On some classes of bipartite unitary operators

Julien Deschamps\(^1\), Ion Nechita\(^{2,3,5}\) and Clément Pellegrini\(^4\)

\(^1\) Dipartimento di Matematica, Università degli Studi di Genova, Via Dodecaneso, 35, I-16146 Genova, Italy
\(^2\) Zentrum Mathematik, M5, Technische Universität München, Boltzmannstrasse 3, D-85748 Garching, Germany
\(^3\) CNRS, Laboratoire de Physique Théorique, Toulouse, France
\(^4\) Institut de Mathématiques de Toulouse, Laboratoire de Statistique et de Probabilité, Université Paul Sabatier (Toulouse III), F-31062 Toulouse Cedex 9, France

E-mail: deschamps@dima.unige.it, nechita@irsamc.ups-tlse.fr and clement.pellegrini@math.univ-toulouse.fr

Received 16 February 2016, revised 19 May 2016
Accepted for publication 10 June 2016
Published 6 July 2016

Abstract

We investigate unitary operators acting on a tensor product space, with the property that the quantum channels they generate, via the Stinespring dilation theorem, are of a particular type, independently of the state of the ancilla system in the Stinespring relation. The types of quantum channels we consider are those of interest in quantum information theory: unitary conjugations, constant channels, unital channels, mixed unitary channels, positive partial transpose channels, and entanglement breaking channels. For some of the classes of bipartite unitary operators corresponding to the above types of channels, we provide explicit characterizations, necessary and/or sufficient conditions for membership, and we compute the dimension of the corresponding algebraic variety. Inclusions between these classes are considered, and we show that for small dimensions, many of these sets are identical.

Keywords: bipartite unitary operator, quantum channel, complete positivity, quantum entanglement
Mathematics Subject Classification: 47B65, 47A20, 94A40, 81P40
1. Introduction

In this work, we study some families of unitary operators acting on a tensor product of two finite dimensional Hilbert spaces, having some special properties in relation to the Stinespring dilation theorem. This fundamental result in operator algebras [22] states that any linear, completely positive, trace preserving map $L$ acting on $\mathcal{M}_n(\mathbb{C})$ can be written as

$$L(\rho) = [\text{id} \otimes \text{Tr}](U(\rho \otimes \beta)U^*),$$

where $U$ is a unitary operator acting on the tensor product $\mathbb{C}^n \otimes \mathbb{C}^k$, $\beta \in \mathcal{M}_k(\mathbb{C})$ is a positive semidefinite matrix of unit trace, and $k$ is a large enough parameter ($k = n^2$ suffices). In quantum information theory [20], the map $L$ is called a quantum channel, and the matrix $\beta$ is called a density matrix (or simply a quantum state). The Hilbert space $\mathbb{C}^k$ by which the original space $\mathbb{C}^n$ needs to be extended is called the environment, or the ancilla space.

The starting point of our investigation is the remark that the channel $L$ in (1) depends, a priori, on the quantum state $\beta$. In the practice of quantum theory, the environment space $\mathbb{C}^k$ is usually large (most of the times much larger than the system space $\mathbb{C}^n$), and thus it is inconvenient to describe the aforementioned dependence of $L$ on $\beta$. More precisely, we would like to characterize the unitary operators $U$, for which, independently on the value of $\beta$, the channel $L$ given by (1) belongs to some given class $\mathcal{L}$ of quantum channels.

In this work, we answer the question above for several classes $\mathcal{L}$ of relevance in quantum information theory: unitary conjugations $V \cdot V^*$, constant channels ($L(\rho)$ does not depend on the quantum state $\rho$), unital channels, ($L(I) = I$), mixed unitary channels (convex combinations of unitary conjugations), positive partial transpose (PPT) channels (channels for which the Choi matrix has a positive semidefinite partial transpose), and entanglement breaking channels (channel which, acting on one half of any entangled state, yield separable states).

This work is motivated by a conjecture formulated in [1, 2], where the emergence of ‘classical noise’ in quantum open systems is studied in details. In particular, it is shown that a particular class of bipartite unitary operators (the set $U^\mathbf{A}_{\text{block-diag}}$ in the present work, see (12)) gives rise to quantum evolutions which can be described by classical noises (obtuse complex random variables and complex normal martingales). Briefly speaking, bipartite unitary operators of $U^\mathbf{A}_{\text{block-diag}}$ are naturally associated to the so-called obtuse random variables (see [1] for all details on obtuse random variables). When implementing unitary operators of $U^\mathbf{A}_{\text{block-diag}}$ in the scheme of quantum repeated interactions, one recovers quantum Langevin equations as continuous time limit models (see [3] for the complete description of quantum repeated interaction models and the associated continuous time limits, and [2, section 1.2] for an example). More precisely, the quantum Langevin equations (or quantum stochastic differential equations$^6$) induced by this class of unitary operators can be described by (classical) stochastic differential equations, that is, driven by the usual Brownian motion or Poisson point process. Besides this ‘classical’ aspect, unitary operators of $U^\mathbf{A}_{\text{block-diag}}$ give rise to quantum channels which are convex combinations of unitary conjugations (the so-called mixed quantum channels), whatever is the state of the ancilla system. A natural question (conjecture) is whether these are the only ones (see [9, definition 9.3.6] for the motivation of this question; in particular, [9, chapter 9] is a preliminary version of [2]). In this work, we prove this conjecture, under some additional assumptions. We show also that the conjecture is true in a particular case corresponding to the case $n = 2$, without additional assumptions.

$^6$ A quantum stochastic differential equation is a stochastic equation driven by so-called quantum noises which are particular operators on Fock spaces [21].
summarize our main contribution informally in the following theorem; for precise statements, see theorem 7.1 and proposition 7.2; the technical assumption to which we are referring below is the linearity of the probabilities appearing in the convex decomposition of channels, see (11).

**Theorem 1.1.** Any bipartite unitary operator which, independently of the state of the ancilla, gives rise to mixed unitary channels, under some technical assumption, is a block-diagonal (or control) unitary operator. Moreover, for qubit channels, one can drop the technical assumption above.

It is very important to state at this time that we are not concerned with classes of channels, but with classes of bipartite unitary operators. Although these classes are defined in terms of channels, we are interested in characterizing the ‘interaction’ unitaries $U$ with the property that, for all ancilla states $\beta$, the channel $L$ given by (1) has some fixed set of properties. A similar question was studied in [16], where the authors characterize the unitary operators $U$ having the property that the only matrices $\beta$ which give quantum channels in (1) are quantum states.

The paper is structured as follows. In section 2 we define the classes of unitary operators we are interested in, and we present some general properties. Sections 3–7 deal each with one or more of these classes. We close the work with a section containing some open problems. Finally, in appendix, we discuss the block singular value decomposition of operators.

2. Some classes of unitary operators

Let us fix, once and for all, the space on which the unitary operators we investigate will act. Put $\mathcal{H}_A = \mathbb{C}^n$, $\mathcal{H}_B = \mathbb{C}^k$ and let $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^n \otimes \mathbb{C}^k$. The compact group of unitary operators acting on $\mathcal{H}_{AB} = \mathbb{C}^{nk}$ will be denoted by $\mathcal{U}_{nk}$ or, simply, $\mathcal{U}$:

$$\mathcal{U} := \mathcal{U}_{nk} = \{ U \in \mathcal{M}_{nk}(\mathbb{C}) \mid UU^* = U^*U = I \}. $$

Starting from the trace linear form $\text{Tr} : \mathcal{M}_k(\mathbb{C}) \rightarrow \mathbb{C}$ and the transposition operation $t : \mathcal{M}_k(\mathbb{C}) \rightarrow \mathcal{M}_k(\mathbb{C})$, define the *partial trace* and the *partial transposition* respectively by

$$ \text{Tr}_B = \text{id} \otimes \text{Tr} $$

$$ t_B = \text{id} \otimes t. $$

In other words

$$ \text{Tr}_B : \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C}) \rightarrow \mathcal{M}_n(\mathbb{C}) $$

$$ A \otimes B \mapsto (\text{Tr} B)A $$

and

$$ t_B : \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C}) \rightarrow \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C}) $$

$$ A \otimes B \mapsto A \otimes B^T. $$

Note that we use the following notation for the transposition $t(B) = B^T$. For obvious aesthetic reasons, we shall write $X^T = t_B(X)$.

We denote by $\mathcal{M}_k^{++}(\mathbb{C})$ the set of $k$-dimensional density matrices (or quantum states)

$$ \mathcal{M}_k^{++}(\mathbb{C}) := \{ \beta \in \mathcal{M}_k(\mathbb{C}) \mid \beta \geq 0 \text{ and } \text{Tr}(\beta) = 1 \}. $$

To a unitary transformation $U \in \mathcal{U}$ and a quantum state $\beta \in \mathcal{M}_k^{++}(\mathbb{C})$, we associate the quantum channel $L_{U,\beta} : \mathcal{M}_n(\mathbb{C}) \rightarrow \mathcal{M}_n(\mathbb{C})$ defined by the Stinespring formula (see, e.g., [20,
Let us introduce some classes of quantum channels having the unitary invariance property:
\[ \forall L \in \mathcal{L}, \ V_1, V_2 \in \mathcal{U}_n, \quad L(V_1 \cdot V_1^*) V_2^* \in \mathcal{L}. \]

We present next a list of such classes of channels, leaving the task of verifying the unitary invariance property as an exercise for the reader:

- **Unitary conjugations**
  \[ \mathcal{L}_{\text{aut}} = \{ X \mapsto VXV^* \}_{V \in \mathcal{U}_n}. \]

- **Constant channels**
  \[ \mathcal{L}_{\text{const}} = \{ L : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C}) : \exists \sigma \in \mathcal{M}_n^{1,+}(\mathbb{C}) \text{ s.t. } \forall \rho \in \mathcal{M}_n^{1,+}(\mathbb{C}), \ L(\rho) = \sigma \}. \]

- **Unital channels**
  \[ \mathcal{L}_{\text{unital}} = \{ L : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C}) : L(I_n) = I_n \}. \]

- **Mixed unitary channels**
  \[ \mathcal{L}_{\text{mixed}} = \text{conv} \{ X \mapsto VXV^* \}_{V \in \mathcal{U}_n}. \]

- **PPT channels**
  \[ \mathcal{L}_{\text{PPT}} = \{ L : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C}) : \forall \rho \in \mathcal{M}_n^{1,+}(\mathbb{C}), \ ||L \otimes \text{id}_n(\rho)||^2 \geq 0 \}. \]

- **Entanglement breaking channels**
  \[ \mathcal{L}_{\text{EB}} = \{ L : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C}) : \forall \rho \in \mathcal{M}_n^{1,+}(\mathbb{C}), \ [L \otimes \text{id}_n](\rho) \text{ is separable} \}. \]

We move next to the main definition of this paper, the classes of bipartite unitary channels we are interested in. These classes are defined in a natural way as the set of unitary operators inducing, via the Stinespring formula (2), independent of the state \( \beta \) of the environment system \( B \), quantum channels belonging to one of the classes above. This exact notion, in the case of degradable channels and entanglement breaking channels, has been considered respectively in [17, definition 15] and [18]; similar questions were investigated in [15, 25], where the authors call them ‘quantum processors’. More precisely, we define, for any \( * \in \{ \text{aut, const, unital, mixed, PPT, EB} \} \),
\[ \mathcal{U}_* = \{ U \in \mathcal{U}_{id} | \forall \beta \in \mathcal{M}_n^{1,+}(\mathbb{C}), L_{U,\beta} \in \mathcal{L}_* \}. \]
We have, in order:

\[
\mathcal{U}_{\text{aut}} = \{ U \in \mathcal{U}_n \mid \forall \beta \in \mathcal{M}_k^{1+}(\mathbb{C}), L_{U,\beta}(\rho) = V_\beta \rho V_\beta^* \text{ for some } V_\beta \in \mathcal{U}_n \},
\]

\[
\mathcal{U}_{\text{const}} = \{ U \in \mathcal{U}_n \mid \forall \beta \in \mathcal{M}_k^{1+}(\mathbb{C}), L_{U,\beta} \text{ is a constant channel} \},
\]

\[
\mathcal{U}_{\text{unital}} = \{ U \in \mathcal{U}_n \mid \forall \beta \in \mathcal{M}_k^{1+}(\mathbb{C}), L_{U,\beta}(I) = I \},
\]

\[
\mathcal{U}_{\text{mixed}} = \{ U \in \mathcal{U}_n \mid \forall \beta \in \mathcal{M}_k^{1+}(\mathbb{C}), L_{U,\beta}(X) = \sum_{i=1}^r p_i(\beta) U_i(\beta) X U_i(\beta)^* \\
\quad \text{with } p_i(\beta) \geq 0, \sum_{i=1}^r p_i(\beta) = 1 \text{ and } U_i(\beta) \in \mathcal{U}_n \},
\]

\[
\mathcal{U}_{\text{PPT}} = \{ U \in \mathcal{U}_n \mid \forall \beta \in \mathcal{M}_k^{1+}(\mathbb{C}), L_{U,\beta} \text{ is a PPT channel} \},
\]

\[
\mathcal{U}_{\text{EB}} = \{ U \in \mathcal{U}_n \mid \forall \beta \in \mathcal{M}_k^{1+}(\mathbb{C}), L_{U,\beta} \text{ is an entanglement breaking channel} \}.
\]

