XE_{ji}) E_{ij} = \frac{1}{d} X, \quad \text{and} \quad \frac{1}{d} \sum_{i,j} \text{Tr}(X^* E_{ij}) \text{Tr}(XE_{ji}) = \frac{1}{d} \sum_{i,j} |x_{ij}|^2,$$

where $X = (x_{ij})$, which completes the proof. □

Before presenting the next lemma, we remind the reader that a homogeneous function of degree n from M_d to M_d is a function $f(\cdot)$ satisfying $f(kX) = k^n f(X)$ for all $k \in \mathbb{C}$ and all $X \in M_n$. Similarly a conjugate homogeneous function of degree n from M_d to M_d is a function satisfying $f(kX) = \bar{k}^n f(X)$ for all $k \in \mathbb{C}$ and all $X \in M_d$.

Lemma 8. Let n be a nonzero integer and let $f: M_d \rightarrow M_d$ be either a homogenous function or conjugate homogenous function of degree n . Then $\int_{U \in \mathcal{U}(d)} f(U) d\mu(U) = 0$.

Proof. If $f: M_d \rightarrow M_d$ is either a homogenous function or conjugate homogenous function of degree n , then there exists ω a complex number of modulus one such that $f(\omega U) = -f(U)$. Since $\omega I_d \in \mathcal{U}(d)$, by translation invariance of the Haar measure we have $\int_{U \in \mathcal{U}(d)} f(U) d\mu(U) = \int_{U \in \mathcal{U}(d)} f(\omega U) d\mu(U) = - \int_{U \in \mathcal{U}(d)} f(U) d\mu(U)$. Rearranging, we get $\int_{U \in \mathcal{U}(d)} f(U) d\mu(U) = 0$. □

Using these facts, in the next pair of results we can derive useful properties of the $L(\cdot)$ map. Before beginning the proofs in earnest, as preparation we briefly discuss the Haar integral over the group $\mathcal{U}(\mathcal{A}') = \mathcal{A}' \cap \mathcal{U}(d)$ and explain some facts that we will use to simplify expressions in the analysis below. First of all, the group of unitaries in \mathcal{A}' is, as a group, simply the product of the groups $I_{m_k} \otimes \mathcal{U}(n_k)$. The Haar measure on these component groups is just the Haar measure on each $\mathcal{U}(n_k)$, and so the Haar measure on the finite product of these groups is just the product of these Haar measures; thus we have

$$\int_{U \in \mathcal{U}(\mathcal{A}')} X d\mu(U) = \int_{U_1 \in \mathcal{U}(n_1)} \cdots \int_{U_r \in \mathcal{U}(n_r)} X d\mu(U_r) \cdots d\mu(U_1),$$

and indeed the right-hand-side can be arranged into any permutation of the groups $\mathcal{U}(n_j)$ [15]. In our evaluation of integrals below, our integrand will be an expression containing only a small number of the U_j ; we will as a matter of course rewrite all integrals so that integrals over $\mathcal{U}(n_j)$ where there is no appearance of U_j or U_j^* inside the integrals become the innermost integrals. This is because such integrals will reduce to trivial integrals; and since we then

integrate over normalized Haar measure, these inner integrals integrate to 1, and thus no longer appear explicitly. We will do all of this implicitly, so as not to clutter notation. For example,

$$\begin{aligned} \int_{U \in \mathcal{U}(\mathcal{A}')} U_1 d\mu(U) &= \int_{U_1 \in \mathcal{U}(n_1)} U_1 \left(\cdots \int_{U_{r-1} \in \mathcal{U}(n_{r-1})} \underbrace{\left[\int_{U_r \in \mathcal{U}(n_r)} d\mu(U_r) \right]}_{=1} d\mu(U_{r-1}) \cdots \right) d\mu(U_1) \\ &= \int_{U_1 \in \mathcal{U}(n_1)} \left(\cdots \underbrace{\int_{U_{r-1} \in \mathcal{U}(n_{r-1})} 1 d\mu(U_{r-1}) \cdots}_{=1} \right) d\mu(U_1) \\ &= \int_{U_1 \in \mathcal{U}(n_1)} U_1 d\mu(U_1). \end{aligned}$$

Thus, from here on out, we will immediately jump to the simplified form, and all integrals will only be taken over variables that actually appear in a non-trivial way in any given expression. Finally, even for the remaining variables, we will only leave one integral sign, to avoid clutter and confusion; for instance, if the variables U_j, U_k appear inside an integration, the expression $\int f(U_j, U_k) d\mu(U_j) d\mu(U_k)$ should be understood as $\int_{U_k \in \mathcal{U}(n_k)} \int_{U_j \in \mathcal{U}(n_j)} f(U_j, U_k) d\mu(U_j) d\mu(U_k)$.

Lemma 9. *Suppose $\Phi : M_d \rightarrow M_d$ is a unital channel that fixes the algebra \mathcal{A} . Then for all $X \in M_d$,*

$$L(\Phi)(X) = \Phi(X) + (D - 1) \mathcal{E}_{\mathcal{A}}(X) + \sum_{k:n_k > 1} \frac{1}{n_k^2 - 1} \left(\widehat{\Phi}_k(X) - \widehat{\delta}_{n_k}(X) \right).$$

Proof. We first expand, using the following form for a generic element of M_d :

$$X = \sum_{k_1, k_2, s, t} E_{k_1 k_2} \otimes E_{st} \otimes X_{k_1 k_2, st},$$

where for each pair $1 \leq k_1, k_2 \leq r$, the matrices E_{st} , with $1 \leq s \leq m_{k_1}$ and $1 \leq t \leq m_{k_2}$ are matrix units for the $m_{k_1} \times m_{k_2}$ matrices, and $X_{k_1 k_2, st}$ is a $n_{k_1} \times n_{k_2}$ matrix. So in this form, $U \in \mathcal{A}'$ is written $U = \sum_{k=1}^r E_{kk} \otimes I_{m_k} \otimes U_k$ with $U_k \in M_{n_k}$.

From the definition of L , and using the expansion of X , also keeping in mind the integral note in the text above this result, we have,

$$\begin{aligned} L(\Phi)(X) &= \sum_i \sum_{k_1, k_2, s, t, j, l} E_{k_1 k_2} \otimes E_{st} \\ &\quad \otimes \int U_{k_1} X_{k_1 k_2, st} U_{k_2}^* n_j n_l \text{Tr}(U_j^* K_{ij}) \text{Tr}(U_l K_{ii}^*) d\mu(U_{k_1}) d\mu(U_{k_2}) d\mu(U_j) d\mu(U_l), \end{aligned}$$

and so we will analyze this depending on whether or not $k_1 = k_2$.

If $k_1 \neq k_2$, then, using the fact that the Haar integral satisfies $\int_U U d\mu(U) = 0$, non-zero contributions in this expression can only possibly come from either the terms where $j = k_1$ and $l = k_2$ or the terms where $j = k_2$ and $l = k_1$.

The sum of all terms where $j = k_2$ and $l = k_1$, for a given value of i , is

$$\sum_{k_1, k_2, s, t} E_{k_1 k_2} \otimes E_{st} \otimes \left(\sum_i \left(n_{k_1} \int U_{k_1} \text{Tr}(U_{k_1} K_{i k_1}^*) d\mu(U_{k_1}) \right) X_{k_1 k_2, st} \right. \\ \left. \times \left(n_{k_2} \int (U_{k_2} \text{Tr}(U_{k_2} K_{i k_2}^*))^* d\mu(U_{k_2}) \right) \right).$$

Now since $U_{k_1} \text{Tr}(U_{k_1} K_{i k_1}^*)$ is a homogeneous function of degree two in U_{k_1} and $(U_{k_2} \text{Tr}(U_{k_2} K_{i k_2}^*))^*$ is a conjugate homogeneous function of degree two in U_{k_2} , by lemma 8 every integral in this expression is zero and hence the full expression itself is equal to zero.

So, in fact, non-zero contributions can come only from the terms where $j = k_1$ and $l = k_2$. Restricting our attention only to these terms and using corollary 7, we get

$$\sum_{k_1, k_2, s, t} E_{k_1 k_2} \otimes E_{st} \otimes \left(\sum_i \left(n_{k_1} \int U_{k_1} \text{Tr}(U_{k_1}^* K_{i k_1}) d\mu(U_{k_1}) \right) X_{k_1 k_2, st} \right. \\ \left. \times \left(n_{k_2} \int (U_{k_2} \text{Tr}(U_{k_2}^* K_{i k_2}))^* d\mu(U_{k_2}) \right) \right) \\ = \sum_{k_1, k_2, s, t} E_{k_1 k_2} \otimes E_{st} \otimes \left(\sum_i K_{i k_1} X_{k_1 k_2, st} K_{i k_2}^* \right),$$

which gives us the off-diagonal blocks of $\Phi(X) = \sum_i K_i X K_i^*$. Thus, on the blocks corresponding to $k_1 \neq k_2$, we get a term of the corresponding block form of $\Phi(X)$.

