

# Characterization of linear maps on $M_n$ whose multiplicity maps have maximal norm, with an application in quantum information

Daniel Puzzuoli

Department of Applied Mathematics and Institute for Quantum Computing  
University of Waterloo, Waterloo, Ontario, Canada  
February 5, 2018

Given a linear map  $\Phi : M_n \rightarrow M_m$ , its multiplicity maps are defined as the family of linear maps  $\Phi \otimes \text{id}_k : M_n \otimes M_k \rightarrow M_m \otimes M_k$ , where  $\text{id}_k$  denotes the identity on  $M_k$ . Let  $\|\cdot\|_1$  denote the trace-norm on matrices, as well as the induced trace-norm on linear maps of matrices, i.e.  $\|\Phi\|_1 = \max\{\|\Phi(X)\|_1 : X \in M_n, \|X\|_1 = 1\}$ . A fact of fundamental importance in both operator algebras and quantum information is that  $\|\Phi \otimes \text{id}_k\|_1$  can grow with  $k$ . In general, the rate of growth is bounded by  $\|\Phi \otimes \text{id}_k\|_1 \leq k\|\Phi\|_1$ , and matrix transposition is the canonical example of a map achieving this bound. We prove that, up to an equivalence, the transpose is the unique map achieving this bound. The equivalence is given in terms of complete trace-norm isometries, and the proof relies on a particular characterization of complete trace-norm isometries regarding preservation of certain multiplication relations.

We use this result to characterize the set of single-shot quantum channel discrimination games satisfying a norm relation that, operationally, implies that the game can be won with certainty using entanglement, but is hard to win without entanglement. Specifically, we show that the well-known example of such a game, involving the Werner-Holevo channels, is essentially the unique game satisfying this norm relation. This constitutes a step towards a characterization of single-shot quantum channel discrimination games with maximal gap between optimal performance of entangled and unentangled strategies.

## 1 Introduction

For a linear map  $\Phi : M_n \rightarrow M_m$ , it is a well-known phenomenon that the norm of the multiplicity maps  $\Phi \otimes \text{id}_k : M_n \otimes M_k \rightarrow M_m \otimes M_k$  can grow with  $k$ . This phenomenon has been extensively studied within the theory of  $C^*$ -algebras, leading to the topic of completely bounded maps [1–3]. Within the field of quantum information, this phenomenon is connected to the study of entanglement. For a density matrix  $\rho \in M_n \otimes M_k$ , if

$$\|(\Phi \otimes \text{id}_k)(\rho)\|_1 > \|\Phi\|_1, \quad (1)$$

then  $\rho$  is entangled, and a well-known result in quantum information is that the existence of a positive linear map  $\Phi$  for which the above holds is also necessary for  $\rho$  to be entangled

[4]. Indeed, one of the simplest and most well-known entanglement measures is the *negativity* [5], which, up to additive and multiplicative scalars is defined as  $\|(T_n \otimes \text{id}_k)(\rho)\|_1$ , where  $T_n$  is the transpose on  $M_n$ . Hence, the growth of the norms of multiplicity maps is of fundamental mathematical interest, and is deeply connected to the study and quantification of entanglement in quantum information.<sup>1</sup>

While the norm of  $\Phi \otimes \text{id}_k$  may grow with  $k$ , the growth rate is limited. For any linear map  $\Phi : M_n \rightarrow M_m$  it generically holds that

$$\|\Phi \otimes \text{id}_k\|_1 \leq k\|\Phi\|_1. \quad (2)$$

In this paper we are concerned with linear maps on matrices and will use the trace-norm, but we note that this fact is known much more generally (in terms of the C\*-norm) for maps on unital C\*-algebras (see [3, Exercise 3.10]). Provided  $k \leq n$ , the canonical example of a map achieving equality in Equation (2) is the matrix transpose  $T_n$  [6].