In relation to the class \( \mathcal{U}_{\text{aut}} \), we also define (see section 3)

\[
\mathcal{U}_{\text{single}} = \{ U \in \mathcal{U}_n \mid \text{the set } \{ L_{U,\beta} : \beta \in \mathcal{M}_k^{1+}(\mathbb{C}) \} \text{ has 1 element} \}.
\]

One of the original motivations of this work was to obtain a characterization of the set \( \mathcal{U}_{\text{mixed}} \). As stepping stones towards a description of this set, we introduce the following classes of bipartite unitary operators:

\[
\mathcal{U}_{\text{prob}} = \{ U \in \mathcal{U}_n \mid \exists U_i \in \mathcal{U}_n \text{ s.t. } \forall \beta \in \mathcal{M}_k^{1+}(\mathbb{C}), L_{U,\beta}(X) = \sum_{i=1}^r p_i(\beta) U_i(\beta) X U_i(\beta)^* \\
\quad \text{with } p_i(\beta) \geq 0 \text{ and } \sum_{i=1}^r p_i(\beta) = 1 \},
\]

\[
\mathcal{U}_{\text{prob-lin}} = \{ U \in \mathcal{U}_n \mid \exists U_i \in \mathcal{U}_n \text{ s.t. } \forall \beta \in \mathcal{M}_k^{1+}(\mathbb{C}), L_{U,\beta}(X) = \sum_{i=1}^r p_i(\beta) U_i(\beta) X U_i(\beta)^* \\
\quad \text{with linear functions } p_i(\beta) \geq 0 \text{ and } \sum_{i=1}^r p_i(\beta) = 1 \},
\]

\[
\mathcal{U}^A_{\text{block-diag}} = \{ U \in \mathcal{U}_n \mid U = \sum_{i=1}^k U_i \otimes e_{f_i}^*, \text{ with } U_i \in \mathcal{U}_n \text{ and } \{ e_i \}, \{ f_i \} \text{ orthonormal bases in } \mathbb{C}^k \},
\]

\[
\mathcal{U}^B_{\text{block-diag}} = \{ U \in \mathcal{U}_n \mid U = \sum_{i=1}^n e_{f_i}^* \otimes U_i, \text{ with } U_i \in \mathcal{U}_n \text{ and } \{ e_i \}, \{ f_i \} \text{ orthonormal bases in } \mathbb{C}^n \}.
\]

Note that the elements \( \mathcal{U}^A_{\text{block-diag}}, \mathcal{U}^B_{\text{block-diag}} \) are known in the literature as \textit{control unitary operators}.

Let us mention at this point a simple but fundamental property of the sets of bipartite unitary matrices we have just introduced.

\textbf{Lemma 2.1.} The local unitary group \( \mathcal{U}_n \times \mathcal{U}_k \) acts by left and right multiplication on \( \mathcal{U}_n \), for all \( \ast \in \{ \text{aut, const, unital, mixed, PPT, EB, single, prob, prob-lin, block-diag-A, block-diag-B} \} \).
\forall U \in \mathcal{U}_n, \forall V_1, V_2 \in \mathcal{U}_n, \forall W_1, W_2 \in \mathcal{U}_k, \quad (V_1 \otimes W_1)U(V_2 \otimes W_2) \in \mathcal{U}_n.

**Proof.** In the case of \(* \in \{\text{aut, const, unital, mixed, PPT, EB}\},\) the proof follows from the bi-unitary invariance of the corresponding class \(\mathcal{L}_n\) and from the fact that in the definition of \(\mathcal{U}_n\), we require the condition to hold for all states on the environment \(\beta \in \mathcal{M}_{k}^{+}(\mathbb{C})\). The other cases are easy verifications, we leave the details to the reader. \(\square\)

As suggested by the property above, the subgroup \(\mathcal{U}_n \otimes \mathcal{U}_k \subseteq \mathcal{U}_{nk}\) plays an important role in our study. It turns out that the flip operator

\[
F_n : \mathbb{C}^n \otimes \mathbb{C}^n \to \mathbb{C}^n \otimes \mathbb{C}^n, \quad F_n x \otimes y = y \otimes x
\]

will also be of particular importance, in light of the following classical theorem.

**Theorem 2.2.** ([10, theorem 3.1]) Let \(G\) be a compact group such that \(\mathcal{U}_n \otimes \mathcal{U}_k \subseteq G \subseteq \mathcal{U}_{nk}\). Then \(G\) is one of the following:

1. \(G = \mathcal{U}_n \otimes \mathcal{U}_k\);
2. \(G = \mathcal{U}_{nk}\);
3. If \(n = k\), \(G = \langle \mathcal{U}_n \otimes \mathcal{U}_n, F_n \rangle\).

By direct computation, one can show that the following chain of inclusions holds:

\[
\mathcal{U}_{\text{block-diag}} \subseteq \mathcal{U}_{\text{prob}} \subseteq \mathcal{U}_{\text{mixed}} \subseteq \mathcal{U}_{\text{unital}} \subseteq \mathcal{U}.
\]

Note that one can define ‘\(B\)’-versions of the above sets, in an obvious way, by swapping the tensor factors \(A\) and \(B\) (above inclusions are still true for \(\mathcal{U}_{nk}\)).

One of the main focuses of the current work will be to understand which are the inclusions above which are strict and which are actually equalities.

We end this section by showing that if two interaction unitary operators \(U, V\) generate the same channels for all states \(\beta\) on the environment, then they are related by a unitary operator acting on the environment \(\mathcal{C}^k\); this result will turn out to be useful later on.

**Lemma 2.3.** Let \(U, V \in \mathcal{U}_{nk}\) be two bipartite unitary operators. The following two assertions are equivalent:

1. For all density matrix on \(\beta \in \mathcal{M}_{k}^{+}(\mathbb{C})\), the quantum channels \(U\) and \(V\) induce are equal: \(L_{U,\beta}(\rho) = L_{V,\beta}(\rho)\) for all \(\rho \in \mathcal{M}_{k}^{+}(\mathbb{C})\);
2. There exists a unitary operator \(W \in \mathcal{U}_k\) such that \(U = (I \otimes W)V\).

**Proof.** We only prove ‘\(1 \implies 2\)’, since the converse follows from direct calculation. We start form the hypothesis

\[
\forall \rho \in \mathcal{M}_{n}^{+}(\mathbb{C}), \forall \beta \in \mathcal{M}_{k}^{+}(\mathbb{C}), \quad [\text{id} \otimes \text{Tr}](U\rho \otimes \beta U^*) = [\text{id} \otimes \text{Tr}](V\rho \otimes \beta V^*).
\]

By linearity, we can replace \(\rho\), respectively \(\beta\), by arbitrary complex matrices \(A \in \mathcal{M}_n(\mathbb{C})\), respectively \(B \in \mathcal{M}_k(\mathbb{C})\). Again using linearity, we replace the simple tensor \(A \otimes B\) by a general element \(X \in \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C})\) to obtain the first line below, and we continue by obvious equivalent reformulations:
∀X ∈ \mathcal{M}_{nk}(\mathbb{C}), \quad [\text{id} \otimes \text{Tr}](UXU^*) = [\text{id} \otimes \text{Tr}](VXV^*)
\forall X ∈ \mathcal{M}_{nk}(\mathbb{C}), \quad ∀A ∈ \mathcal{M}_{nk}(\mathbb{C}), \quad \text{Tr}(UXU^* A \otimes I) = \text{Tr}(VXV^* A \otimes I)
\forall X ∈ \mathcal{M}_{nk}(\mathbb{C}), \quad ∀A ∈ \mathcal{M}_{nk}(\mathbb{C}), \quad \text{Tr}(XU^* A \otimes IU) = \text{Tr}(XV^* A \otimes IV)
\forall A ∈ \mathcal{M}_n(\mathbb{C}), \quad U^* A \otimes IU = V^* A \otimes IV
\forall A ∈ \mathcal{M}_n(\mathbb{C}), \quad A \otimes I(UV^*) = (UV^*)A \otimes I
\exists W ∈ \mathcal{M}_n(\mathbb{C}), \quad UV^* = I \otimes W
and we conclude the proof by noticing that W has to be unitary, since UV* is.

3. Bipartite unitary operators producing unitary conjugations and constant channels

In this section we provide characterizations of the sets \( \mathcal{U}_{\text{aut}} \) (3), \( \mathcal{U}_{\text{single}} \) (9), and \( \mathcal{U}_{\text{const}} \) (4), showing that only tensor products of unitary operators (respectively flipped tensor products) belong to these classes.

We start with the set of automorphisms, that is the set of unitary conjugation channels.

**Theorem 3.1.** Let \( U ∈ \mathcal{U}_k \) a bipartite unitary operator such that, for all quantum states \( \beta ∈ \mathcal{M}_k^{1+}(\mathbb{C}) \), there exists an unitary operator \( V_β ∈ \mathcal{U}_n \) such that \( L_{U, β}(ρ) = V_β ρ V_β^* \) for all \( ρ ∈ \mathcal{M}_n^{1+}(\mathbb{C}) \). Then, there exist unitary operators \( V ∈ \mathcal{U}_n \) and \( W ∈ \mathcal{U}_k \) such that \( U = V \otimes W \). In other words
\[ \mathcal{U}_{\text{aut}} = \{ V \otimes W : \ V ∈ \mathcal{U}_n, \ W ∈ \mathcal{U}_k \}. \]

**Proof.** The proof is easy, and consists of two steps: we show first that the unitary operators \( V_β \) can be chosen to not depend on \( β \), and then, using lemma 2.3, we show that the unitary \( U \) has the required form.

Let us first introduce some notation. To any matrix
\[ \mathcal{M}_n(\mathbb{C}) \ni A = \sum_{i,j=1}^n A_{ij} e_i e_j^*, \]
associate its vectorization \( a = \text{vect}(A) \) defined by
\[ \mathbb{C}^n \otimes \mathbb{C}^n \ni a = \sum_{i,j=1}^n A_{ij} e_i \otimes e_j, \]
where \( \{ e_i \}_{i=1}^n \) is some fixed orthonormal basis of \( \mathbb{C}^n \).

Denote \( V := V_1(k) \), the unitary which appears for \( β = I/k \), and let \( v = \text{vect}(V) \). For an arbitrary \( β ∈ \mathcal{M}_k^{1+}(\mathbb{C}) \), let \( \beta = (β + I/k)/2. \) Since quantum channels are linear in \( β \), we have that
\[ ∀ \rho ∈ \mathcal{M}_n^{1+}(\mathbb{C}), \quad 2V_β ρ V_β^* = V_β^* ρ V_β + V_β ρ V_β^*. \]
At the level of Choi matrices, the above equation reads
\[ 2v_β v_β^* = v_β^* v_β + vv*. \]
On the left side of the equation above the operator is a rank one operator. This way, in order that the sum in the right side is a rank one operator, the vector has to be proportional. Since all
the involved vectors are of norm $\sqrt{n}$, it follows that they should all be the same, up to a phase. The same holds for the unitary operators, which concludes the first step of the proof.