When $k_1 = k_2$, we must have $j = l$ for non-zero contributions, and we split this up into terms for which $k_1 \neq j$ and $k_1 = j$ to get,

$$\sum_{k_1, s, t} E_{k_1 k_1} \otimes E_{st} \otimes \left(\left(\int U_{k_1} X_{k_1 k_1, st} U_{k_1}^* d\mu(U_{k_1}) \right) \left(\sum_{j \neq k_1} n_j^2 \sum_i \int |\text{Tr}(U_j^* K_{ij})|^2 d\mu(U_j) \right) \right) \\ + \sum_{k_1, s, t} E_{k_1 k_1} \otimes E_{st} \otimes n_{k_1}^2 \sum_i \int U_{k_1} X_{k_1 k_1, st} U_{k_1}^* |\text{Tr}(U_{k_1}^* K_{i k_1})|^2 d\mu(U_{k_1}).$$

Now, using the definition of the completely depolarizing channel on M_{n_k} , equation (9), and the fact that $\{K_{ij}\}_i$ defines a channel on M_{n_j} applied to the first term, and then the estimate from the original Watrous Theorem applied to the second term (and assuming for now that $n_{k_1} \neq 1$), we obtain the following:

$$\sum_{k_1, s, t} E_{k_1 k_1} \otimes E_{st} \otimes \left(\delta_{n_{k_1}}(X_{k_1 k_1, st}) \sum_{j \neq k_1} n_j^2 + \frac{n_{k_1}^2}{n_{k_1}^2 - 1} \Phi_{k_1}(X_{k_1 k_1, st}) + \frac{n_{k_1}^2 (n_{k_1}^2 - 2)}{n_{k_1}^2 - 1} \delta_{n_{k_1}}(X_{k_1 k_1, st}) \right).$$

The last tensor factor can be rewritten as,

$$\delta_{n_{k_1}}(X_{k_1 k_1, st}) (D - n_{k_1}^2) + \Phi_{k_1}(X_{k_1 k_1, st}) + \frac{1}{n_{k_1}^2 - 1} \Phi_{k_1}(X_{k_1 k_1, st}) + \frac{n_{k_1}^2 (n_{k_1}^2 - 2)}{n_{k_1}^2 - 1} \delta_{n_{k_1}}(X_{k_1 k_1, st}) \\ = \Phi_{k_1}(X_{k_1 k_1, st}) + D \delta_{n_{k_1}}(X_{k_1 k_1, st}) + \frac{1}{n_{k_1}^2 - 1} \Phi_{k_1}(X_{k_1 k_1, st}) - \frac{n_{k_1}^2}{n_{k_1}^2 - 1} \delta_{n_{k_1}}(X_{k_1 k_1, st});$$

which follows from splitting $\frac{n_{k_1}^2}{n_{k_1}^2 - 1}$ into $1 + \frac{1}{n_{k_1}^2 - 1}$ and $\frac{n_{k_1}^2(n_{k_1}^2 - 2)}{n_{k_1}^2 - 1} - n_{k_1}^2 = -\frac{n_{k_1}^2}{n_{k_1}^2 - 1}$. This latter quantity, in turn, we can write as $-\frac{1}{n_{k_1}^2 - 1} - 1$, and so we have the last tensor factor rewritten as,

$$\Phi_{k_1}(X_{k_1 k_1, st}) + (D - 1) \delta_{n_{k_1}}(X_{k_1 k_1, st}) + \frac{1}{n_{k_1}^2 - 1} \left(\Phi_{k_1}(X_{k_1 k_1, st}) - \delta_{n_{k_1}}(X_{k_1 k_1, st}) \right).$$

We must also consider the case when $n_{k_1} = 1$, in which case we cannot use the Watrous Theorem as written, to avoid dividing by $n_{k_1}^2 - 1 = 0$. In this case, note that Φ_{k_1} is a channel on $M_1 \equiv \mathbb{C}$; but there is only one such map, which is the identity map. In this case, $\Phi_{k_1} = \delta_{n_{k_1}}$ is just the identity map on \mathbb{C} , and so in that case, we would write the relevant integral in the last tensor factor as,

$$n_{k_1}^2 \sum_i \int U_{k_1} X_{k_1 k_1, st} U_{k_1}^* |\text{Tr}(U_{k_1}^* K_{ik_1})|^2 d\mu(U_{k_1}) = X_{k_1 k_1, st} = \Phi_{k_1}(X_{k_1 k_1, st}) = \delta_{n_{k_1}}(X_{k_1 k_1, st}).$$

So in this case, the diagonal term would be

$$(D - 1) \delta_{n_{k_1}}(X_{k_1 k_1, st}) + \Phi_{k_1}(X_{k_1 k_1, st}).$$

Hence, summing over k_1, k_2 in the decomposition of $L(\Phi)(X)$, we first get a copy of $\Phi(X)$. Further, the $(D - 1) \delta_{n_{k_1}}(X_{k_1 k_1, st})$ down the diagonal combine to give us $(D - 1) \mathcal{E}_{\mathcal{A}}(X)$. Thus, bringing everything together, we have

$$L(\Phi)(X) = \Phi(X) + (D - 1) \mathcal{E}_{\mathcal{A}}(X) + \sum_{k: n_k > 1} \frac{1}{n_k^2 - 1} \left(\widehat{\Phi}_k(X) - \widehat{\delta}_{n_k}(X) \right),$$

and this completes the proof. □

Lemma 10. Given \mathcal{A} and Φ as above, for each unital channel Φ_k , we have for all $X \in M_d$,

$$L(\widehat{\Phi}_k)(X) = n_k^2 \mathcal{E}_{\mathcal{A}}(X) + \frac{n_k^2}{n_k^2 - 1} \left(\widehat{\Phi}_k(X) - \widehat{\delta}_{n_k}(X) \right),$$

if $n_k > 1$, and otherwise,

$$L(\widehat{\Phi}_k)(X) = \mathcal{E}_{\mathcal{A}}(X).$$

Proof. Notice that $\langle U, \widehat{K}_{ik} \rangle_{\mathcal{A}'} = n_k \text{Tr}(U_k^* K_{ik})$ for all i since all other blocks of \widehat{K}_{ik} are 0. Thus when we do the same calculation as in the previous Lemma proof with $\widehat{\Phi}_k$ instead of Φ , we get in the last tensor factor,

$$\sum_i \int U_{k_1} X_{k_1 k_2, st} U_{k_2}^* n_k^2 |\text{Tr}(U_k^* K_{ik})|^2 d\mu(U_{k_1}) d\mu(U_k) d\mu(U_{k_2}).$$

For $k_1 \neq k_2$, to get a non-zero contribution we must have in the integral, $k_1 = k$ and $k_2 = k$, a contradiction. So we only get (potentially) non-zero terms when $k_1 = k_2$.

If $k_1 = k_2 \neq k$, we get

$$\left(\int U_{k_1} X_{k_1 k_1, st} U_{k_1}^* d\mu(U_{k_1}) \right) \left(n_k^2 \sum_i \int |\text{Tr}(U_k^* K_{ik})|^2 d\mu(U_k) \right),$$

and this simplifies, from the definition of the completely depolarizing channel applied to the first term and corollary 7 and that $\{K_{ik}\}_i$ define a channel on M_{n_k} applied to the second term, to:

$$n_k^2 \delta_{n_{k_1}}(X_{k_1 k_1, st}).$$

Otherwise, if $k_1 = k = k_2$, and $n_k > 1$, we get using the original Watrous Theorem,

$$\frac{n_k^2}{n_k^2 - 1} (\Phi_k(X_{kk, st}) + (n_k^2 - 2) \delta_{n_k}(X_{kk, st})).$$

From this, we take a term of the form $n_k^2 \delta_{n_k}(X_{kk, st})$ to combine with the other diagonal terms, giving us $n_k^2 \mathcal{E}_{\mathcal{A}}(X)$, and leaving us with

$$\frac{n_k^2}{n_k^2 - 1} (\widehat{\Phi}_k(X) - \widehat{\delta}_{n_k}(X))$$

from the remaining terms.

Finally, if $n_k = 1$, we just get

$$n_k^2 \delta_{n_k}(X_{kk, st})$$

since both δ_{n_k} and Φ_k are just the identity map on scalars.

So, we can sum over k_1, k_2 and the $n_k^2 \delta_{n_{k_1}}(X_{k_1 k_1, st})$ terms will combine to give us $n_k^2 \mathcal{E}_{\mathcal{A}}(X)$, plus, if $n_k > 1$, a term of the form $\frac{n_k^2}{n_k^2 - 1} (\widehat{\Phi}_k - \widehat{\delta}_{n_k})(X)$. \square

Applying the previous Lemma to the case $\Phi_k = \delta_{n_k}$, we immediately have the following:

$$L(\widehat{\delta}_{n_k})(X) = n_k^2 \mathcal{E}_{\mathcal{A}}(X). \tag{10}$$

Now we prove the theorem, with explicit constants given.