Our main result is a characterization of the maps achieving equality in Equation (2). We prove that, up to an equivalence, the transpose is in fact the *only* map achieving equality in Equation (2). More specifically, a linear map  $\Phi : M_n \rightarrow M_m$  satisfies Equation (2) with equality if and only if there exists an isometric embedding of  $M_k$  into  $M_n$  on which  $\Phi$  acts as the transpose followed by a complete trace-norm isometry.

The proof relies on a characterization of complete trace-norm isometries particularly suited to the problem. This characterization (among others proved) relates to how complete trace-norm isometries preserve certain multiplication relations. For example, if a linear map  $\Phi : M_n \rightarrow M_m$  is a complete trace-norm isometry, and if  $A^*B = C^*D$  for  $A, B, C, D \in M_n$ , then  $\Phi(A)^*\Phi(B) = \Phi(C)^*\Phi(D)$ . These statements and their proofs are somewhat similar to multiplicative domain proofs for unital completely-positive maps on C\*-algebras [7] (see also [3, Theorem 3.18]). We remark that the structure of complete trace-norm isometries on  $M_n$ , and consequently some of the other characterizations we give, may be deduced from the more general structure of (not necessarily complete) trace-norm isometries given in [8]. Nevertheless, we give self-contained proofs, and in some cases are able to utilize the “complete” assumption to prove certain implications in more generality (e.g. when the domain is a subspace  $V \subset M_n$ ), which may be of independent interest.

We also apply the main result in the setting of single-shot quantum channel discrimination, which is the task of determining which of two known quantum channels is acting on a system given only a single use of the channel. As we will describe in detail in Section 5, this task may be formulated as a game parametrized by a triple  $(\lambda, \Gamma_0, \Gamma_1)$ , where  $\Gamma_0, \Gamma_1 : M_n \rightarrow M_m$  are quantum channels, and  $\lambda \in [0, 1]$  is a probability. Letting  $\|\cdot\|_1$  denote the completely bounded trace-norm (see Section 2), we characterize such triples satisfying the norm relation

$$1 = \|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1 = n\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1. \quad (3)$$

Operationally, the above norm relations imply that the game can be won with certainty using entanglement, but is hard to win without entanglement. In particular, we prove that the triple  $(\lambda, \Gamma_0, \Gamma_1)$  satisfies Equation (3) if and only if it is in some sense equivalent to a game involving the Werner-Holevo channels which is known to satisfy Equation (3) (see [9, Example 3.36]).

In Section 2 we provide some background and definitions. In Section 3 we prove various characterizations of complete trace-norm isometries. One characterization in particular is

<sup>1</sup>Note that, in quantum information the trace-norm is typically used, whereas in operator algebras the operator norm is typically used. Due to the duality of these norms, it is possible to translate facts about one norm into facts about the other. For example, in this paper, we reference the C\*-algebra literature for facts about the trace-norm, even though the trace-norm does not explicitly appear in the references. For readers unfamiliar with this duality, we describe the relevant facts in Appendix A.

specially suited for later use, but we also include other characterizations; including one that may naturally be interpreted as a linear map being a complete trace-norm isometry if and only if its Choi matrix is maximally entangled. In Section 4 we prove the main result, which characterizes the linear maps  $\Phi : M_n \rightarrow M_m$  for which  $\|\Phi \otimes \text{id}_k\|_1 = k\|\Phi\|_1$ , and as a Corollary characterize the maps for which  $\|\Phi\|_1 = n\|\Phi\|_1$ . In Section 5 we use the main result to prove that the Werner-Holevo channel discrimination game is in some sense the unique game (with input dimension  $n$ ) satisfying Equation (3). Finally, we end with a discussion of open problems in Section 6.

## 2 Notation and background

For an integer  $1 \leq a \leq n$  we denote  $e_a \in \mathbb{C}^n$  to be the vector with a 1 in the  $a^{\text{th}}$  entry, and zeroes everywhere else. Similarly, for integers  $1 \leq a, b \leq n$ , we denote  $E_{a,b} \in M_n$  to be the elementary matrix with a 1 in the  $(a, b)$ -entry and zeroes in all other entries.