Let $\bar{U} := V \otimes I$. It is easy to see that

$$\forall \rho \in \mathcal{M}_n^{1,+}(\mathbb{C}), \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), \quad L_{\bar{U},\beta}(\rho) = V \rho V^* = L_{U,\beta}(\rho),$$

so, by lemma 2.3, there exists an unitary operator $W \in \mathcal{U}_k$ such that $U = (I \otimes W) \bar{U}$, and the proof is complete.

We show next that the class $\mathcal{U}_{\text{single}}$, i.e. the set of unitary operators $U \in \mathcal{U}_{nk}$ with the property that the map $\beta \mapsto L_{U,\beta}$ is constant, is actually identical to $\mathcal{U}_{\text{aut}}$.

For the proof of theorem 3.3, we need the following lemma.

**Lemma 3.2.** Let $M \in \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C})$ be a given matrix. The following conditions are equivalent:

1. For all matrices $X \in \mathcal{M}_n(\mathbb{C})$ and $Y \in \mathcal{M}_k(\mathbb{C})$ such that $\text{Tr} Y = 0$, we have $\text{Tr}(M \cdot X \otimes Y) = 0$;
2. There exist a matrix $A \in \mathcal{M}_n(\mathbb{C})$ such that $M = A \otimes I_k$.

**Proof.** The non-trivial implication follows from the following equation

$$[\mathcal{M}_n(\mathbb{C}) \otimes (\mathcal{M}_k(\mathbb{C}) \otimes \mathbb{C}I)]^* = \mathcal{M}_n(\mathbb{C}) \otimes \mathbb{C}I.$$

**Theorem 3.3.** Let $U \in \mathcal{U}_{nk}$ a bipartite unitary operator such that, for all quantum states $\rho \in \mathcal{M}_n^{1,+}(\mathbb{C})$ and $\beta, \gamma \in \mathcal{M}_k^{1,+}(\mathbb{C})$, we have that $L_{U,\beta}(\rho) = L_{U,\gamma}(\rho)$. Then, there exist unitary operators $V \in \mathcal{U}_n$ and $W \in \mathcal{U}_k$ such that $U = V \otimes W$. In other words, the set $\mathcal{U}_{\text{single}}$ defined in (9) is equal to

$$\mathcal{U}_{\text{single}} = \{ V \otimes W : V \in \mathcal{U}_n, W \in \mathcal{U}_k \} = \mathcal{U}_{\text{aut}}.$$

**Proof.** By using linearity, the hypothesis translates to the following equality

$$\forall X, Y \in \mathcal{M}_n(\mathbb{C}), \forall Z \in \mathcal{M}_k(\mathbb{C}) \text{ s.t. } \text{Tr} Z = 0, \quad \text{Tr}[(U \otimes Z)U^*(Y \otimes I_k)] = 0.$$

By reshaping the operator $U$, the previous equality can be re-written as

$$\text{Tr}[Y^T \otimes X \otimes Z : U^*U] = 0.$$

By using linearity, the hypothesis translates to the following equality

$$\forall X, Y \in \mathcal{M}_n(\mathbb{C}), \forall Z \in \mathcal{M}_k(\mathbb{C}) \text{ s.t. } \text{Tr} Z = 0, \quad \text{Tr}[(U \otimes Z)U^*(Y \otimes I_k)] = 0.$$

By reshaping the operator $U$, the previous equality can be re-written as

$$\text{Tr}[Y^T \otimes X \otimes Z : U^*U] = 0.$$

where $\hat{U} \in \mathcal{M}_{nk \times nk}(\mathbb{C})$ is the operator

$$\hat{U} = \sum_{i,j=1}^n \sum_{k,l=1}^k (e_i \otimes f_k, U e_j \otimes f_j) f_k^* (e_j^* \otimes e_i^* \otimes f_j^*),$$

see figure 1 for a graphical representation of $\hat{U}$ and of the previous equality (for the Penrose graphical notation for tensors, in the form used here, see [7, section 3]). From lemma 3.2, it follows that there exist an operator $A \in \mathcal{M}_n^{1,+}(\mathbb{C})$ such that $\hat{U}^* \hat{U} = A \otimes I_k$. Since the rank of $\hat{U}^* \hat{U}$ is at most $k$, it follows that $A$ has rank at most 1, i.e. there exists a vector $a \in \mathbb{C}^n \otimes \mathbb{C}^n$ such that $A = aa^*$. From the equality $\hat{U}^* \hat{U} = aa^* \otimes I_k$, we deduce that there exists an operator $W \in \mathcal{U}_k$ such that $\hat{U} = a^* \otimes W$. Writing
we get $U = V \otimes W$. The fact that $V \in \mathcal{U}_\rho$ follows from the unitarity of $U$, and this concludes
the proof of the first implication. The fact that tensor product unitary operators belong to $\mathcal{U}_{\text{single}}$
can be verified by direct computation.

For the case of $\mathcal{U}_{\text{const}}$, it is easy to see that it is related to the previous case via a flip
operation, although there is a slight technical complication. This question has also been
considered in [18].

**Theorem 3.4.** Consider the set $\mathcal{U}_{\text{const}}$ of bipartite unitary operators such that, for all
quantum states $\rho, \sigma \in \mathcal{M}_n^{+}(\mathbb{C})$ and $\beta \in \mathcal{M}_k^{+}(\mathbb{C})$, we have that $L_{U,\beta}(\rho) = L_{U,\beta}(\sigma)$.

If $k = nr$ for $r = 1, 2, \ldots$, then $\mathcal{U}_{\text{const}}$ is empty.

If $k = nr$ for some positive $r$, then we have

$$\mathcal{U}_{\text{const}} = \{(I_n \otimes V)(F_n \otimes I_k)(I_n \otimes W) : V, W \in \mathcal{U}_k\},$$

where $F_n \in \mathcal{U}_n$ denotes the flip operator (14); see figure 2 for the diagrammatic
representation of such an operator.

**Proof.** Let us start with the easy implication, considering an operator $U$ as in (16). By direct
computation, one can see that

$$L_{U,\beta}(\rho) = [\text{id}_n \otimes \text{Tr}_r](\beta),$$

proving that, for arbitrary $\beta$, the channel $L_{U,\beta}$ is constant.

The proof of the difficult implication starts in the same way as the one of theorem 3.3.

The hypothesis that the channels $L_{U,\beta}$ are constant translates to the following condition:

$$\forall X, Y \in \mathcal{M}_n(\mathbb{C}), \forall Z \in \mathcal{M}_k(\mathbb{C}) \text{ s.t. } \text{Tr} X = 0, \quad \text{Tr}[U(X \otimes Z)U^*Y \otimes I_k] = 0.$$

As before, after reshaping the matrix $U$ into $\hat{U}$, the previous relation becomes (15), with the
difference that this time, we have $\text{Tr} X = 0$. Using lemma 3.2, we conclude that there exists
an operator $A \in \mathcal{M}_{nk}(\mathbb{C})$ such that
where the superscripts indicate on which factor of the tensor products the operators are acting (A acts on the first copy of $\mathbb{C}^n$ and on $\mathbb{C}^k$, while the identity operator acts on the second copy of $\mathbb{C}^n$). Using the fact that $U$ is unitary, we have that the rank of the matrix $\hat{U}^* \hat{U}$ is precisely $k$, so we must have $k = n \times \text{rank}(A)$. We conclude that if $k$ is not a multiple of $n$, then operators $U$ with the above property cannot exist. We put now $r := \text{rank}(A)$, so that $k = mn$. Since $\hat{U}^* \hat{U}$ is a positive semidefinite matrix, $A$ is a positive semidefinite matrix of rank $r$, so we write $A = B^* B$, for a matrix $B \in \mathcal{M}_{r \times nk}(\mathbb{C}) = \mathcal{M}_{r \times nk}(\mathbb{C})$. The fact that $U$ is unitary translates to the following equality

$$\hat{B}B^* = I_{nr},$$

where

$$\mathcal{M}_{nr}(\mathbb{C}) \ni \hat{B} = \sum_{i,j=1}^{r} \sum_{x,y=1}^{n} \langle g_x, Be_i \otimes e_j \otimes g_y \rangle e_i \otimes g_x \cdot e_j^* \otimes g_y^*,$$

for some orthonormal basis $\{g_1, \ldots, g_n\}$ of $\mathbb{C}^r$; see figure 3 for a graphical representation of the previous equalities. Thus $W := \hat{B}$ is a unitary operator. From equation (17), we find that there is another unitary operaor $V \in \mathcal{U}_{nr}$ such that

$$U^{(1,2,3)} = (I^{(1)}_{n} \otimes V^{(2,3)}) \cdot (F^{(1,2)}_{\hat{U}} \otimes I^{(3)}_{r}) \cdot (I^{(1)}_{n} \otimes W^{(2,3)}),$$

where the three tensor legs correspond to $\mathbb{C}^n \otimes \mathbb{C}^n \cong \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$. The conclusion follows.

\begin{remark}
If $n = k$ in the previous result, equation (16) can be written as $U = F_{\hat{U}}(V \otimes W)$ for a pair of unitary operators $V, W \in \mathcal{U}_n$, so in this case we have

$$\mathcal{U}_{\text{const}} = F_{\hat{U}} \mathcal{U}_{\text{single}} = \mathcal{U}_{\text{single}} F_{\hat{U}}.$$

\end{remark}

### 4. Bipartite unitary operators producing unital channels

In this section we study the set $\mathcal{U}^A_{\text{unital}}$ of bipartite unitary operations which yield unital channels for every choice of the state on the auxiliary space.

Using linearity, one can extend the definition (5) to the whole space of $k \times k$ complex matrices:

$$\mathcal{U}_{\text{unital}} = \{U \in \mathcal{U} \mid \forall B \in \mathcal{M}_k(\mathbb{C}), \ L_{U,B}(I) = (\text{Tr } B)I \}.$$
Theorem 4.1. One has
\[ \mathcal{U}_{\text{unital}} = \mathcal{U}_n \cap \mathcal{U}_{n,k}^\text{unital}. \]
In particular, \( \mathcal{U}_n^\text{unital} = \mathcal{U}_{n,k}^\text{unital}. \)

Proof. Let us first show the ‘\( \subseteq \)' inclusion in the above equality. Take \( U \in U_{\text{unital}} \) and put \( V = U^\dagger \in \mathcal{M}_k(\mathbb{C}) \), and \( W = VV^\dagger \). One has, for any \( B \in \mathcal{M}_k(\mathbb{C}) \),
\[
(\text{Tr } B)I_n = L_{U,B}(I_n) = [\text{id} \otimes \text{Tr}](U \otimes I \otimes B \cdot U^\dagger),
\]
\[
= [\text{id} \otimes \text{Tr}](VV^\dagger \cdot I \otimes B^\dagger)
= [\text{id} \otimes \text{Tr}](W \cdot I \otimes B^\dagger).
\] (19)

By block-decomposing \( W \) in an arbitrary orthonormal basis \( e_j \) of \( \mathbb{C}^k \)
\[
W = \sum_{i,j=1}^k W_{ij} \otimes e_i e_j^\dagger,
\]
we get that for all \( B \in \mathcal{M}_k(\mathbb{C}) \),
\[
(\text{Tr } B)I_n = \sum_{i,j=1}^k W_{ij} \cdot \langle e_j, Be_i \rangle.
\] (20)

Choosing \( B = e_i e_i^\dagger \), we get \( W_{ij} = \delta_{ij} I_n \) and hence \( W = I_n \). In other words, \( V = U^\dagger \in \mathcal{U}_n \), which finishes the proof of the first inclusion.

The second inclusion follows by working backwards the previous arguments: since \( V = U^\dagger \in \mathcal{U}_n \), equations (20) and (19) hold.

Since both sets \( \mathcal{U}_n \) and \( \mathcal{U}_n^\text{unital} \) are algebraic varieties (i.e. they can be describes as the zero-set of a system of polynomial equations), we obtain the following corollary.

Corollary 4.2. The set \( \mathcal{U}_{\text{unital}} \) is a real algebraic variety.