Theorem 11. *Let $\Phi : M_d \rightarrow M_d$ be a unital channel that fixes the unital algebra $\mathcal{A} = \bigoplus_{i=1}^r M_{m_k} \otimes I_{n_k}$. Let $D = \dim(\mathcal{A}')$ and let \widehat{r} be the number of direct summands of \mathcal{A}' for which the matrix component satisfies $n_i > 1$.*

If $r = 1$, and $\mathcal{A}' = I_{m_1} \otimes M_{n_1}$, with $n_1 > 1$, we have that

$$\frac{1}{n_1^2 - 1} (\Phi(X) + (n_1^2 - 2) \mathcal{E}_{\mathcal{A}}(X))$$

is mixed unitary. If $r > 1$, we have that

$$\frac{1}{D - \widehat{r} + \sum_{k:n_k > 1} n_k^2} \left(\Phi(X) + \left(D - \widehat{r} - 1 + \sum_{k:n_k > 1} n_k^2 \right) \mathcal{E}_{\mathcal{A}}(X) \right)$$

is mixed unitary.

Proof. We begin with the statement of lemma 9, combined with that of lemma 10:

$$L(\Phi)(X) = \Phi(X) + (D - 1)\mathcal{E}_{\mathcal{A}}(X) + \sum_{k:n_k > 1} \frac{1}{n_k^2 - 1} \left(\widehat{\Phi}_k - \widehat{\delta}_{n_k} \right)(X),$$

and

$$L\left(\widehat{\Phi}_k\right)(X) = n_k^2 \mathcal{E}_{\mathcal{A}}(X) + \frac{n_k^2}{n_k^2 - 1} \left(\widehat{\Phi}_k - \widehat{\delta}_{n_k} \right)(X)$$

for all $n_k > 1$. Thus we can write

$$L(\Phi)(X) = \Phi(X) + (D - 1)\mathcal{E}_{\mathcal{A}}(X) + \sum_{k:n_k > 1} \left(\frac{1}{n_k^2} L\left(\widehat{\Phi}_k\right)(X) - \mathcal{E}_{\mathcal{A}}(X) \right),$$

which we can rearrange to obtain

$$L(\Phi)(X) - \sum_{k:n_k > 1} \frac{1}{n_k^2} L\left(\widehat{\Phi}_k\right)(X) = \Phi(X) + (D - \widehat{r} - 1)\mathcal{E}_{\mathcal{A}}(X). \tag{11}$$

Before continuing, we first consider the case where $r = 1$; that is, where $\mathcal{A} = M_m \otimes I_n$ and $\mathcal{A}' = I_m \otimes M_n$ (and $n > 1$, as the $r = 1 = n$ case is trivial). Then $\widehat{r} = 1$, and we have that $\widehat{\Phi}_1 = \widehat{\Phi}_1 = \Phi$, since there are no blocks other than the first block to zero out, in order to create $\widehat{\Phi}_1$. In this case, $n_1 = n$, and so we see that $L(\Phi) - \frac{1}{n^2} L(\widehat{\Phi}_1)$ is just $\frac{n^2 - 1}{n^2} L(\Phi)$, and, using equation (11) (and $D = n^2$), we have

$$\frac{n^2 - 1}{n^2} L(\Phi)(X) = \Phi(X) + (n^2 - 2)\mathcal{E}_{\mathcal{A}}(X).$$

In any other case, for any k for which $n_k > 1$, we have that $\Phi_k : M_{n_k} \rightarrow M_{n_k}$ is a unital channel. Thus $\text{Tr}(J(\Phi_k)) = n_k$, and since $J(\Phi_k) \geq 0$, we have that $n_k I_{n_k} \otimes I_{n_k} \geq J(\Phi_k)$. Hence

$$J(\delta_{n_k}) = \frac{1}{n_k} I_{n_k} \otimes I_{n_k} \geq \frac{1}{n_k^2} J(\Phi_k),$$

and so the map $\delta_{n_k} - \frac{1}{n_k^2} \Phi_k$ is a completely positive map. From this, we obtain that the map $\widehat{\delta}_{n_k} - \frac{1}{n_k^2} \widehat{\Phi}_k = \widehat{\delta}_{n_k} - \frac{1}{n_k^2} \widehat{\Phi}_k$ is also completely positive as it is just the direct sum of $\delta_{n_k} - \frac{1}{n_k^2} \Phi_k$ with the zero map a number of times.

Finally, using the fact that $L(\Phi + \Psi) - L(\Psi) = L(\Phi)$ for completely positive maps with Kraus operators in \mathcal{A}' , we have that

$$L\left(\widehat{\delta}_{n_k} - \frac{1}{n_k^2} \widehat{\Phi}_k\right)(X) = L\left(\widehat{\delta}_{n_k}\right)(X) - \frac{1}{n_k^2} L\left(\widehat{\Phi}_k\right)(X)$$

is a positive combination of unitary adjunctions.

Thus we may add $L\left(\widehat{\delta}_{n_k}\right)(X)$ to both sides of equation (11). By equation (10), this is equivalent to adding $n_k^2 \mathcal{E}_{\mathcal{A}}(X)$, and so we obtain

$$L(\Phi)(X) + \sum_{k:n_k > 1} L\left(\widehat{\delta}_{n_k} - \frac{1}{n_k^2} \widehat{\Phi}_k\right)(X) = \Phi(X) + \left(D - \widehat{r} - 1 + \sum_{k:n_k > 1} n_k^2 \right) \mathcal{E}_{\mathcal{A}}(X).$$

In all cases, we now have on the left-hand-side a positive combination of terms of the form $L(\Psi)$ where Ψ is completely positive, and so this is a positive combination of unitary adjunctions. Hence the right-hand-side is now simply a positive combination of Φ and $\mathcal{E}_{\mathcal{A}}$. Thus, after suitably normalizing, the left-hand-side will be an expression of the right-hand-side as a mixed unitary. In particular, we obtain either

$$\frac{1}{n^2}L(\Phi) = \frac{1}{n^2 - 1} (\Phi(X) + (n^2 - 2) \mathcal{E}_{\mathcal{A}}(X))$$

is mixed unitary in the case that $r = 1$, or

$$\begin{aligned} & \frac{1}{D - \widehat{r} + \sum_{k:n_k > 1} n_k^2} \left(L(\Phi)(X) + \sum_{k:n_k > 1} L\left(\widehat{\delta_{n_k} - \frac{1}{n_k^2} \Phi_k}\right)(X) \right) \\ &= \frac{1}{D - \widehat{r} + \sum_{k:n_k > 1} n_k^2} \left(\Phi(X) + \left(D - \widehat{r} - 1 + \sum_{k:n_k > 1} n_k^2 \right) \mathcal{E}_{\mathcal{A}}(X) \right) \end{aligned}$$

is mixed unitary when $r > 1$. This completes the proof. □

4. Application: all unital channels are eventually mixed unitary

In this section we prove that every unital quantum channel has the property that some power of it becomes mixed unitary. This involves proving several supporting results that may be of independent interest, and, at the final stage, applying our theorem 4. We note for the reader that following the logical flow of this section does not require the results of the previous section until the final result proof.

4.1. Asymptotic result for primitive unital channels

We first show how Watrous’ theorem 2 yields an asymptotic result for the case of primitive unital channels. We begin with a result that we expect is well-known (see [6] for instance), but for completeness we provide a short proof that makes use of convexity theory (see [35]).

Lemma 12. *Let \mathcal{A} be any unital $*$ -subalgebra of M_d . Let $\mathcal{E}_{\mathcal{A}}$ be the trace preserving conditional expectation onto \mathcal{A} . Then $\mathcal{E}_{\mathcal{A}}$ is a mixed unitary channel.*

Proof. Let $\mathcal{U}(\mathcal{A}')$ be the unitary group of the commutant algebra $\mathcal{A}' = \{X \in M_d : AX = XA, \forall A \in \mathcal{A}\}$. It follows that the conditional expectation can be written as follows for all $X \in M_d$:

$$\mathcal{E}_{\mathcal{A}}(X) = \int_{U \in \mathcal{U}(\mathcal{A}')} UXU^* d\mu(U),$$

where $\mu(U)$ is the normalized Haar measure on $\mathcal{U}(\mathcal{A}')$. Indeed, it is easy to see that this integral operator is trace preserving, projects onto \mathcal{A} , and satisfies the other conditional expectation properties from the invariance of the Haar measure. So by uniqueness the map is $\mathcal{E}_{\mathcal{A}}$.