For a matrix  $A$ , the trace-norm is defined as  $\|A\|_1 = \text{Tr}(\sqrt{A^*A})$ , and for a linear map  $\Phi : M_n \rightarrow M_m$ , the induced trace-norm of  $\Phi$  is given by

$$\|\Phi\|_1 = \max\{\|\Phi(X)\|_1 : X \in M_n, \|X\|_1 \leq 1\}. \quad (4)$$

The completely bounded trace norm is given by

$$\|\Phi\|_1 = \sup\{\|\Phi \otimes \text{id}_k\|_1 : k \geq 1\} = \|\Phi \otimes \text{id}_n\|_1. \quad (5)$$

For a linear map  $\Phi : M_n \rightarrow M_m$ , we will use  $J(\Phi)$  to denote its Choi matrix [10], which we define as

$$J(\Phi) = \sum_{a,b=1}^n \Phi(E_{a,b}) \otimes E_{a,b}. \quad (6)$$

We will use  $T_n$  to denote the transpose on  $M_n$ , and write  $T_n(A)$  or  $A^T$  to denote the transpose of a matrix  $A \in M_n$ .

We will need a few concepts from quantum information, even for the sections not directly involving that topic. An element  $\rho \in M_n$  is called a *density matrix* if  $\rho \geq 0$  and  $\text{Tr}(\rho) = 1$ . A *quantum channel* is a linear map  $\Gamma : M_n \rightarrow M_m$  that is completely positive and trace preserving.

We will also use the term *maximal entanglement*. A unit vector  $u \in \mathbb{C}^n \otimes \mathbb{C}^m$  is called *maximally entangled* if, for  $r = \min(n, m)$ , there exists orthonormal sets of unit vectors  $\{x_a\}_{a=1}^r \subset \mathbb{C}^n$  and  $\{y_a\}_{a=1}^r \subset \mathbb{C}^m$  for which

$$u = \sqrt{\frac{1}{r}} \sum_{a=1}^r x_a \otimes y_a. \quad (7)$$

As mentioned in the introduction, the *negativity* of a density matrix  $\rho \in M_n \otimes M_m$  is defined (up to multiplicative and additive scalars) as  $\|(T_n \otimes \text{id}_m)(\rho)\|_1$  [5]. This expression is meant to quantify the entanglement of the density matrix  $\rho$ . If  $\rho$  is *pure*, i.e.  $\rho = uu^*$  for a unit vector  $u \in \mathbb{C}^n \otimes \mathbb{C}^m$ , then the negativity achieves its maximum value of  $\min(n, m)$  if and only if  $u$  is maximally entangled. Theorem 7 of [11], which we now state, provides a characterization of matrices  $X \in M_n \otimes M_m$  with  $\|X\|_1 = 1$  and satisfying  $\|(T_n \otimes \text{id}_m)(X)\|_1 = n$ . While it is not physically meaningful if  $X$  is not a density matrix, the theorem loosely provides a notion of “maximal entanglement” for arbitrary elements of  $M_n \otimes M_m$ .

**Theorem 1.** Let  $X \in M_n \otimes M_m$  with  $\|X\|_1 \leq 1$ . The following are equivalent.

1.  $\|(T_n \otimes \text{id}_m)(X)\|_1 = n$ .
2.  $m \geq n$ , and there exists a positive integer  $r \leq m/n$ , a density matrix  $\sigma \in M_r$ , and isometries  $U, V : \mathbb{C}^n \otimes \mathbb{C}^r \rightarrow \mathbb{C}^m$  for which

$$X = (\mathbb{1}_n \otimes U)(\tau_n \otimes \sigma)(\mathbb{1}_n \otimes V^*), \quad (8)$$

where  $\tau_n = \frac{1}{n} \sum_{a,b=1}^n E_{a,b} \otimes E_{a,b} \in M_n \otimes M_n$  is the canonical maximally entangled state.