We are going to investigate next \( \mathcal{U}_{\text{unital}} \), as an algebraic variety. In order to get an estimate of the size of \( \mathcal{U}_{\text{unital}} \), we shall compute a proxy for its dimension, that is the number of real parameters needed to describe it. More precisely, we shall compute the dimension of the ‘enveloping tangent space’ of \( \mathcal{U}_{\text{unital}} \) at a point which is a block-diagonal unitary.

\[ U = \sum_{i=1}^k U_i \otimes e_i f_i^\dagger \in \mathcal{U}_{\text{block-diag}}^A. \]

The notion of enveloping tangent spaces was introduced in [23] (also called defect), and it is simply defined by (see also [5])
\[
\tilde{T}_U(\mathcal{U}_{\text{unital}}) := T_U(\mathcal{U}_n) \cap T_U(\mathcal{U}_n^\text{unital}).
\]

Proposition 4.3. The dimension of the enveloping tangent space of \( \mathcal{U}_{\text{unital}} \) at a point which is a block-diagonal unitary of the form
\[ U = \sum_{i=1}^{k} U_i \otimes e_i f_i^* \]

is given by

\[ D_U = \sum_{i,j=1}^{k} \sum_{(\lambda, d_i) \in \Lambda_i} d_i^2, \quad (21) \]

where \( \Lambda_i \) is the set \{ (\lambda, d_i) \} where \( \lambda \) is an eigenvalue of the unitary operator \( U_i U_j^* \) having multiplicity \( d_i \).

**Proof.** A matrix \( A \in \mathcal{M}_{nk}(C) \) is an element of the enveloping tangent space at \( U \) if and only if both matrices \( U + \varepsilon A \) and \( (U + \varepsilon A)^\dagger \) are unitary, up to the first order in \( \varepsilon \). The unitarity of \( U + \varepsilon A \) is equivalent to the condition \( U A^\varepsilon + A U^\varepsilon = 0 \), while the unitarity of \( (U + \varepsilon A)^\dagger \) is equivalent to \( U A^\varepsilon + A U^\varepsilon = 0 \) (note that we have used the fact \( U = U^\dagger \)).

Writing \( A \) as a block matrix

\[ A = \sum_{i,j} A_{ij} \otimes e_i f_j^*, \]

the first condition \( U A^\varepsilon + A U^\varepsilon = 0 \) is equivalent to the following system of equations

\[ \forall i, j, \quad U A_{ij}^\varepsilon + A_{ij} U_j^\varepsilon = 0, \]

while the condition \( U (A^\varepsilon)^* + A^U U^* = 0 \) is equivalent to

\[ \forall i, j, \quad U A_{ij}^\varepsilon + A_{ij} U_j^* = 0. \]

First, let us note that the diagonal blocks \( A_{ii} \) appear only in two identical equations

\[ U A_{ii}^\varepsilon + A_{ii} U_i^\varepsilon = 0. \]

The general solution to the equation above is \( A_{ii} = B_{ii} U_i \), where \( B_{ii} \) is an arbitrary anti-hermitian matrix \( (B_{ii} + B_{ii}^* = 0) \). Hence, the total dimension of the diagonal blocks of \( A \) is \( kn^2 \). Note that this corresponds to the case \( i = j \) in formula (21); there, \( \Lambda_i = \{ (1, n) \} \).

Let us now study off-diagonal blocks of \( A \). Again, the equations are decoupled: for \( i < j \), one has to solve

\[ U A_{ij}^\varepsilon + A_{ij} U_j^\varepsilon = 0, \quad (22) \]

\[ U A_{ji}^\varepsilon + A_{ji} U_i^\varepsilon = 0. \quad (23) \]

From the first equation, one finds \( A_{ji} = -U_j A_{ij}^* U_i \). Plugging this into the second equation, we have to solve now

\[ RA_{ij} - A_{ij} S = 0, \]

where \( R = U_j U_i^* \) and \( S = U_i^* U_j \). This is the well-known Sylvester equation. From the analysis in [12, chapter VIII], the dimension of the solution space of this homogenous equation depends of the Jordan block structure of the matrices \( R \) and \( S \). Since in our case both \( R \) and \( S \) are unitary (hence diagonalizable), the Jordan blocks have unit dimension. Moreover, \( R \) and \( S \) have the same spectrum \( \Lambda_{ij} \). It follows from [12, chapter VIII, equation (19)] that the complex dimension of the solutions of the system (22) and (23) is precisely

\[ \sum_{(\lambda, d_i) \in \Lambda_i} d_i^2, \]

and the proof is complete. \( \square \)
The proof above can be adapted \textit{mutatis mutandis} to the case of \((B)\)-classical unitary operators, as follows.

**Corollary 4.4.** The same result holds for \(B\)-block-diagonal unitary operators of the from
\[
U = \sum_{i=1}^{n} e_i f_i^* \otimes U_i.
\]

**Corollary 4.5.** The dimension of the enveloping tangent space of \(\mathcal{U}_{\text{unital}}\) at a product unitary operator \(U = V \otimes W\) is \(n^2 k^2\), which is also the dimension of \(\mathcal{U}_{nk}\).

**Corollary 4.6.** For \(k = 2\), the dimension of the enveloping tangent space of \(\mathcal{U}_{\text{unital}}\) at a point \(U = I \otimes V = I \otimes e_k f_k^* + V \otimes e_2 f_2^*\) is
\[
D_U \leq V = 2n^2 + 2 \sum_{\lambda} d_\lambda^2,
\]
where \(d_\lambda\) are the multiplicities of the eigenvalues \(\lambda\) of \(V\).

**Corollary 4.7.** Consider a block-diagonal unitary operator
\[
U = \sum_{i=1}^{k} U_i \otimes e_i f_i^*,
\]
where the operators \(U_i\) are in generic position:
\[
\forall i \neq j, \quad U_i U_j^* \text{ has a simple spectrum}.
\]
The dimension of the enveloping tangent space of \(\mathcal{U}_{\text{unital}}\) at \(U\) is then
\[
D_U = kn^2 + nk^2 - nk\quad (24)
\]
Note that the expression above is symmetric in \(n\) and \(k\).

We conjecture that the expression (24) is the dimension of \(\mathcal{U}_{\text{unital}}\), as an algebraic variety, see conjecture 8.1.

### 5. Bipartite unitary operators producing PPT channels

We consider in this section PPT channels and bipartite unitary operators which produce such channels via the Stinespring formula, independent of the state of the environment.

Recall that the maximally entangled state is the matrix (here, we drop the normalization constant)
\[
\mathcal{M}_n^\otimes(\mathbb{C}) \ni \Omega_n := \sum_{i,j=1}^{n} e_i e_j^* \otimes e_i e_j^*.
\]

A quantum channel \(L\) is said to be PPT if and only if its Choi matrix
\[
C_L = [\text{id} \otimes L](\Omega_n)
\]
is PPT, i.e. \(C_L^T \succeq 0\). Hence, the set \(\mathcal{U}_{\text{PPT}}\) admits the following characterization:
\[
\mathcal{U}_{\text{PPT}} = \{ \ U \in \mathcal{U}_{nk} : \text{the map } \beta \mapsto C_{L_{\beta},\beta}^\Gamma \text{ is positive} \}.
\]
Since the structure of positive maps between matrix algebras is rather poorly understood, we focus for the moment on a subset of $\mathcal{PPT}$, namely $\mathcal{PPT} = \{ \alpha \}$.

We have the following description of the set $\mathcal{CPPT}$, in which, remarkably, the partial transpose of $U$ plays a special role.

**Proposition 5.1.** For all $n, k$, we have

$$\mathcal{CPPT} = \{ U \in \mathcal{U}_{nk} : (I_n \otimes U^T)(F_n \otimes I_k)(I_n \otimes U^T)^* \geq 0 \}.$$

**Proof.** We use again the fact that complete positivity is characterized by the fact that the Choi matrix is positive semidefinite. In figure 4, we have depicted in the left image the matrix $G^{b}_b C L$, while in the center panel we have the Choi matrix of the map $\alpha_b G^{b}_b C L$. The rightmost panel contains the diagram of the same Choi matrix, where we have replaced $U$ by its partial transpose $U^T$, in order to obtain a nicer expression. The equality of the last two panels contains the proof of the claim.

In order to further simplify the description given above, by conjugating the above expression by the pseudo-inverse of the matrix $U^T$, we are focusing next on the study of the set

$$\mathcal{PPT} := \{ P \in \mathcal{M}_{nk}^n(\mathbb{C}) \text{ orthogonal projection : } (I_n \otimes P)(F_n \otimes I_k)(I_n \otimes P) \geq 0 \},$$

and we have $\mathcal{CPPT} = \{ U \in \mathcal{U}_{nk} : \text{Ran}(U^T) \in \mathcal{PPT} \}$.

We have gathered the following properties of the set $\mathcal{PPT}$; we leave the proofs of these simple facts to the reader.

1. It is locally unitarily invariant: for all $U \in \mathcal{U}_n$ and $V \in \mathcal{U}_k$, if $\tilde{P} = (U \otimes V)P(U \otimes V)^*$, then

$$\begin{align*}
(I_n \otimes P)(F_n \otimes I_k)(I_n \otimes \tilde{P})
&= (U \otimes U \otimes V)(I_n \otimes P)(F_n \otimes I_k)(I_n \otimes P)(U \otimes U \otimes V)^*.
\end{align*}$$

2. $I_{nk} \notin \mathcal{PPT}$. In other words, no product unitary lies inside $\mathcal{CPPT}$, nor inside $\mathcal{U}_{PPT}$. As a consequence, we have $\mathcal{U}_{\text{unital}} \cap \mathcal{U}_{PPT} = \emptyset$.

3. Since $\mathcal{U}_{\text{unital}} \subseteq \mathcal{U}_{PPT}$, if $k = n$, for any unitary operator $V \in \mathcal{U}_n$, $P_V \in \mathcal{PPT}$, where $P_V$ is depicted in figure 5.

4. If $x \otimes y \in \text{Ran}P$, then, for any $x' \in \mathbb{C}^n$ such that $x' \perp x, x' \otimes y \notin \text{Ran}P$.

5. For any $x \in \mathbb{C}^n$, $\|x\| = 1$, and any orthogonal projection $Q \in \mathcal{M}_k$, $xx^* \otimes Q \in \mathcal{P}_\text{CPPT}$.
At the level of examples, the only observation here is that $P_{\text{const}} \subseteq U_{\text{PTP}}$. We refer the reader to section 8 for some related open problems.

6. Block-diagonal bipartite unitary operations

In this section we study the set of block-diagonal operators, $U_{A}^{A,B}$, which are also known in the literature as control unitary operators. Before proving any results on this class, let us provide another way of writing equation (12), which has the benefit of being unique in a certain sense. As a corollary, we deduce that the only unitary transformations which are block-diagonal with respect to both sub-systems $A$ and $B$ are given by partial isometries.

**Definition 6.1.** Two unitary operators $U$ and $V$ are said to be in relation, denoted by $U \sim V$, if there exists a constant $\lambda$ in $\mathbb{C}$ with $|\lambda| = 1$, such that $U = \lambda V$.

**Proposition 6.2.** A bipartite unitary transformation $U \in U$ is an element of $U_{A}^{A,B}$ if and only if it can be written as

$$U = \sum_{i} U_{i} \otimes R_{i},$$

where $U_{i}$ are unitary operators acting on $\mathbb{C}^{n}$ and $R_{i}$ are partial isometries $R_{i} : \mathbb{C}^{k} \rightarrow \mathbb{C}^{k}$ such that

$$\sum_{i} R_{i} R_{i}^{*} = \sum_{i} R_{i}^{*} R_{i} = I_{k}$$

and $U_{i} \sim U_{j}$ for all $i \neq j$.

Moreover, the decomposition (26) is unique, up to $\sim$ and permutation of the terms in the sum.

**Proof.** Consider two decompositions of a same operator in $U_{A}^{A,B}$ of the form of (26)

$$\sum_{i} U_{i} \otimes R_{i} = \sum_{j} V_{j} \otimes Q_{j},$$

with

$$\sum_{i} R_{i} R_{i}^{*} = \sum_{i} R_{i}^{*} R_{i} = \sum_{j} Q_{j} Q_{j}^{*} = \sum_{j} Q_{j}^{*} Q_{j} = I_{k},$$

$U_{p} \sim U_{q}$ for all $p \neq q$ and $V_{l} \sim V_{m}$ for all $l \neq m$.