Now as the commutant \mathcal{A}' is a finite dimensional subalgebra, the group $\mathcal{U}(\mathcal{A}')$ is closed (and hence compact) and so the convex hull of the set $\{UXU^* : U \in \mathcal{U}(\mathcal{A}')\}$ is a compact (and hence closed) convex set by the Minkowski-Caratheodory convexity theorem. Thus $\mathcal{E}_{\mathcal{A}}(X)$ lies in the convex hull of mappings of the form UXU^* , with $U \in \mathcal{U}(\mathcal{A}')$, and so $\mathcal{E}_{\mathcal{A}}$ is a mixed unitary map. □

Remark 13. Note that from the above result, it is clear that the completely depolarizing channel $\delta_d(X) = d^{-1}\text{Tr}(X)I_d$, which is the trace preserving conditional expectation onto the trivial algebra $\mathcal{A} = \{CI\}$, is a mixed unitary map. A concrete representation of this map can be written down:

$$\delta_d(X) = d^{-1}\text{Tr}(X)I_d = \frac{1}{d^2} \sum_{a,b=0}^{d-1} W_{a,b} X W_{a,b}^*$$

where $W_{a,b}$ are the Weyl-Heisenberg unitaries defined by

$$W_{a,b} = S^a D^b, 0 \leq a, b \leq d - 1,$$

and $S = \sum_{j=1}^d E_{j+1(\text{mod } d),j} \in M_d$ is the forward cyclic shift operator and $D = \sum_{j=1}^d \omega^j E_{j,j} \in M_d$ is the ‘clock operator’ with $\omega = \exp(2\pi i/d)$.

We use the above result to prove the following. Let us denote $MU(d)$ to be the set of all mixed-unitary channels on M_d , which note is a closed convex set of linear maps. See [29] for basic properties of the completely bounded distance measure.

Lemma 14. *Let $\Phi : M_d \rightarrow M_d$ be any unital quantum channel. Then*

$$\liminf_{n \rightarrow \infty} d_{CB}(\Phi^n, MU(d)) = 0,$$

where $d_{CB}(\Phi^n, MU(d))$ is the completely bounded distance of Φ^n from the closed convex set $MU(d)$.

Proof. By Kuperberg’s Theorem (see theorem 2.1 in [22]), for a unital completely positive map Φ , there is a subsequence n_1, n_2, \dots such that

$$\lim_{j \rightarrow \infty} \Phi^{n_j} = \mathcal{E}_\Phi,$$

where \mathcal{E}_Φ is a unique idempotent map. Note that for trace-preserving completely positive maps, such a map also exists (see proposition 6.3 in [39]).

Now note that since Φ is trace preserving, \mathcal{E}_Φ is also trace preserving. And hence its range $\text{Range}(\mathcal{E}_\Phi)$ is a C^* -algebra. Indeed, let $a \in \text{Range}(\mathcal{E}_\Phi)$, then from Schwarz inequality it follows that

$$\mathcal{E}_\Phi(aa^*) \geq \mathcal{E}_\Phi(a)\mathcal{E}_\Phi(a^*) = aa^*.$$

And using the trace preservation property and faithfulness of trace, we get that $\mathcal{E}_\Phi(aa^*) = aa^*$. Thus, $aa^* \in \text{Range}(\mathcal{E}_\Phi)$. This means $\mathcal{E}_\Phi(aa^*) = \mathcal{E}_\Phi(a)\mathcal{E}_\Phi(a^*) = aa^*$. And hence a is in the multiplicative domain of \mathcal{E}_Φ ([7]). From here, it follows that if $a, b \in \text{Range}(\mathcal{E}_\Phi)$, then $\mathcal{E}_\Phi(ab) = ab$. Hence, $ab \in \text{Range}(\mathcal{E}_\Phi)$, showing $\text{Range}(\mathcal{E}_\Phi)$ is a C^* -algebra.

Now the result follows from lemma 12. □

For a special class of channels (e.g. see [1, 33, 34]), one can make a stronger statement.

Definition 15. A unital channel $\Phi : M_d \rightarrow M_d$ is *primitive* if it is *irreducible* (i.e. $\Phi(P) \leq \lambda P$ for some projection P implies $P = 0$ or $P = I$) and it has a trivial *peripheral spectrum* (i.e. $\text{spec}(\Phi) \cap \mathbb{T} = \{1\}$, where \mathbb{T} is the unit circle in the complex plane).

Theorem 16. *For every primitive unital channel $\Phi : M_d \rightarrow M_d$, there is a finite $k \in \mathbb{N}$ such that Φ^k is mixed unitary, and subsequently for every $l \geq k$, Φ^l is mixed unitary.*

Proof. It follows from the proof of the previous result that for a primitive unital channel Φ , the conditional expectation \mathcal{E}_Φ described above is the completely depolarizing channel δ_d . Now by Watrous’s theorem (2) there is a ball around δ_d where every unital channel is mixed-unitary. So from the subsequence n_1, n_2, \dots , if we take sufficiently large n_i ’s, the maps Φ^{n_i} must fall in the ball around δ_d . Hence there is a $k \in \mathbb{N}$ such that Φ^k is in this ball and it is mixed unitary.

The second statement follows easily from the above argument and the CB norm estimate:

$$\|\Phi^{k+r} - \delta_d\|_{CB} = \|\Phi^r (\Phi^k - \delta_d)\|_{CB} \leq \|(\Phi^k - \delta_d)\|_{CB},$$

which also uses the fact that $\Phi \circ \delta_d = \delta_d$ as Φ is unital. □

In what follows, we will show how theorem 4 allows us to prove an analogous result for all unital channels.

4.2. Irreducible channels and peripheral eigenvalues

Next we derive some properties of peripheral eigenvalues for irreducible unital channels.

Let us first observe that a unital channel Φ is irreducible if and only if its fixed point algebra $\text{Fix}(\Phi)$ is just the scalar algebra, $\mathcal{A} = \mathbb{C}I$. Indeed, if Φ is irreducible, then only the trivial projections are fixed by Φ , and hence its fixed point algebra (which is spanned by its projections as a von Neumann algebra) must be trivial. Conversely, if the fixed point algebra for Φ is trivial and P is a projection with $\Phi(P) \leq \lambda P$, then $\Phi(P)$ is supported on the range of P , which for a unital channel implies (as proved in [20]) that in fact $\Phi(P) = P$ if it is non-zero, and hence $P = 0$ or $P = I$.

In the following result, we denote the set of unital channels that fix a given algebra \mathcal{A} by $\mathcal{F}(\mathcal{A})$. Evidently this set has the structure of a convex semigroup under composition of maps. It is also $*$ -closed, in the sense that a map is in the set if and only if its dual map is as well (which can be seen as a consequence of the fixed point theorem for unital channels [20]).

Lemma 17. *Let \mathcal{A} be a unital subalgebra of M_d that is unitarily equivalent to $\bigoplus_{k=1}^r I_{m_k} \otimes M_{n_k}$, and let $\mathcal{F}(\mathcal{A})$ be the semigroup of unital channels on M_d that fix \mathcal{A} . Let $\widehat{\mathcal{A}} = \bigoplus_{k=1}^r \mathbb{C}I_{m_k}$, with associated semigroup $\mathcal{F}(\widehat{\mathcal{A}})$ of unital channels on $M_{(\sum_k m_k)}$ that fix $\widehat{\mathcal{A}}$.*

Then, there is a convex $$ -semigroup isomorphism $\alpha : \mathcal{F}(\mathcal{A}) \rightarrow \mathcal{F}(\widehat{\mathcal{A}})$ with the property that $\alpha(\Phi) \in \mathcal{F}(\widehat{\mathcal{A}})$ is mixed unitary if and only if $\Phi \in \mathcal{F}(\mathcal{A})$ is mixed unitary.*

Proof. Let $\Phi \in \mathcal{F}(\mathcal{A})$ with Kraus operators $\{K_i\}_{i=1}^n$. Since Φ fixes \mathcal{A} , we have $\mathcal{A} \subseteq \text{Fix}(\Phi) = \{K_i\}'$, and so $K_i \in \mathcal{A}'$. Hence there exists a unitary $U \in M_d$ and matrices $K_{ik} \in M_{m_k}$ such that $U^* K_i U = \bigoplus_{k=1}^r K_{ik} \otimes I_{n_k}$ for all i .

Then $\alpha(\Phi)$ is defined to be the map whose Kraus operators are $\widehat{K}_i := \bigoplus_{k=1}^r K_{ik}$, which, as a notational convenience, we sometimes write as $\widehat{K}_i = \alpha(K_i)$. To show that $\alpha(\Phi)$ fixes $\widehat{\mathcal{A}}$, we note that the Kraus operators of $\alpha(\Phi)$ always lies in the algebra $\bigoplus_{k=1}^r M_{m_k}$, and that $\widehat{\mathcal{A}}$ thus necessarily commutes with \widehat{K}_i ; hence it is contained in the fixed point algebra.

It is easy to see that the image of α does not depend on a particular operator-sum representation of Φ , and, moreover, that an operator-sum representation of Φ is minimal in terms of number of Kraus operators if and only if the image of the Kraus operators under α is a minimal representation of $\alpha(\Phi)$.