For all $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, s\}$, applying $I \otimes R_{i}^{*}$ on the left and $I \otimes Q_{j}^{*} Q_{j}$ on the right, equation (28) becomes
This particularly means that
\[ R^*Q_j = 0 \quad \text{or} \quad \exists \lambda_{ij}, |\lambda_{ij}| = 1, \ U_i = \lambda_{ij} V_j \quad \text{and} \quad R^*R_i Q_j^*Q_j = \frac{1}{\lambda_{ij}} R^*Q_j. \]

Now note that we have
\[ U_i \otimes R^*R_i = \sum_{j=1}^r U_i \otimes R^*R_i Q_j^*Q_j = 0. \]

This implies that at least one of the terms in the sum is non-trivial. Moreover, since \( V_j \sim V_m \) for all \( j = m \), the operator \( U_i \) can be in relation with only one of the \( V_j \)'s. Therefore, we obtain \( r = s \) and for all \( i \), there exist a unique \( j \) such that \( U_i = \lambda_{ij} V_j \) and \( R^*R_i Q_j^*Q_j = 1/\lambda_{ij} R^*Q_j \).

After following the same strategy with \( I \otimes Q_j Q_j^* \) on the left and \( I \otimes R_i^* \) on the right, we now can deduce that \( R_i = 1/\lambda_{ij} Q_j \). The result follows.

Another point of view on block-diagonal unitaries is the fact captured in the next proposition.

**Proposition 6.3.** A bipartite unitary operation is block-diagonal if and only if it admits a block-singular value decomposition with respect to \( B \):

\[ \mathcal{U}^A_{\text{block-diag}} = \mathcal{U}_{\text{blk}} \cap \mathcal{M}^A_{\text{block-diag}}, \quad (30) \]

where \( \mathcal{M}^A_{\text{block-diag}} \) is the set (see appendix)

\[ \mathcal{M}^A_{\text{block-diag}} = \{ X = \sum_{i=1}^k X_i \otimes e_i f_i^*, \ X_i \in \mathcal{M}_n(\mathbb{C}) \text{ and orthonormal bases } e_i, f_i \text{ of } \mathbb{C}^k \}. \]

In particular, the sets \( \mathcal{U}^A_{\text{block-diag}} \), \( \mathcal{U}^B_{\text{block-diag}} \) and \( \mathcal{U}^A_{\text{block-diag}} \cap \mathcal{U}^B_{\text{block-diag}} \) are algebraic varieties.

**Proof.** For \( U \in \mathcal{M}^A_{\text{block-diag}} \), write

\[ UU^* = \sum_{i=1}^k X_i X_i^* \otimes e_i e_i^*. \]

The above matrix is the identity if and only if each of its diagonal blocks \( X_i X_i^* \) is the identity, and the claim follows.

Let us now investigate the relation between the two classes \( \mathcal{U}^A_{\text{block-diag}} \) and \( \mathcal{U}^B_{\text{block-diag}} \). We start by presenting an algorithm allowing to check if a unitary matrix \( U \) in \( \mathcal{U}_{\text{blk}} \) belongs to \( \mathcal{U}^A_{\text{block-diag}} \). This key result relies on theorem \( A.1 \).

**Proposition 6.4.** Let \( U \) be in \( \mathcal{U}_{\text{blk}} \). Consider the operators \( (X_{\alpha})_{\alpha=1}^{n^2} \) in \( \mathcal{M}_n(\mathbb{C}) \) defined, for all \( \alpha = 1, \ldots, n^2 \), by

\[ X_{\alpha} = [\text{Tr} \otimes \text{id}]((E^{\alpha^*}_{\alpha}) \otimes I)U, \]

with \( \{ E^{\alpha}_{i} \}_{i=1}^{n^2} \) an orthonormal basis of \( \mathcal{M}_n(\mathbb{C}) \). Then, \( U \) belongs to \( \mathcal{U}^A_{\text{block-diag}} \) if and only if the families \( (X_{\alpha} X_{\beta})^{\alpha^*}_{\alpha,\beta=1} \) respectively \( (X_{\alpha}^* X_{\beta})^{\alpha^*}_{\alpha,\beta=1} \) consist of commuting, normal operators.
Proof. Fix $U \in U_{nk}$. Thanks to theorem A.1, the matrix $U$ has a block-diagonal SVD, that is, there exists matrices $U_1, \ldots, U_p \in \mathcal{M}_n(\mathbb{C})$ and partial isometries $R_1, \ldots, R_p \in \mathcal{M}_k(\mathbb{C})$ having orthogonal initial, respectively final, projections such that

$$U = \sum_{i=1}^p U_i \otimes R_i,$$

(32)

if and only if the families $\{X_{\alpha}X_{\beta}^*\}_{\alpha,\beta=1}^n$, respectively $\{X_{\alpha}^*X_{\beta}\}_{\alpha,\beta=1}^n$, consist of commuting, normal operators. Then the unitarity of the $(U_i)_{i=1}^p$’s directly follows from the unitarity of $U$.

As a first application of the above result let us present the relation between $U^A_{\text{block-diag}}$ and $U^B_{\text{block-diag}}$ in the case of the qubit space $\mathbb{C}^2$.

**Proposition 6.5.** If $n = 2$, then

$$U^B_{\text{block-diag}} \subseteq U^A_{\text{block-diag}}.$$

**Proof.** Any element $U \in U^B_{\text{block-diag}}$ can be written as

$$U = e_1 f_1^* \otimes U_1 + e_2 f_2^* \otimes U_2.$$

In order to apply proposition 6.4 we consider the orthonormal basis $\{E_{ij} = f_i^* e_j, i, j = 1, 2\}$. In particular

$$X_{ij} = \delta_{ij} U_j,$$

for all $i, j = 1, 2$. Consider now the sets

$$\{X_{ij} X_{kl}^*, i, j, k, l = 1, 2\} = \{I, U_1 U_2^*, U_2 U_1^*\}$$

and

$$\{X_{ij}^* X_{kl}, i, j, k, l = 1, 2\} = \{I, U_1^* U_2, U_2^* U_1\}.$$

It is obvious that these sets consist of commuting, normal operators, finishing the proof. □

**Corollary 6.6.** In the case $n = k = 2$, we have

$$U^A_{\text{block-diag}} = U^B_{\text{block-diag}}.$$

Note however that the inclusion in the above result is strict (in the case $n \geq 3, k = 2$). For $n = 3$, and arbitrary $k \geq 2$, we construct next an example of a unitary operator being in $U^B_{\text{block-diag}}$ but not in $U^A_{\text{block-diag}}$.

Consider two non-commuting unitary operators $V, W$ in $\mathcal{M}_k(\mathbb{C})$ and an orthonormal basis $(e_i)$ of $\mathbb{C}^3$ and define

$$U = e_1 e_1^* \otimes I + e_2 e_2^* \otimes V + e_3 e_3^* \otimes W.$$

By construction, the operator $U$ belongs to $U^B_{\text{block-diag}}$. Let us now check that it is not in $U^A_{\text{block-diag}}$. Consider the orthonormal basis $\{E_{ij} = e_i e_j^*, i, j = 1, 2, 3\}$ of $\mathcal{M}_3(\mathbb{C})$, we have for example
We immediately note that the operators $X_{11}^* X_{22} = V$ and $X_{11}^* X_{33} = W$ do not commute. Since this commutativity is necessary to be in $\mathcal{U}^A_{\text{block-diag}}$ (proposition 6.4), we conclude that $U$ doesn’t belong to $\mathcal{U}^A_{\text{block-diag}}$.

Another class of interesting block-diagonal (with respect to the second system, $B$) operators are circulant unitary matrices.

**Proposition 6.7.** Let $X \in \mathcal{M}_{nk}(\mathbb{C})$ be a circulant matrix. Then $X \in \mathcal{M}_{\text{block-diag}}^B$. In particular, any circulant unitary operator $U$ is block-diagonal with respect to the $B$ factor.

**Proof.** In the proof of this result, since we are going to make us of circularity properties, the indices for the matrices we consider are starting at zero. Recall that a matrix $X \in \mathcal{M}_{nk}(\mathbb{C})$ is circulant iff

\[ X_{ij} = x_{(j-i)\bmod n}, \]

where $x \in \mathbb{C}^{nk}$ is the first row of $X$ and we write $[a]_p = a \mod p$, for any integers $a$ and $p$. Circulant matrices are known to be precisely the matrices which are diagonal in the Fourier basis. Recall that the Fourier matrix (which implements the change of bases between the canonical basis and the Fourier basis) is given by

\[ F_p(i, j) = \omega^{ij}, \]

where $\omega = \exp(2\pi i/p)$ is a primitive $p$th root of unity. Finally, since we are going to work with matrices living in a tensor product space, the element $(s, t)$ of the block $(i, j)$ of a matrix $A \in \mathcal{M}_k(\mathbb{C}) \otimes \mathcal{M}_{l}(\mathbb{C})$ is $A_{i+k, j+l}$.

Now that the notation is fixed, consider a circular unitary matrix $X \in \mathcal{M}_{nk}(\mathbb{C})$ and let $x$ be its first row. For any matrix $A \in \mathcal{M}_k(\mathbb{C})$, define

\[ X_A = [\text{id} \otimes \text{Tr}](X \cdot I \otimes A). \]

We show next that the matrices $X_A$ are all circulant, fact which, by theorem A.1, suffices to conclude, since all the matrices appearing in the theorem will be simultaneously diagonalizable in the Fourier basis.

For all $0 \leq i, j < n$, we have

\[ X_A(i, j) = \sum_{s, t=0}^{k-1} U_{k+s, k+t} A_{ts} \]

\[ = \sum_{s, t=0}^{k-1} a_{(j-i)k + (t-s)l} A_{ts}. \]

The crucial observation is that the above quantity only depends on the difference $j - i$: indeed, if $[(j - i) = (j' - i')]_{nk}$, then there exists some $r$ such that $j' - i' = j - i + nr$, and thus

\[ [(j' - i')k + (t - s)]_{nk} = [(j - i)k + (t - s) + nkr]_{nk} = [(j' - i')k + (t - s)]_{nk}, \]

showing that the matrix $X_A$ is circular, and finishing the proof.

The statement about circular unitary operators follows from the general case using proposition 6.3.

We turn next to the study of the unitary operators which are block-diagonal with respect to both systems $A$ and $B$.  

18
Proposition 6.8. A unitary operator $U$ is block diagonal with respect to both tensor factors $A$ and $B$ (i.e. $U \in \mathcal{U}_{\text{block-diag}}^A \cap \mathcal{U}_{\text{block-diag}}^B$) iff

$$U = \sum_{i=1}^{s} \sum_{j=1}^{r} \lambda_{ij} \mathcal{Q}_i \otimes \mathcal{R}_j,$$

where, for all $i = 1, \ldots, s$, $j = 1, \ldots, r$, $|\lambda_{ij}| = 1$, and where $(\mathcal{Q}_i)_{i=1}^{s}$, $(\mathcal{R}_j)_{j=1}^{r}$ are two family of orthogonal partial isometries respectively on $\mathbb{C}^n$ and $\mathbb{C}^k$ satisfying

$$\sum_{i=1}^{s} \mathcal{Q}_i \mathcal{Q}_i^* = \sum_{i=1}^{s} \mathcal{Q}_i^* \mathcal{Q}_i = I_n, \quad \sum_{j=1}^{r} \mathcal{R}_j \mathcal{R}_j^* = \sum_{j=1}^{r} \mathcal{R}_j^* \mathcal{R}_j = I_k. \quad (33)$$

Proof. Let $U$ be an element in the intersection $\mathcal{U}_{\text{block-diag}}^A \cap \mathcal{U}_{\text{block-diag}}^B$. Then, $U$ admits both decompositions

$$U = \sum_{i=1}^{s} \mathcal{Q}_i \otimes \mathcal{V}_i = \sum_{j=1}^{r} \mathcal{U}_j \otimes \mathcal{R}_j.$$

Applying $\mathcal{Q}_i^* \otimes \mathcal{R}_j^*$ on the left, we obtain

$$\mathcal{Q}_i^* \mathcal{Q}_i \otimes \mathcal{R}_j^* \mathcal{V}_i = \mathcal{Q}_i^* \mathcal{U}_j \otimes \mathcal{R}_j^* \mathcal{R}_j.$$

Then there exists $\mu_{ij} \neq 0$ such that

$$\mathcal{Q}_i^* \mathcal{Q}_i = \mu_{ij} \mathcal{U}_j \quad \text{and} \quad \mathcal{R}_j^* \mathcal{V}_i = \frac{1}{\mu_{ij}} \mathcal{R}_j^* \mathcal{R}_j.$$

Now since the $\mathcal{Q}_i$’s and the $\mathcal{R}_j$’s satisfy (33) we end up with

$$\mathcal{U}_j = \sum_{i=1}^{s} \mu_{ij} \mathcal{Q}_i \quad \text{and} \quad \mathcal{V}_i = \sum_{j=1}^{r} \frac{1}{\mu_{ij}} \mathcal{R}_j.$$

Since the operators $\mathcal{U}_j$ and $\mathcal{V}_i$ are unitary, we conclude that $|\mu_{ij}| = 1$ and that gives the result. \hfill $\Box$

Finally, we compute next the (real) dimension of $\mathcal{U}_{\text{block-diag}}^A$ and $\mathcal{U}_{\text{block-diag}}^B \cap \mathcal{U}_{\text{block-diag}}^A$.