It is also clear that α is a $*$ -homomorphism, since for any $\Phi, \Psi \in \mathcal{A}$ with respective Kraus operators $U^* K_i U = \bigoplus_{k=1}^r K_{ik} \otimes I_{n_k}$ and $U^* L_i U = \bigoplus_{k=1}^r L_{ik} \otimes I_{n_k}$, we have that $\Phi \circ \Psi$ has Kraus operators $U(\bigoplus_{k=1}^r K_{ik} L_{i'k} \otimes I_{n_k})U^*$. The image under α of these operators are $\bigoplus_{k=1}^r K_{ik} L_{i'k}$, which are exactly the Kraus operators of $\alpha(\Phi) \circ \alpha(\Psi)$.

To see that α is an isomorphism, let $\Phi, \Psi \in \mathcal{F}(\mathcal{A})$, and suppose Φ has a minimal set of Kraus operators given by $\{K_i = U(\oplus_{k=1}^r K_{ik} \otimes I_{n_k})U^*\}_{i=1}^n$ and Ψ has a minimal set of Kraus operators $\{L_i = U(\oplus_{k=1}^r L_{ik} \otimes I_{n_k})U^*\}_{i=1}^{n'}$. Then $\alpha(\Phi)$ has Kraus operators $\{\widehat{K}_i = \oplus_{k=1}^r K_{ik}\}_{i=1}^n$ and $\alpha(\Psi)$ has $\{\widehat{L}_i = \oplus_{k=1}^r L_{ik}\}_{i=1}^{n'}$. If $\alpha(\Phi) = \alpha(\Psi)$, then we have $\{\widehat{K}_i\}_{i=1}^n$ and $\{\widehat{L}_i\}_{i=1}^{n'}$ are two different minimal Kraus representations of the same channel, so $n = n'$. Hence there exists a scalar unitary matrix $V = (v_{ij})$ such that $\widehat{L}_i = \sum_j v_{ij} \widehat{K}_j$ and so $L_{ik} = \sum_j v_{ij} K_{jk}$. Thus

$$\begin{aligned} L_i &= U(\oplus_{k=1}^r L_{ik} \otimes I_{n_k})U^* = U\left(\oplus_{k=1}^r \left(\sum_{j=1}^n v_{ij} K_{jk}\right) \otimes I_{n_k}\right)U^* \\ &= U\left(\sum_j v_{ij} (\oplus_{k=1}^r K_{jk} \otimes I_{n_k})\right)U^* = \sum_j v_{ij} K_j, \end{aligned}$$

and so $\{L_i\}$ and $\{K_i\}$ are two different representations of the same channel, giving $\Phi = \Psi$.

Finally, $\alpha(\Phi)$ is a unitary adjunction channel if and only if Φ is; since $\oplus_{k=1}^r U_k \otimes I_{j_k}$ is unitary if and only if each U_k is unitary, which in turn is equivalent to $\oplus_{k=1}^r U_k$ being unitary. So, in one direction, if $\Phi = \sum_i p_i \text{ad}_{U_i}$ expresses Φ as a convex combination of unitary adjunction maps (where $\text{ad}_U(X) = UXU^*$), the (convex) linearity of α guarantees that

$$\alpha(\Phi) = \sum_i p_i \alpha(\text{ad}_{U_i})$$

expresses $\alpha(\Phi)$ as a convex combination of the unitary adjunctions $\alpha(\text{ad}_{U_i})$. In the other direction, suppose

$$\alpha(\Phi) = \sum_i p_i \text{ad}_{\widehat{U}_i}$$

for some unitaries \widehat{U}_i . Since $\alpha(\Phi)$ fixes the algebra $\widehat{\mathcal{A}} = \oplus_{k=1}^r I_{m_k}$, it must be that each $\widehat{U}_i \in \widehat{\mathcal{A}}' = \oplus_{k=1}^r M_{m_k}$ and hence $\widehat{U}_i = \oplus_{k=1}^r U_{ik}$ for some unitaries U_{ik} on each block. If we define $U_i = U(\oplus_{k=1}^r U_{ik} \otimes I_{n_k})U^* \in \mathcal{A}'$, it is clear that $\alpha(\Phi)$ is now the image of $\Psi := \sum_i p_i \text{ad}_{U_i}$, which is mixed unitary. Since α is an isomorphism, and $\alpha(\Phi) = \alpha(\Psi)$, it must in fact be that $\Phi = \Psi$ and hence is mixed unitary. \square

Remark 18. Notice that if \mathcal{A} is the fixed point algebra of Φ , i.e. the largest unital algebra fixed by Φ , then the algebra generated by its Kraus operators K_i is \mathcal{A}' . So $\alpha(\Phi)$ has Kraus operators that generate the algebra $\alpha(\mathcal{A}) = \oplus_{k=1}^r M_{m_k}$, and so the fixed point algebra of $\alpha(\Phi)$ is the abelian algebra $\oplus_{k=1}^r \mathbb{C}I_{m_k}$. Also notice that the channels Φ_k , with Kraus operators $\{K_{ik}\}$ are irreducible. Thus, without loss of generality, we will prove our result for channels with abelian fixed point algebra, as any unital channel is identified with a channel that has abelian fixed point algebra, and where the identification carries through the relevant properties (i.e. commutes with powers and preserves mixed unitarity).

We next consider the *peripheral spectrum* for a map $\Phi : M_d \rightarrow M_d$, which is the set

$$\{X \in M_d \mid \Phi(X) = \lambda X \text{ for some } |\lambda| = 1\}.$$

In the case of an irreducible unital channel, there is a positive integer m such that the peripheral spectrum is $\{\omega^i\}_{i=0}^{m-1}$ for some primitive m^{th} root of unity (see for instance theorem 6.6 from

[39]). Further, as shown in [32] (theorem 2.5), for a unital channel Φ , the algebra generated by all peripheral eigen-operators for Φ is equal to the algebra $\mathcal{M}_{\Phi^\infty}$, which is defined as the decreasing intersection of the multiplicative domains \mathcal{M}_{Φ^k} for Φ^k , $k \geq 1$; in particular, the peripheral spectrum of Φ^k is a subset of the peripheral spectrum of Φ .

The following useful fact for us comes as a simple consequence of the spectral mapping theorem, from which it follows that the spectrum of Φ^m consists of the elements of the spectrum of Φ raised to the m th power.

Lemma 19. *Suppose Φ is an irreducible unital channel with peripheral spectrum $\{\omega^i\}_{i=0}^{m-1}$ for some primitive m th root of unity. Then Φ^m has no non-trivial peripheral spectrum; that is, $\text{spec}(\Phi^m) \cap \mathbb{T} = \{1\}$.*

We next recall basic features of peripheral eigenvalues, with a short proof for completeness.

Lemma 20. *Let $\Phi : M_d \rightarrow M_d$ be a unital channel, and let X be a peripheral eigenvector for Φ : $\Phi(X) = \lambda X$ for some $|\lambda| = 1$. Then $K_i X = \lambda X K_i$ for all Kraus operators K_i , and so if X is a peripheral eigenvector for Φ with eigenvalue λ , then we have*

$$\Phi(XA) = \lambda X \Phi(A) \quad \Phi(AX) = \bar{\lambda} \Phi(A) X,$$

for all $A \in M_d$.

Proof. Define $A_i = K_i X - \lambda X K_i$. Then we have,

$$\begin{aligned} \sum_i A_i A_i^* &= \sum_i K_i X X^* K_i^* - \bar{\lambda} \sum_i K_i X K_i^* X^* - \lambda X \sum_i K_i X^* K_i^* + |\lambda|^2 X \sum_i K_i K_i^* X^* \\ &= \Phi(X X^*) - X X^*, \end{aligned}$$

where we use the fact that $\Phi(X) = \lambda X$, $\Phi(X^*) = \bar{\lambda} X^*$, and that Φ is unital. Then, by trace preservation, we have that

$$\sum_i \text{Tr}(A_i A_i^*) = \text{Tr}(\Phi(X X^*)) - \text{Tr}(X X^*) = 0,$$

and hence each $A_i = 0$. The final statement immediately follows. □

We also need the following characterization of peripheral eigenvectors in the commutative fixed point algebra case. We note a possible connection between this result and results obtained recently in [2].

Lemma 21. *Let Φ be a unital channel with fixed point algebra unitarily equivalent to $\bigoplus_{k=1}^r \mathbb{C} I_{m_k}$. Let X be a peripheral eigenvector. Then one of the two following cases holds:*

1. $X = \bigoplus_{k=1}^r X_k$ where each X_k is a peripheral eigenvector for the irreducible channel Φ_k obtained by restricting the Kraus operators of Φ to the k^{th} diagonal block.
2. There exists j, k such that $m_j = m_k$, and there is a unitary U on \mathbb{C}^{m_j} such that $\Phi_j = \text{ad}_U \circ \Phi_k \circ \text{ad}_{U^*}$.