Proposition 6.9. The real dimension of the algebraic variety $\mathcal{U}_{\text{block-diag}}^A$ is

$$\dim \mathcal{U}_{\text{block-diag}}^A = \begin{cases} k^2 & \text{if } n = 1 \\ k(n^2 + 2k - 2) & \text{if } n > 1. \end{cases}$$

The real dimension of the algebraic variety $\mathcal{U}_{\text{block-diag}}^B \cap \mathcal{U}_{\text{block-diag}}^A$

$$\dim(\mathcal{U}_{\text{block-diag}}^A \cap \mathcal{U}_{\text{block-diag}}^B) = \begin{cases} (nk)^2 & \text{if } \min(n, k) = 1 \\ 2n^2 + 2k^2 + nk - 2n - 2k & \text{if } \min(n, k) > 1. \end{cases}$$

Proof. Let us first perform a heuristic parameter counting for a generic element

$$\mathcal{U}_{\text{block-diag}}^A \ni U = \sum_{i=1}^{k} \mathcal{U}_i \otimes \mathcal{E}_i^f.$$
The choice of the two orthonormal bases \( \{ e_i \} \) and \( \{ f_j \} \) in (32) corresponds to a total of \( 2k^2 \) real parameters, since \( \dim(\mathcal{U}_k) = k^2 \). Each matrix \( U_i \) accounts for \( n^2 \) real parameters, so, in total, we get \( kn^2 \) extra real parameters. However, in each term \( U_i \otimes e_i f_i^* \), two of the three complex phases of \( X_i, e_i, f_i \) are redundant, so we have over counted \( 2k \) real parameters. We conclude that the real dimension of \( \mathcal{U}_k^{\alpha} \) should be \( 2k^2 + kn^2 - 2k \). The above reasoning overcounts in the case \( n = 1 \). Indeed, in that case one can ignore the matrices \( U_i \) (the phase can be absorbed in the \( e_i f_i^* \) part), and we are left with an unitary matrix, which counts for \( k^2 \) real parameters. The rigorous proof of this result is very similar to the one of proposition A.6, and is left to the reader.

Let us now find the dimension of the intersection. Similarly, let us count parameters for a generic element of the form

\[
\mathcal{U}_k^{\alpha} \cap \mathcal{U}_k^{\beta} \ni U = \sum_{i=1}^{n} \sum_{j=1}^{k} \lambda_{ij} e_i f_i^* \otimes g_j h_j^*,
\]

where, for all \( i = 1, \ldots, n, j = 1, \ldots, k, |\lambda_{ij}| = 1 \), and \( (e_i), (f_j), (g_j) \) and \( (h_j) \) are orthonormal bases of \( \mathbb{C}^n \) and \( \mathbb{C}^k \), respectively.

The choice of the four orthonormal bases corresponds to a total of \( 2n^2 + 2k^2 \) real parameters, the choice of the coefficients \( nk = 2nk - nk \). Since, in \( \lambda_{ij} e_i f_i^* \otimes g_j h_j^* \), all the phases can be absorbed in the coefficient \( \lambda_{ij} \), we have over counted \( 2n + 2k \) real parameters. Again, the case \( \min(n, k) = 1 \) is degenerated, since any unitary operator is of the desired form. \( \square \)

7. Bipartite unitary operators producing mixed unitary channels

In this section we investigate the set \( \mathcal{U}_{\text{mixed}} \). We provide necessary conditions for a bipartite unitary operator \( U \) to belong to \( \mathcal{U}_{\text{mixed}} \), and we show that in the case of qubit channels (\( n = 2 \)), the sets \( \mathcal{U}_{\text{mixed}} \) and \( \mathcal{U}_{\text{unital}} \) are equal.

As discussed in the introduction, the following chain of inclusions holds:

\[
\mathcal{U}_k^{\alpha} \cap \mathcal{U}_k^{\beta} \subseteq \mathcal{U}_{\text{prob-lin}} \subseteq \mathcal{U}_{\text{prob}} \subseteq \mathcal{U}_{\text{mixed}} \subseteq \mathcal{U}_{\text{unital}}.
\]

The major conjecture formulated in [1, 2] is whether the equality \( \mathcal{U}_k^{\alpha} \cap \mathcal{U}_k^{\beta} = \mathcal{U}_{\text{mixed}} \) holds. The difficulty of this statement stems from the fact that in the definition of \( \mathcal{U}_{\text{mixed}} \) we have a lot of flexibility concerning the unitary conjugations which appear in the definition of the quantum channels, whereas in the set \( \mathcal{U}_k^{\alpha} \cap \mathcal{U}_k^{\beta} \) the unitary operators \( U_i \) are fixed by the definition of the corresponding bipartite unitary operator. If we relax the flexibility of the unitary operators, that is we impose that they are all the same, and if we impose that the probabilities \( p_i(\beta) \) are linear, the conjecture holds.

**Theorem 7.1.** For all \( n, k \), the sets \( \mathcal{U}_k^{\alpha} \cap \mathcal{U}_k^{\beta} \) and \( \mathcal{U}_{\text{prob-lin}} \) are equal.

**Proof.** Without loss of generality, we assume that the unitary operators \( U_i \) are different up to a phase, i.e. \( U_i \neq U_j \), for all \( i \neq j \).

Due to the decomposition of any matrix into a linear combination of at most four matrices in \( \mathcal{M}_k^+ (\mathbb{C}) \) (positive and negative hermitian parts and their equivalents for the anti-hermitian part), the \( p_i \)'s can be extended by linearity to positive functionals on \( \mathcal{M}_k (\mathbb{C}) \). By Riesz theorem, for each \( i \), there exists a matrix \( M_i \) such that

\[
\forall X \in \mathcal{M}_k (\mathbb{C}), \quad p_i (X) = \text{Tr}(M_i X).
\]
Note now that the values \( p_i(\beta) = \text{Tr}(M_i \beta) \) are non-negative for all \( \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}) \). Therefore the matrix \( M_i \) is actually positive semi-definite since we have

\[
\text{Tr}(M_i \beta) = p_i(\beta) = \frac{1}{p_i(0)} \text{Tr}(M_i^* \beta), \quad \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}).
\]

We then conclude that the matrices \( M_i \) can be written as \( M_i = R_i R_i^* = R_i^* R_i = R_i^2 \) for some hermitian and positive semi-definite \( R_i \).

Moreover, using that for all \( \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}) \)

\[
\sum_{i=1}^{r} p_i(\beta) = \text{Tr} \left( \sum_{i=1}^{r} M_i \right) \beta = 1,
\]

it follows that \( \sum_{i=1}^{r} M_i = I \). Then, for all \( \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}) \), we can write the quantum channel \( L_{U,\beta} \) as

\[
L_{U,\beta}(X) = \text{Tr}_g(U \cdot X \otimes \beta \cdot U^*) = \text{Tr}_g \left( \sum_{i=1}^{r} U_i \otimes R_i \cdot X \otimes (U_i \otimes R_i)^* \right).
\]

By linearity, the previous equality gives

\[
\forall Y \in \mathcal{M}_{nk}(\mathbb{C}), \quad \text{Tr}_g(U \cdot Y \cdot U^*) = \text{Tr}_g \left( \sum_{i=1}^{r} U_i \otimes R_i \cdot Y \cdot (U_i \otimes R_i)^* \right).
\]

Then, by definition of the partial trace, we obtain the following equivalences

\[
\forall Y \in \mathcal{M}_{nk}(\mathbb{C}), \quad A \in \mathcal{M}_n(\mathbb{C}),
\]

\[
\text{Tr}(U \cdot Y \cdot U^* A \otimes I) = \text{Tr} \left( \sum_{i=1}^{r} U_i \otimes R_i \cdot Y \cdot (U_i \otimes R_i)^* A \otimes I \right),
\]

\[
\forall Y \in \mathcal{M}_{nk}(\mathbb{C}), \quad A \in \mathcal{M}_n(\mathbb{C}),
\]

\[
\text{Tr}(Y \cdot U^* A \otimes I U) = \text{Tr} \left( Y \cdot \sum_{i=1}^{r} U_i^* A U_i \otimes M_i \right).
\]

\[
\forall A \in \mathcal{M}_n(\mathbb{C}), \quad U^* A \otimes I U = \sum_{i=1}^{r} U_i^* A U_i \otimes M_i.
\]  \hspace{1cm} (35)

Let us now study (35). Consider two matrices \( A, B \in \mathcal{M}_n(\mathbb{C}) \). Since \( U^* A B \otimes I U = U^* A \otimes I U \cdot U^* B \otimes I U \), we obtain from (35)

\[
\sum_{i=1}^{r} U_i^* A U_i \otimes M_i = \sum_{i,j=1}^{r} U_i^* A U_i U_j^* B U_j \otimes M_i M_j.
\]  \hspace{1cm} (36)

Applying (36) with \( A = ee^* \) and \( B = ff^* \) where \( e \) and \( f \) are orthogonal vectors of \( \mathbb{C}^n \), it directly follows

\[
0 = \sum_{i,j \neq j} \langle (U_i^* e, U_j^* f) \rangle^2 \text{Tr}(M_i M_j) = \sum_{i,j \neq j} \langle (e, U_i U_j^*) \rangle^2 \text{Tr}(M_i M_j).
\]

Taking the trace, we obtain

\[
\forall e \perp f, \quad 0 = \sum_{i,j \neq j} |\langle (U_i^* e, U_j^* f) \rangle|^2 \text{Tr}(M_i M_j) = \sum_{i,j \neq j} |\langle (e, U_i U_j^*) \rangle|^2 \text{Tr}(M_i M_j).
\]

Note that the previous equation is actually a sum of non-negative terms equals to 0. Therefore, we conclude that for \( i \neq j \)
Now since for all $i \neq j$, $U_i \nRightarrow U_j$, the unitary matrix $U_i U_j^*$ is not a multiple of the identity. Thus, we claim that we can find orthogonal vectors $e$ and $f$, such that $\langle e, U_i U_j^* f \rangle = 0$. Indeed, the matrix $U_i U_j^*$ is diagonalizable in an orthonormal basis $(u_p)_{p=1,\ldots,n}$ with related eigenvalues $(\mu_p)_{p=1,\ldots,n}$. Since $U_i U_j^* \not\approx CI$, all the eigenvalues are not equal, for instance $\mu_1 \neq \mu_2$. Let us consider the orthogonal vectors $e = u_1 - u_2$ and $f = u_1 + u_2$. We can easily check that $\langle e, U_i U_j^* f \rangle = \mu_1 - \mu_2 \neq 0$.

Finally, we deduce from (37) that $\text{Tr}(M M_i) = 0$ for all $i \neq j$ and thus $M M_i = 0$. The $M_i$’s being orthogonal and sum to the identity, we define the matrix $V = \sum_{i=1}^r U_i \otimes R_i$ belonging to $\mathcal{U}_k^\Delta$. We can now easily check that the unitary operators $U$ and $V$ induce the same quantum channels for all $\beta$ in $\mathcal{M}_k^{\Delta+}(\mathbb{C})$. By lemma 2.3, there exists $W$ of $\mathcal{U}_k$ such that $U = (I \otimes W)V$; this proves the result.

As we have mentioned in the beginning of this section the conjecture $U_{\text{block-diag}}^A = U_{\text{mixed}}$ is a complicated question in general. In the case $n = 2$, we can show that the conjecture is true without imposing additional conditions.

**Proposition 7.2.** If $n = 2$, then $U_{\text{block-diag}}^A = U_{\text{unital}}$. In particular, the chain of inclusions (34) collapses:

$$U_{\text{block-diag}}^A = U_{\text{prob-lin}} = U_{\text{prob}} = U_{\text{mixed}} = U_{\text{unital}}.$$ 

**Proof.** Consider $\{e_1, e_2\}$ the canonical orthonormal basis of $\mathbb{C}^2$ and consider a matrix $U$ in $U_{\text{unital}}$ written as $2 \times 2$ block matrices

$$U = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = e_1 e_1^* \otimes A + e_1 e_2^* \otimes B + e_2 e_1^* \otimes C + e_2 e_2^* \otimes D$$

with $A$, $B$, $C$ and $D$ in $\mathcal{M}_k(\mathbb{C})$. As proved in theorem 4.1, both $U$ and $(U^T)^T$ are unitary matrices and therefore

$$A A^* + B B^* = A^* A + B^* B = I, \quad A A^* + C C^* = A^* A + C^* C = I,$$

$$C C^* + D D^* = C^* C + D^* D = I, \quad D D^* + B B^* = D^* D + B^* B = I,$$

$$A C^* + B D^* = A^* C + B^* D = 0, \quad A B^* + C D^* = A^* B + C^* D = 0.$$ (38)

Our aim is to applied proposition 6.4. Consider the orthonormal basis $\{E_{ij} = e_i e_j^*, i, j = 1, 2\}$ of $\mathcal{M}_2(\mathbb{C})$, it is clear that

$$\{X_{ij} X_{kl}^*, i, j, k, l = 1, 2\} = \{XY^* | X, Y = A, B, C, D\},$$

$$\{X_{ij} X_{kl}^* | i, j, k, l = 1, 2\} = \{X^* Y | X, Y = A, B, C, D\}.$$ 

Let us now prove that $\{XY^* | X, Y = A, B, C, D\}$ and $\{X^* Y | X, Y = A, B, C, D\}$ consist of normal commuting matrices. It can be noticed that it is sufficient to check that, for all $X, Y, Z = A, B, C, D$,

$$XY^* Z = ZY^* X.$$ 

Using the symmetry $A, D$ in (38) together with the symmetry $B, C$, the 64 different cases boil down to 11 non-trivial cases: $A A^* B, A A^* D, A B^* B, A B^* C, A B^* D, A D^* B, A D^* D, B A^* C, B A^* D, B B^* C$ and $B C^* D$. Each of them can be easily checked as for instance
or
\[ BC^*D = B(C^*D) = B(-A^*B) = (-BA^*)B = DC^*B. \]
The result then holds.

**Remark 7.3.** A similar result has been obtained in [17, theorem 9], under more stringent assumptions. More precisely, it is shown in [17] that, when \( n = 2 \), \( \mathcal{U}^{\text{block-diag}} = \mathcal{U}^{\text{prob}} \), assuming that the unitary operators appearing in the mixed-unitary decomposition of channels are linearly independent.

Swapping the roles of \( n \) and \( k \), we obtain the following result.

**Proposition 7.4.** If \( k = 2 \), then \( \mathcal{U}^{\text{block-diag}} = \mathcal{U}^{\text{unital}} \).

Let us now show that, in general, the inclusion \( \mathcal{U}^{\text{mixed}} \subset \mathcal{U}^{\text{unital}} \) is strict. Recall that the Kraus operator space of a quantum channel \( L(\rho) = \sum E_i \rho E_i^* \) is the space \( K(L) = \text{span} \{ E_i \} \) [11, 24]; note that \( K(L) \) does not depend on the choice of Kraus operators for \( L \), since all Kraus representations are related by unitary transformations [20, theorem 8.2]. One of the main observations in [24] was that for a mixed unitary channel \( L \), \( K(L) \cap \mathcal{U}_n \neq \emptyset \). The next result builds on this remark.

**Proposition 7.5.** Let \( U \in \mathcal{U}^{\text{mixed}} \) be a bipartite unitary operator. Then, for any unit vector \( f \in \mathbb{C}^k \) and any orthonormal basis \( \{ e_i \} \) of \( \mathbb{C}^k \), we have
\[
\text{span} \{ I_n \otimes e_i^* \cdot U \cdot I_n \otimes f \}_{i=1}^{k} \cap \mathcal{U}_n \neq \emptyset.
\]

**Proof.** For any choice of \( f \) and \( \{ e_i \} \), the operators
\[ E_i = I_n \otimes e_i^* \cdot U \cdot I_n \otimes f \]
are Kraus operators for the channel \( L_{U, f} \). Since the channel is mixed unitary, it follows from [24, section IV] that the linear span of the \( E_i \) should contain a unitary operator.

**Remark 7.6.** Note that in the statement above, the set
\[
\text{span} \{ I_n \otimes e_i^* \cdot U \cdot I_n \otimes f \}_{i=1}^{k}
\]
does not depend on the particular choice of the basis \( \{ e_i \} \), but only on the vector \( f \).

As a direct consequence of the above result, we obtain the following simple criterion for deciding if a given unitary matrix \( U \) is an element of \( \mathcal{U}^{\text{mixed}} \).

**Corollary 7.7.** Let \( U \in \mathcal{U}_n \) be a bipartite unitary operator with the following property:
\[
\exists f \in \mathbb{C}^k \text{ s.t. } \forall e \in \mathbb{C}^k, \quad I_n \otimes e^* \cdot U \cdot I_n \otimes f \notin \mathcal{U}_n.
\]
Then, \( U \notin \mathcal{U}^{\text{mixed}} \).

With the help of the criterion above, we present next an example of an element \( U \in \mathcal{U}^{\text{block-diag}} \setminus \mathcal{U}^{\text{mixed}} \), which shows, in particular, that the inclusion \( \mathcal{U}^{\text{mixed}} \subset \mathcal{U}^{\text{unital}} \) is strict;
this example is motivated by [19, section 4.3] and [24, example 1]. Let $U \in \mathcal{U}_{4,2}$ be

$$U = e_1 e_1^* \otimes I_2 + e_2 e_2^* \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + e_3 e_3^* \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} + e_4 e_4^* \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ -i & -1 \end{bmatrix}$$

Obviously, $U \in \mathcal{U}_{4,4}$. In the spirit of the criterion above, compute

$$I_4 \otimes \begin{bmatrix} z & w \end{bmatrix} \cdot U \cdot I_4 \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \text{Diag}(z, w, z+w/\sqrt{2}, z-iw/\sqrt{2}).$$

Asking for the diagonal matrix above to be unitary leads to a contradiction, and thus, by corollary 7.7, we conclude $U \not\in \mathcal{U}_{\text{mixed}}$.

8. Open questions and further remarks

We end this work with a list of questions that we have left unanswered (or even untouched). We hope to get back to some of these problems in some future work.

We start with the problem of computing the dimension of the algebraic variety $\mathcal{U}_{\text{unital}}$: recall that previously, we have looked at the enveloping tangent space of this variety, at some particular points.

Conjecture 8.1. Show that $\dim \mathcal{U}_{\text{unital}} = kn^2 + nk^2 - nk$.

It has been shown in theorem 7.1 that any operator in the set $\mathcal{U}_{\text{prob-lin}}$ (which is a subset of $\mathcal{U}_{\text{mixed}}$) is block diagonal, with respect to the system $A$. Moreover, in the qubit case $n = 2$, we have $\mathcal{U}_{\text{block-diag}} = \mathcal{U}_{\text{mixed}}$, see proposition 7.2. We conjecture that this equality always hold, and that the technical restrictions appearing in the definition of $\mathcal{U}_{\text{prob-lin}}$ are actually superfluous.

Conjecture 8.2. For all values of $n, k$, it holds that

$$\mathcal{U}_{\text{block-diag}} = \mathcal{U}_{\text{mixed}}.$$  

Regarding bipartite unitary operators producing PPT channels, we have left the following problem open.

Question 8.3. Given a subspace $V \subseteq \mathbb{C}^n \otimes \mathbb{C}^k$, let $P \in \mathcal{M}_{nnk}(\mathbb{C})$ be the orthogonal projection on $V$. Characterize the set of subspaces $V$ such that

$$\mathcal{M}_{nnk}(\mathbb{C}) \ni (I_n \otimes P)(F_n \otimes I_k)(I_n \otimes P) \succeq 0,$$

where $F$ is the flip operator.

This brings us to the problem of characterizing the set $\mathcal{U}_{EB}$ and comparing it to $\mathcal{U}_{\text{PPT}}$ (at the level of quantum states, this would be the fact that the PPT criterion for separability is necessary in all dimensions, and sufficient for $nk \leq 6$). We refer to [18] for some further results in this direction.
**Question 8.4.** Provide a description of the set $U_{EB}$. For which values of $n$, $k$, is it true that $U_{PPT} = U_{EB}$?

At the level of examples, beside the obvious inclusion $U_{const} \subseteq U_{EB}$, we also have\(^7\), when $n = k$,

$$U_{block-diag} \cdot F_n \subseteq U_{EB}.$$ 

Indeed, for a unitary operator $U = \left(\sum_{i=1}^n U_i \otimes e_i^*\right)F_n$, the corresponding quantum channel reads

$$L_{U,\beta}(\rho) = \sum_{i=1}^n \langle f_i, \rho f_i^*\rangle U_i \beta U_i^*,$$

which is entanglement-breaking.

Finally, we consider the following classes of bipartite unitary matrices yielding channels of interest in quantum information theory.

- $U_{CQ} = \{ U \in U \mid \forall \beta \in \mathcal{M}_k^2(\mathbb{C}), L_{U,\beta} \text{ is a classical-quantum channel}\}$,
- $U_{QC} = \{ U \in U \mid \forall \beta \in \mathcal{M}_k^2(\mathbb{C}), L_{U,\beta} \text{ is a quantum-classical channel}\}$,
- $U_{CC} = \{ U \in U \mid \forall \beta \in \mathcal{M}_k^2(\mathbb{C}), L_{U,\beta} \text{ is a classical-classical channel}\}$.

The study of these classes has been initiated in [17, 18], where mainly the qubit case $n = 2$ has been discussed. The structure of these operators in the general case remains open.

**Question 8.5.** Characterize the sets $U_{CQ}$, $U_{QC}$, and $U_{CC}$.

**Acknowledgments**

We would like to thank Stéphane Attal for suggesting the question, and Denis Bernard and Michael Kech for inspiring discussions. We are also grateful to Siddharth Karumanchi for pointing out to us reference [17] and sharing with us the unpublished notes [18]. IN’s research has been supported by a von Humboldt fellowship and by the ANR projects OSQPI 2011 BS01 008 01 and RMTQIT ANR-12-IS01-0001-01. The three authors have been supported by the ANR project StoQ ANR-14-CE25-0003-01.

**Appendix. Necessary and sufficient conditions for the existence of a block-SVD**

In this section, we establish necessary and sufficient conditions for the existence of a block singular value decomposition of a bipartite operator with respect to the second sub-system $B$. Moreover, we present an algorithm for obtaining such a decomposition when it does exist. These results are inspired from [4, 8], see also [14, theorem 2.5.5 and section 7.3, problem 25].