Proof. Up to unitary equivalence, the fixed point algebra has minimal central (orthogonal) projections $P_i = \bigoplus_{k=1}^r \delta_{ik} I_{m_k}$ with $\sum_i P_i = I$. As these are fixed points of Φ , we have by lemma 20

that $\Phi(P_kXP_j) = P_k\Phi(X)P_j$ for all X and k, j . In particular, applying this to the peripheral eigenvector X with eigenvalue λ , we get

$$\Phi(P_kXP_j) = \lambda P_kXP_j$$

for all pairs j, k . That is, P_kXP_j is also a peripheral eigenvector for Φ with eigenvalue λ .

Now, lemma 20 also shows that, for any peripheral eigenvector X we have

$$\Phi(XX^*) = |\lambda|^2 XX^* = XX^*,$$

and so XX^* must be in the span of the P_i . Hence the same is true for X^*X , $P_kXP_jX^*P_k$ and $P_kX^*P_jXP_k$.

Thus we can find scalars c_i such that

$$P_kXP_jX^*P_k = \sum_i c_i P_i,$$

which yields after multiplying on the left or right by P_k that

$$P_kXP_jX^*P_k = c_k P_k.$$

If we let X_{kj} be the operator corresponding to the (k, j) block in the decomposition determined by the $\{P_j\}$, which is P_kX restricted to the range of P_j , then we have that

$$X_{kj}X_{kj}^* = c_k I_{m_k} \quad \text{normal and} \quad X_{kj}^*X_{kj} = c_j I_{m_j}. \tag{12}$$

There are two possibilities: either $c_k = c_j = 0$, or both scalars are non-zero and X_{kj} is a (non-zero) multiple of a unitary (and $m_j = m_k$). Thus, in this block matrix form, any peripheral eigenvector has the form,

$$X = \sum_{i_1, i_2} E_{i_1 i_2} \otimes X_{i_1 i_2},$$

where each $X_{i_1 i_2}$ is either 0 or a (non-zero) multiple of a unitary. Moreover, we know by lemma 20 that $K_i X = \lambda X K_i$, and so we have that

$$K_{ij} X_{jk} = \lambda X_{jk} K_{ik}$$

for all i and all (j, k) . In the case that X_{jk} is non-zero, we therefore have, after multiplying both sides on the right by X_{jk}^* and using equation (12) with the roles of k and j reversed,

$$K_{ij} = \frac{1}{c_j} \lambda X_{jk} K_{ik} X_{jk}^*.$$

Since $\frac{X_{jk}}{\sqrt{c_j}}$ is unitary, and $|\lambda| = 1$, this expresses K_{ij} as a unitary conjugation of K_{ik} for all i ; that is, if Φ_i is the channel whose Kraus operators are $\{K_{ij}\}_{j=1}^n$, then $\Phi_j = \text{ad}_U \circ \Phi_k \circ \text{ad}_{U^*}$ with $U = \sqrt{\frac{\lambda}{c_j}} X_{jk}$. □

Combining these last results with Kuperberg's Theorem [22] and our main result from the last section, allows us to prove the following.

Theorem 22. *Let Φ be a unital channel. Then there exists an integer $k > 0$ such that Φ^k is mixed unitary.*

Proof. By lemma 17, perhaps by replacing Φ with $\alpha(\Phi)$, we can without loss of generality assume Φ has a commutative fixed point algebra. Then, lemmas 19 and 21 show that a high enough power, $M \geq 1$ say, of Φ has no non-trivial peripheral spectrum; for instance, M can be taken as the lowest common multiple of the m 's from lemma 19 applied to a representative from each of the irreducible channel unitary equivalence classes found in lemma 21.

Thus, Φ^M is a unital channel with no non-trivial peripheral spectrum, and so its peripheral algebra is just its fixed point algebra. We can now apply Kuperberg's Theorem in this case to find a subsequence $\{k_i\}$ such that $(\Phi^M)^{k_i} = \Phi^{Mk_i} \rightarrow \mathcal{E}_{\mathcal{A}}$ where \mathcal{A} is the fixed point algebra of Φ^M . By theorem 4, there is a ball around $\mathcal{E}_{\mathcal{A}}$ whose intersection with $\mathcal{F}(\mathcal{A})$, the set of unital channels with fixed point algebra \mathcal{A} , consists only of mixed unitaries, and so any channel in $\mathcal{F}(\mathcal{A})$ sufficiently close to $\mathcal{E}_{\mathcal{A}}$ is mixed unitary. Therefore, it follows that there is a k_N such that, for all $i > N$, the channel $(\Phi^M)^{k_i}$ is sufficiently close to $\mathcal{E}_{\mathcal{A}}$ that it is mixed unitary, and this completes the proof. \square

Remark 23. Notice that in order to obtain this result, we cannot use Kuperberg's Theorem directly with the conditional expectation onto the peripheral algebra; this is because the ball of mixed unitaries we obtain around $\mathcal{E}_{\mathcal{A}}$ is in the relative interior of $\mathcal{F}(\mathcal{A})$, the set of all unital channels with fixed point algebra \mathcal{A} . So if Φ^M only has peripheral algebra \mathcal{A} , but not fixed point algebra \mathcal{A} , although $\Phi^{Mk_i} \rightarrow \mathcal{E}_{\mathcal{A}}$, it may approach from outside the relative interior $\mathcal{F}(\mathcal{A})$ where the Theorem does not apply.

Remark 24. We also draw the attention of the reader to a conjecture called the 'Asymptotic Quantum Birkhoff Conjecture', which asks whether for a unital quantum channel $\Phi : M_n \rightarrow M_n$, it holds that,

$$\lim_{k \rightarrow \infty} d_{CB}(\Phi^{\otimes k}, MU(M_n^{\otimes k})) = 0,$$

where, as above, d_{CB} is the completely bounded distance of $\Phi^{\otimes k}$ to the set of mixed unitary maps on $M_n^{\otimes k}$. The conjecture was resolved in the negative by Haagerup and Musat ([13]). They introduced a new class of maps called *factorizable maps* and showed that maps which are not factorizable, fail to satisfy the above conjecture. In essence, this means that not every unital channel, after taking tensor powers with itself, becomes mixed unitary even if we take larger and larger tensor powers. In contrast, lemma 14 shows that every unital channel 'asymptotically becomes' mixed unitary. Quite significantly, theorem 22 goes further and uncovers an interesting aspect of unital channels the contrasts with tensor powers: it says under composition, every unital channel becomes mixed unitary after finitely many applications.

5. The case of the diagonal algebra: correlation matrices and Schur product channels

We finish by considering the case of the diagonal algebra in theorem 4 in more detail; that is, $\mathcal{A} = \Delta_d \cong \bigoplus_{k=1}^d \mathbb{C}1$, the algebra of $d \times d$ diagonal complex matrices. We shall give two alternate proofs of the theorem in this case using different approaches, and in doing so, we make connections with the theory of correlation matrices and Schur product maps [16, 29] (which have also recently arisen in other quantum information settings [14, 25, 31]), and Abelian group theory.

We begin by noting that the trace preserving conditional expectation onto Δ_d is the map-to-diagonal, defined by

$$\Delta(X) = \sum_{i=1}^d x_{ii} E_{ii}, \tag{13}$$

where $X = (x_{ij})$ and $E_{ij}, 1 \leq i, j \leq d$, are the matrix units for M_d .

Recall that a correlation matrix is a positive semi-definite matrix with 1's down its main diagonal. Further, the Schur (or Hadamard) product of two matrices $A = (a_{ij}), B = (b_{ij}) \in M_d$ is $A \circ B = (a_{ij} b_{ij})$. Given any $C \in M_d$, one can define a linear map $\Phi(X) = X \circ C$, and then Φ is completely positive if and only if C is a positive semidefinite matrix [29]. It is also clear that such a map is unital if and only if it is trace preserving.

Proposition 25 [23, 26]. Any unital channel $\Phi : M_d \rightarrow M_d$ whose fixed point algebra contains Δ_d is a Schur product channel; that is, there exists a correlation matrix C such that

$$\Phi(X) = X \circ C,$$

where \circ denotes the Schur product.

Since the commutant of $\mathcal{A} = \Delta_d$ is $\mathcal{A}' = \Delta_d$ again, as a consequence of proposition 25, we have theorem 4 restated in this particular case as follows.

Theorem 26. There exists a constant $0 \leq p \leq 1$ such that for all Schur product channels $\Phi : M_d \rightarrow M_d$, the map

$$p\Phi + (1-p)\Delta$$

is a mixed unitary channel defined by diagonal unitary matrices.

We provide the following alternative proof for this case.

Lemma 27. A channel $\Phi : M_d \rightarrow M_d$ is of the form UXU^* where U is a diagonal unitary if and only if $\Phi(X) = X \circ C$ where $C = zz^*$ is a rank-one correlation matrix with $z \in \mathbb{C}^d$ and $|z_i| = 1$ for all i .

Proof. If $U = \text{diag}(z_1, \dots, z_d)$ is unitary, then $|z_i| = 1$ and

$$UXU^* = \sum_{i,j} z_i z_j^* x_{ij} E_{ij} = X \circ C,$$

where $c_{ij} = z_i z_j^*$.

Conversely, if C is a rank-one correlation matrix, then $C = zz^*$ for some vector $z = (z_1, \dots, z_d)^T$. We have $c_{ii} = 1 = z_i z_i^* = |z_i|^2$, and now it is easy to see that $X \circ C$ is equal to UXU^* where $U = \text{diag}(z)$ is unitary since each $|z_i| = 1$. \square

Since the map-to-diagonal Δ is equal to the Schur-product channel with the correlation matrix I_d , theorem 26 can be restated as follows. This is the version that we prove; equivalence to the previously stated version follows by replacing all Schur product maps with their associated correlation matrices or vice-versa.

Theorem 28. *There exists a constant $0 \leq p \leq 1$ such that every $d \times d$ correlation matrix C satisfies that*

$$pC + (1 - p)I_d$$

is in the convex hull of rank-one correlation matrices.

Proof. Let C be a correlation matrix. Let $z = (z_1, \dots, z_d)^T$ where $|z_i| = 1$, and take the integral

$$\int_{z_1, \dots, z_d} z z^* \langle z, Cz \rangle d\mu(z_1) \cdots d\mu(z_d), \tag{14}$$

where the measure is just Haar measure on the unit circle. As $\langle z, Cz \rangle = \sum_{k,l=1}^d c_{kl} z_k^* z_l$, we can write this as

$$\sum_{k,l} c_{kl} \sum_{i,j} E_{ij} \int_z z_i z_j^* z_k^* z_l d\mu(z),$$

and since $\int z_i^k d\mu(z_i) = 0$ for any $k \neq 0$, the only non-zero terms in this sum come when either $i = j$ and $k = l$ or $i = k$ and $j = l$, or the intersection, $i = j = k = l$. Thus, to avoid double-counting, we get the following result:

$$\sum_{k,l} c_{kl} E_{kl} + \sum_{i,k} c_{kk} E_{ii} - \sum_i c_{ii} E_{ii}$$

which, since $c_{ii} = 1$, is just

$$C + (d - 1)I_d.$$

After suitably normalizing, we see that the integral gives $\frac{1}{d}(C + (d - 1)I_d)$. Since $z z^*$ is always a rank-one correlation matrix, and $\langle z, Cz \rangle$ is always positive, we have written this correlation matrix as a positive combination of rank-ones; normalizing makes it a convex combination, proving the result, with $p = \frac{1}{d}$. \square

Remark 29. We mention here that the above result elucidates the fact that the identity matrix is in the interior of the set of all correlation matrices that can be written as a convex combination of rank-1 correlation matrices. This fact was previously pointed out in the article [10] (cf section 4). Here we have found a new way to realize this fact and our method evidently provides better estimates of the convex combinations in some cases, based on a cursory comparison to the estimates of [10].

5.1. Group theory approach

Let G be an Abelian group. We now fix some notation. Since G is Abelian we use additive notation and hence 0 is the group identity. The group G^d is the Cartesian product of d copies of G . Reminiscent of the standard basis in linear algebra, if $G = \mathbb{Z}_m$ or $G = \mathbb{Z}$, then e_k denotes the element in G^d consisting of an d -tuple of elements of G where the k th element is 1 and all other elements are 0. So for instance, $e_i - e_j$ is the d -tuple of elements of G where the i th element is 1, the j th element is -1 , and all of other $n - 2$ elements are 0.

We let \widehat{G} be the set of all group homomorphisms from G to \mathbb{T} , the unit circle in the complex plane. The set \widehat{G} is a group under multiplication and is called the dual group. The Abelian

groups \mathbb{Z}^d and \mathbb{T}^d are duals to one another and any finite Abelian group is self-dual. While these are well known results in abstract harmonic analysis, it is illustrative to prove one of these results. Suppose h is a homeomorphism from \mathbb{Z}^d to \mathbb{T} , then h is completely determined by the d values $h(e_1), h(e_2), \dots, h(e_n)$. The map $h \rightarrow (h(e_1), h(e_2), \dots, h(e_n))$ is a group isomorphism between $\widehat{\mathbb{Z}^d}$ and \mathbb{T}^d proving that $\widehat{\mathbb{Z}^d} = \mathbb{T}^d$.

Let μ be any measure on an Abelian group G , then the Fourier transform of μ is the complex valued function on \widehat{G} defined as follows: $\widehat{\mu}(\chi) = \int_G \chi(g) d\mu(g)$. A complex-valued function on \widehat{G} is said to be positive definite if it is the Fourier transform of a measure on G .

We can characterize the convex hulls of rank one correlation matrices in both the real and the complex cases in terms of positive definite functions. The real version of the result which we present first is essentially equivalent to [4, proposition 2.1] and [28, theorem 7].

Theorem 30. *Let C be an $d \times d$ real matrix. Then C is in the convex hull of the real rank one correlation matrices if and only if there exists a positive definite function $f: \mathbb{Z}_2^d \rightarrow \mathbb{R}$ with the following properties:*

1. $f(0) = 1$
2. $f(e_i - e_j) = c_{ij}$ for $1 \leq i < j \leq d$

The complex version of this theorem, which we now state, appears to be new.

Theorem 31. *Let C be an $d \times d$ complex matrix. Then C is in the convex hull of the complex rank one correlation matrices if and only if there exists a positive definite function $f: \mathbb{Z}^d \rightarrow \mathbb{C}$ with the following properties:*

1. $f(0) = 1$
2. $f(e_i - e_j) = c_{ij}$ for $1 \leq i < j \leq d$.

We can combine these two versions into a common generalization as follows.

Theorem 32. *Let C be an $d \times d$ complex matrix. Let G be any topologically closed subgroup of \mathbb{T} . Then C is in the convex hull of the rank one correlation matrices with all entries in G if and only if there exists a positive definite function $f: \widehat{G}^d \rightarrow \mathbb{C}$ with the following properties:*

1. $f(0) = 1$
2. $f(e_i - e_j) = c_{ij}$ for $1 \leq i < j \leq d$

Setting $G = \mathbb{Z}_2$ in theorem 32 gives us theorem 30 and setting $G = \mathbb{T}$ in theorem 32 gives us theorem 31. Hence we only need prove theorem 32.

Proof. Let G be any topologically closed subgroup of \mathbb{T} . If v is any n -vector all of whose entries are in G , then let δ_v denote the probability measure on G^d satisfying $\delta_v(\{v\}) = 1$. Let $\widehat{\delta}_v$ be the corresponding positive definite function (i.e. for any $\chi \in \widehat{G}^d$, $\widehat{\delta}_v(\chi) = \int_G \chi(g) d\delta_v = \chi(v)$). If $\chi = (c_1, c_2, \dots, c_d) \in \widehat{G}^d$ and $v = (v_1, v_2, \dots, v_d) \in G^d$, then $\chi(v) = \prod_{k=1}^d v_k^{c_k}$. Hence $\widehat{\delta}_v(e_i - e_j) = v_i v_j^{-1} = v_i \overline{v_j}$ since $|v_j| = 1$. Therefore for all i, j , $\widehat{\delta}_v(e_i - e_j)$ is the (i, j) th entry of the matrix $v v^*$. Now if C is in the convex hull of the rank one correlation matrices with all entries in G , there exists $\{\lambda_i\}_i$ positive numbers summing to one and $\{v_i\}_i$ n -vectors having all elements in G such that $C = \sum_i \lambda_i v_i v_i^*$. It follows from linearity that the Fourier transform of the probability measure $\sum_i \lambda_i \delta_{v_i}$ is the f which satisfies all the hypotheses of the theorem. The converse follows by reversing the steps of this argument. For the $G = \mathbb{T}$ case, we note that the

set of all probability measures on \mathbb{T} is weak- $*$ compact by the Banach–Alaoglu theorem and hence is the closed convex hull of the point measures on \mathbb{T} by the Krein–Milman theorem. The result now follows using a similar argument to the topologically closed subgroup case. \square

We can use theorem 31 to construct an improvement on theorem 28. We begin with the following lemma which gives a useful example of a positive definite function on the integers.

Lemma 33. *Let c be a complex number of modulus less than or equal to one. Then the function $f_c(n) : \mathbb{Z} \rightarrow \mathbb{C}$ defined as*

$$f_c(n) = \begin{cases} c^n & n \geq 0 \\ \bar{c}^{|n|} & n < 0 \end{cases}$$

is positive definite.