We shall denote, for any matrices $X \in \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C})$ and $A \in \mathcal{M}_n(\mathbb{C})$,

$$X_A := [\text{Tr} \otimes \text{id}](X \cdot A \otimes I_k).$$

\(^7\) We thank Siddharth Karumanchi for pointing this out to us.
Theorem A.1. Let $X \in \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C})$. The following conditions are equivalent:

1. The matrix $X$ has a block-diagonal SVD: there exists matrices $X_1, \ldots, X_p \in \mathcal{M}_n(\mathbb{C})$ and partial isometries $R_1, \ldots, R_p \in \mathcal{M}_k(\mathbb{C})$ having orthogonal initial, respectively final, projections such that

$$X = \sum_{i=1}^p X_i \otimes R_i.$$

2. The families \( \{X_A X_B^*\}_{A,B \in \mathcal{M}_n(\mathbb{C})} \) respectively \( \{X_A^* X_B\}_{A,B \in \mathcal{M}_n(\mathbb{C})} \) consist of commuting operators.

3. The families \( \{X_A X_B^*\}_{A,B \in \mathcal{M}_n(\mathbb{C})} \) respectively \( \{X_A^* X_B\}_{A,B \in \mathcal{M}_n(\mathbb{C})} \) consist of commuting operators.

We denote the set of matrices $X$ satisfying the above condition(s) by $\mathcal{M}^\text{block-diag}_A$.

\[ \mathcal{M}^\text{block-diag}_A = \{ X \in \mathcal{M}_n(\mathbb{C}) | X = \sum_{i=1}^p X_i \otimes e_i f_i^* \}. \]

The set $\mathcal{M}^\text{block-diag}_B$ is defined in a similar way, by swapping the roles of the two tensor factors.

**Proof.** The implication (2) $\implies$ (3) is obvious. Let us first show (1) $\implies$ (2). For a matrix $X$ as in (32), we have

$$X_A X_B^* = \sum_{i=1}^p \text{Tr}(X_A) \text{Tr}(X_B) P_i,$$

where $P_i = R_i R_i^*$ is the orthogonal projection on the image of the partial isometry $R_i$. This relation shows that the matrices \( \{X_A X_B^*\}_{A,B \in \mathcal{M}_n(\mathbb{C})} \) are normal and diagonalizable in the same orthonormal basis of $\mathbb{C}^n$. A similar argument shows the result for the matrices \( \{X_A^* X_B\}_{A,B \in \mathcal{M}_n(\mathbb{C})} \).

Let us now show (3) $\implies$ (1). The fact that the matrices $X_A X_B^*$ commute implies that they are normal. Normality and the commutation relations imply they have the same set of eigenprojectors $P_i$:

$$\forall \alpha, \beta, \quad X_A X_B^* = \sum_{i=1}^p \lambda_i^{(\alpha, \beta)} P_i.$$  \hspace{1cm} (39)

In the same vein, we have, for another set of orthogonal eigenprojectors $Q_i$:

$$\forall \alpha, \beta, \quad X_A^* X_B = \sum_{i=1}^p \mu_i^{(\alpha, \beta)} Q_i.$$  \hspace{1cm} (40)

Letting $\alpha = \beta$ in (39) and (40) and using the fact that the matrices $X_A X_B^*$ and $X_A^* X_B$ have the same (positive) eigenvalues (counting multiplicities), we have that $p = p'$ and there exists permutations $\sigma_i \in \mathcal{S}_p$ and complex numbers $\lambda_i^{(\alpha)}$ such that

$$X_A = \sum_{i=1}^p \lambda_i^{(\alpha)} R_i^{(\sigma_i)}$$

for some partial isometries $R_i^{(\sigma_i)}$ having initial projection $Q_{\sigma_i}$ and final projection $P_{\sigma_i}$. Plugging the last expression into (39) and (40), we find that the permutations $\sigma_i$ must be equal; we shall assume, by re-ordering the eigenprojectors $Q_i$, that these permutations are all
equal to the identity. Using similar arguments, the partial isometries \( R_i^{(\alpha)} \) cannot depend on \( \alpha \), and we write \( R_i^{(\alpha)} = R_i \). We have thus

\[
X_\alpha = \sum_{i=1}^r \lambda_i^{(\alpha)} R_i,
\]

and thus

\[
X = \sum_{\alpha=1}^{n^2} E_\alpha \otimes \left( \sum_{i=1}^r \lambda_i^{(\alpha)} R_i \right) = \sum_{i=1}^r \left( \sum_{\alpha=1}^{n^2} \lambda_i^{(\alpha)} E_\alpha \right) \otimes R_i.
\]

Setting

\[
X_i := \sum_{\alpha=1}^{n^2} \lambda_i^{(\alpha)} E_\alpha
\]

concludes the proof.

\[\square\]

**Remark A.2.** The commutation relations in points (2), (3) above imply that the respective matrices are normal.

**Remark A.3.** The above result provides us with an efficient way of checking whether a given bipartite operator \( X \) has a block-SVD: pick a basis of \( M_n(\mathbb{C}) \) (e.g. the usual matrix units) and check the condition in (3) above.

**Remark A.4.** Restricting to \( \alpha = \beta \) in the condition (3) does not yield an equivalent statement, as it is shown in the example below. For \( X \in M_{2 \times 2}(\mathbb{C}) \) given by

\[
X = \begin{bmatrix}
1 & 0 & 0 & 1 \\
0 & 2 & 1 & 0 \\
0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1
\end{bmatrix}
\]

(41)

with the choice of the canonical matrix units for \( M_2(\mathbb{C}) \), the matrices \( X_\alpha \) are \( X_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \), \( X_{12} = X_{21} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \), and \( X_{22} = I_2 \). All the matrices \( X_\alpha X_\alpha^* \) are diagonal, hence they are normal and commute. However, the matrices \( X_{11}X_{22}^* \) and \( X_{12}X_{22}^* \) do not commute, so the \( 4 \times 4 \) matrix \( X \) does not satisfy the equivalent conditions from theorem A.1, hence it does not have a block-SVD.

**Corollary A.5.** The set \( M_{\text{block-diag}}^A \) is a real algebraic variety.

**Proof.** A matrix \( X \) belongs to \( M_{\text{block-diag}}^A \) if and only if the two families of \( n^4 \) matrices \( \{ X_\alpha X_\alpha^* \} \) and \( \{ X_\alpha^* X_\alpha \} \) commute; these commutations conditions can be restated as (degree 4) polynomial conditions in the real and imaginary parts of the elements of \( X \). \[\square\]

Before computing in the next proposition the dimension of the real algebraic variety \( M_{\text{block-diag}}^A \), we would like to give a heuristic argument in the form of parameter counting. The
choice of the two orthonormal bases \( \{ e_i \} \) and \( \{ f_i \} \) in (32) corresponds to a total of \( 2k^2 \) real parameters, since \( \text{dim}_\mathbb{R} U_k = k^2 \). Each matrix \( X_i \) accounts for \( 2n^2 \) real parameters, so, in total, we get \( 2kn^2 \) extra real parameters. However, in each term \( X_i \otimes e_if_i^* \), two of the three complex phases of \( X_i \), \( e_i \), \( f_i \) are redundant, so we have over counted \( 2k^2 \) real parameters. We conclude that the real dimension of \( \mathcal{M}^k_{\text{block-diag}} \) should be \( 2k^2 + 2kn^2 - 2k \), fact which we rigorously prove next.

Proposition A.6. The real dimension of the algebraic variety \( \mathcal{M}^k_{\text{block-diag}} \) is \( 2k(n^2 + k - 1) \).

Proof. For the terminology and the results used in this proof, we refer the reader to [13, chapter 11]. Let us introduce the flag manifold (see [13, example 8.34] or [6, section 4.9])

\[
\mathcal{F}l_k = U_k/(U_k^f),
\]

which has real dimension \( \text{dim}_\mathbb{R} \mathcal{F}l_k = k^2 - k \). Consider the map

\[
\varphi : \mathcal{M}_n(\mathbb{C})^k \times \mathcal{F}l_k \times \mathcal{F}l_k \rightarrow \mathcal{M}^k_{\text{block-diag}} \subset \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C})
\]

\[
((A_i)_{i=1}^k, (e_i)_{i=1}^k, (f_i)_{i=1}^k) \mapsto \sum_{i=1}^k A_i \otimes e_if_i^*.
\]

Obviously, \( \varphi \) is surjective, so we have \( \text{dim}_\mathbb{R} \mathcal{M}^k_{\text{block-diag}} \leq 2k(n^2 + k - 1) \). To get the reverse inequality, define \( \mathcal{M}_n(\mathbb{C})^k \) to be the set of pairwise distinct \( k \)-tuples of matrices. It is trivial to check that the map \( \tilde{\varphi} \), obtained by restricting \( \varphi \) to \( \mathcal{M}_n(\mathbb{C})^k \), is \( k! \)-to-one, so the conclusion follows. \( \square \)

References

[1] Attal S, Deschamps J and Pellegrini C Complex obtuse random walks and their continuous-time limit Probab. Theory Relat. Fields 165 65–116
[2] Attal S, Deschamps J and Pellegrini C Classical noises emerging from quantum environments (in preparation)
[3] Attal S and Pautrat Y 2006 From repeated to continuous quantum interactions Ann. Henri Poincaré 7 59–104
[4] Alfsen E and Shultz F 2012 Finding decompositions of a class of separable states Linear Algebr. Appl. 437 2613–29
[5] Banica T 2013 The defect of generalized Fourier matrices Linear Algebr. Appl. 438 3667–88
[6] Bengtsson I and Życzkowski K 2006 Geometry of Quantum States (Cambridge: Cambridge University Press)
[7] Collins B and Nechita I 2010 Random quantum channels: I. Graphical calculus and the Bell state phenomenon Commun. Math. Phys. 297 345–70
[8] Đakić B, Vedral V and Brukner C 2010 Necessary and sufficient condition for non-zero quantum discord Phys. Rev. Lett. 105 190502
[9] Deschamps J Émergence du bruit dans les systèmes ouverts classiques et quantiques PhD Thesis University of Lyon (https://tel.archives-ouvertes.fr/tel-01169896)
[10] Doković D and Li C-K 1994 Overgroups of some classical linear groups with applications to linear preserver problems Linear Algebr. Appl. 197–198 31–61
[11] Duan R and Winter A 2016 No-signalling assisted zero-error capacity of quantum channels and an information theoretic interpretation of the Lovász number IEEE Trans. Inf. Theory 2 891–914
[12] Gantmacher F R 1960 The Theory of Matrices, I (New York: Chelsea Publishing Company)
[13] Harris J 2013 Algebraic Geometry: a First Course vol 133 (New York: Springer Science & Business Media)
[14] Horn R A and Johnson C R 1985 Matrix Analysis 1st edn (Cambridge: Cambridge University Press)
[15] Hillery M, Ziman M and Bužek V 2002 Implementation of quantum maps by programmable quantum processors Phys. Rev. A 66 042302
[16] Jiang Z, Piani M and Caves C M 2013 Ancilla models for quantum operations: for what unitaries does the ancilla state have to be physical? Quantum Inf. Process. 12 1999–2017
[17] Karumanchi S, Mancini S, Winter A and Yang D 2016 Quantum channel capacities with passive environment assistance IEEE Trans. Inf. Theory 62 1733–47
[18] Karumanchi S, Mancini S, Winter A and Yang D 2016 Classical capacities of quantum channels with environment assistance arXiv:1602.02036
[19] Landau L J and Streater R F 1993 On Birkhoff’s theorem for doubly stochastic completely positive maps of matrix algebras Linear Algebr. Appl. 193 107–27
[20] Nielsen M and Chuang I 2010 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[21] Parthasarathy K R 1992 An Introduction to Quantum Stochastic Calculus (Boston, MA: Birkhauser)
[22] Stinespring W F 1955 Positive functions on $C^*$-algebras Proc. Am. Math. Soc. 6 211–6
[23] Tadej W and Óczkowski K 2008 Defect of a unitary matrix Linear Algebr. Appl. 429 447–81
[24] Yu N, Duan R and Xu Q 2012 Bounds on the distance between a unital quantum channel and the convex hull of unitary channels, with applications to the asymptotic quantum Birkhoff conjecture (arXiv:1201.1172)
[25] Ziman M and Bužek V 2005 All (qubit) decoherences: complete characterization and physical implementation Phys. Rev. A 72 022110