Proof. Note that the Möbius transformation $g(z) = \frac{1}{1-z}$ maps the closed unit disk of the complex plane to the half plane $\{z : \operatorname{Re}(z) \geq \frac{1}{2}\}$. It follows from this that when $|c| \leq 1$ and $c \neq 1$, then $\widehat{f_c}(e^{i\theta}) = \sum_{k \in \mathbb{Z}} f_c(k) e^{ik\theta} = -1 + \frac{1}{1-ce^{i\theta}} + \frac{1}{1-ce^{-i\theta}} \geq 0$. Hence f_c is positive definite. The function f_1 is the Fourier transform of the point measure at zero and hence is positive definite. \square

This has some important implications for correlation matrices.

Corollary 34. *Let $v = (v_1, v_2, \dots, v_d) \in \mathbb{C}^d$ with $\|v\|_\infty \leq 1$ and let $M(v)$ denote the $d \times d$ matrix having the same off-diagonal entries as vv^* and all diagonal entries equal to one. Then $M(v)$ is in the convex hull of the complex rank one correlation matrices.*

Proof. It follows from the previous lemma that f_{v_k} is a positive definite function on \mathbb{Z} . Therefore a simple product measure argument shows us that $f(n_1, n_2, \dots, n_d) = \prod_{k=1}^d f_{v_k}(n_k)$ is a positive definite function $f : \mathbb{Z}^d \rightarrow \mathbb{C}$. Then $f(0) = 1$ and $f(e_i - e_j) = f_{v_i}(1)f_{v_j}(-1) = v_i \bar{v}_j$. Our result now follows from theorem 31. \square

Corollary 35. *Let C be a rank r complex correlation matrix. Then $\frac{1}{r}C + \frac{r-1}{r}I$ is in the convex hull of complex rank one correlation matrices.*

Proof. We must have vectors $\{v_k\}_{k=1}^r$ such that $C = \sum_{k=1}^r v_k v_k^*$; then all these vectors must satisfy $\|v_k\|_\infty \leq 1$. Since $\frac{1}{r}C + \frac{r-1}{r}I = \frac{1}{r} \sum_{k=1}^r M(v_k)$, our result now follows from corollary 34. \square

Remark 36. We note that this can be viewed as the complex version of [28, theorem 7] which gave an identical result for real correlation matrices. It was observed in [28] that [28, theorem 7] is not optimal at least in small dimensions, and it is likely that the same is true for corollary 35. We note that any extreme point of the set of $d \times d$ correlation matrices has rank at most $\lfloor \sqrt{d} \rfloor$ and hence for any $d \times d$ complex correlation matrix C , we have that $\frac{1}{\lfloor \sqrt{d} \rfloor}C + \frac{\lfloor \sqrt{d} \rfloor - 1}{\lfloor \sqrt{d} \rfloor}I$ is in the convex hull of complex rank one correlation matrices. This result is an improvement on [10, proposition 4.1].

Data availability statement

No new data were created or analysed in this study.

Acknowledgments

We are grateful for helpful comments from the referees. We thank John Watrous for communicating example 3 to us. D W K is partially supported by the NSERC Discovery Grant RGPIN-2018-400160. R P is partially supported by the NSERC Discovery Grant RGPIN-2022-04149. M R is supported by the Marie Skłodowska-Curie Fellowship from the European Union's Horizon research and innovation programme, Grant Agreement No. HORIZON-MSCA-2022-PF-01 (Project Number: 101108117).

ORCID iDs

David W Kribs  <https://orcid.org/0000-0001-9010-1144>

Rajesh Pereira  <https://orcid.org/0000-0002-3041-4672>

Mizanur Rahaman  <https://orcid.org/0000-0002-0301-0496>

References

- [1] Ahiable J, Kribs D W, Levick J, Pereira R and Rahaman M 2021 Entanglement breaking channels, stochastic matrices and primitivity *Linear Algebr. Appl.* **629** 219–31
- [2] Amato D, Facchi P and Konderak A 2023 Asymptotics of quantum channels *J. Phys. A: Math. Theor.* **56** 265304
- [3] Audenaert K M R and Scheel S 2008 On random unitary channels *New J. Phys.* **10** 023011
- [4] Balasubramian K, Gupta J C and Parthasarathy K R 1998 Remarks on Bell's inequality for spin correlations *Sankhya* **60** 29–35
- [5] Carbone R and Jenčová A 2020 On period, cycles and fixed points of a quantum channel *Ann. Henri Poincaré* **21** 155–88
- [6] Carlen E 2009 Trace inequalities and quantum entropy: an introductory course *Online Lecture Notes*
- [7] Choi M-D 1974 A Schwartz inequality for positive linear maps on C^* -algebras *Illinois J. Math.* **18** 285–90
- [8] Choi M-D 1975 Completely positive linear maps on complex matrices *Linear Algebr. Appl.* **10** 285–90
- [9] Davidson K R 1996 *C^* -Algebras by Example (Fields Institute Monograph Series)* (American Mathematical Society)
- [10] Dykema K and Juschenko K 2011 Matrices of unitary moments *Math. Scand.* **109** 225
- [11] Girard M, Leung D, Levick J, Li C-K, Paulsen V, Poon Y T and Watrous J 2022 On the mixed-unitary rank of quantum channels *Commun. Math. Phys.* **394** 919–51
- [12] Gurvits L 2003 Classical deterministic complexity of Edmonds' problem and quantum entanglement *Proc. 35th Annual ACM Symposium on Theory of Computing* pp 10–19
- [13] Haagerup U and Musat M 2011 Factorization and dilation problems for completely positive maps on von Neumann algebras *Commun. Math. Phys.* **303** 555–94
- [14] Harris S J, Levene R H, Paulsen V I, Plosker S and Rahaman M 2018 Schur multipliers and mixed unitary maps *J. Math. Phys.* **59** 112201
- [15] Hewitt E and Ross K A 2012 *Abstract Harmonic Analysis: Volume 1 Structure of Topological Groups Integration Theory Group Representations* vol 115 (Springer Science & Business Media)
- [16] Holevo A S 2019 Quantum systems, channels, information *Quantum Systems, Channels, Information* (de Gruyter)
- [17] Ioannou L M 2007 Computational complexity of the quantum separability problem *Quantum Inf. Comput.* **7** 335–70
- [18] Jacobson N 1985 *Basic Algebra I* 2nd edn (W.H. Freeman and Company)
- [19] Kraus K 1971 General state changes in quantum theory *Ann. Phys., NY* **64** 311–35
- [20] Kribs D W 2003 Quantum channels, wavelets, dilations and representations of O_n *Proc. Edinburgh Math. Soc.* **46** 421–33
- [21] Kribs D W, Levick J, Olfert K, Pereira R and Rahaman M 2021 Nullspaces of entanglement breaking channels and applications *J. Phys. A: Math. Theor.* **54** 105303

- [22] Kuperberg G 2003 The capacity of hybrid quantum memory *IEEE Trans. Inform. Theory* **49** 1465–73
- [23] Kye K 1995 Positive linear maps between matrix algebras which fix diagonals *Linear Algebr. Appl.* **216** 239–56
- [24] Lee C D-Y and Watrous J 2020 Detecting mixed-unitary quantum channels is NP-hard *Quantum* **4** 253
- [25] Levick J, Kribs D W and Pereira R 2017 Quantum privacy and Schur product channels *Rep. Math. Phys.* **80** 333–47
- [26] Li C-K and Woerdeman H 1997 Special classes of positive and completely positive maps *Linear Algebr. Appl.* **255** 247–58
- [27] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge University Press)
- [28] O’Meara C and Pereira R 2013 Self-dual maps and symmetric bistochastic matrices *Linear Multilinear Algebr.* **61** 23–34
- [29] Paulsen V 2002 *Completely Bounded Maps and Operator Algebras* (Cambridge University Press)
- [30] Pereira R 2006 Representing conditional expectations as elementary operators *Proc. Am. Math. Soc.* **134** 253–8
- [31] Puchała Z, Korzekwa K, Salazar R, Horodecki P and Życzkowski K 2021 Dephasing superchannels *Phys. Rev. A* **104** 052611
- [32] Rahaman M 2017 Multiplicative properties of quantum channels *J. Phys. A: Math. Theor.* **50** 345302
- [33] Rahaman M 2019 A new bound on quantum Wielandt inequality *IEEE Trans. Inf. Theory* **66** 147–54
- [34] Sanz M, Pérez-García D, Wolf M M and Cirac J I 2010 A quantum version of Wielandt’s inequality *IEEE Trans. Inf. Theory* **56** 4668–73
- [35] Simon B 2011 *Convexity: An Analytic Viewpoint* vol 187 (Cambridge University Press)
- [36] Watrous J 2009 Mixing doubly stochastic quantum channels with the completely depolarizing channel *Quantum Inf. Comput.* **9** 403–13
- [37] Watrous J 2018 *Theory of Quantum Information* (Cambridge University Press)
- [38] Werner R F and Holevo A S 2002 Counterexample to an additivity conjecture for output purity of quantum channels *J. Math. Phys.* **43** 4353–7
- [39] Wolf M M 2012 Quantum channels & operations: guided tour Lecture notes widely available online