If  $X$  is a density matrix then the above equivalence holds with  $V = U$ .

**Remark 2.** We will make use of the additional special case of the above theorem when  $X$  is Hermitian. In this case the second statement may be rewritten as:  $m \geq n$ , and there exists a positive integer  $r \leq m/n$ , a Hermitian matrix  $H \in M_r$  with  $\|H\|_1 = 1$ , and an isometry  $U : \mathbb{C}^n \otimes \mathbb{C}^r \rightarrow \mathbb{C}^m$  for which

$$X = (\mathbb{1}_n \otimes U)(\tau_n \otimes H)(\mathbb{1}_n \otimes U^*). \quad (9)$$

The only change necessary to the proof is to take a spectral decomposition of  $X$ , rather than a singular value decomposition. The rest of the proof follows as before.

The last notion in quantum information that we will make use of is that of reversible quantum channels. A linear map  $\Phi : M_n \rightarrow M_m$  is called a *reversible quantum channel* if it is a quantum channel, and has a left inverse  $\Psi : M_m \rightarrow M_n$  that is also a quantum channel.<sup>2</sup> Due to its connection to error correction, conditions for reversibility (or recoverability) of a channel continue to be extensively studied in various settings (for example, see [12, 13]).

### 3 Complete trace-norm isometries

Let  $V \subset M_n$  be a subspace, and  $\Phi : V \rightarrow M_m$  be a linear map. We say that  $\Phi$  is a *k-trace-norm isometry* (or that it is *k-trace-norm isometric*) if  $\Phi \otimes \text{id}_k : V \otimes M_k \rightarrow M_m \otimes M_k$  is a trace-norm isometry, and say that it is a *complete trace-norm isometry* (or that it is *completely trace-norm isometric*) if it is a *k-trace-norm isometry* for all integers  $k \geq 1$ .

The purpose of this section is to give various characterizations of complete trace-norm isometries taking  $M_n$  into  $M_m$ . Note that the structure of surjective operator norm isometries (and hence surjective complete operator norm isometries) between  $\mathbb{C}^*$ -algebras is well-known [14]. Furthermore, in the matrix algebra case, a characterization of (not necessarily surjective) operator norm isometries mapping  $M_n \rightarrow M_k$  has been given for the case  $k \leq 2n - 1$  [15]. However, the dual/adjoint of a trace-norm isometry need not be an operator norm isometry, and so it is not possible to import those results here.

We give the various characterizations in the theorem below. Remarks and some background on what is already known, as well as some intermediate results, are given before its proof.

<sup>2</sup>This terminology is motivated by the fact that quantum channels model physical processes, and so a quantum channel having a left inverse that is also a quantum channel means that it can be physically undone, or reversed.

**Theorem 3.** For a linear map  $\Phi : M_n \rightarrow M_m$  the following are equivalent.

1.  $\Phi$  is a complete trace-norm isometry.
2.  $\Phi$  is a 2-trace-norm isometry.
3. For  $A, B, C, D \in M_n$  the following implications hold:
  - $A^*B = C^*D \implies \Phi(A)^*\Phi(B) = \Phi(C)^*\Phi(D)$ , and
  - $AB^* = CD^* \implies \Phi(A)\Phi(B)^* = \Phi(C)\Phi(D)^*$ ,
and  $\|\Phi(X)\|_1 = \|X\|_1$  for some  $X \in M_n \setminus \{0\}$ .
4. For  $A, B \in M_n$  the following implications hold:
  - $A^*B = 0 \implies \Phi(A)^*\Phi(B) = 0$ , and
  - $AB^* = 0 \implies \Phi(A)\Phi(B)^* = 0$ ,
and  $\|\Phi(X)\|_1 = \|X\|_1$  for some  $X \in M_n \setminus \{0\}$ .
5. For rank-1  $A, B \in M_n$  the following implications hold:
  - $A^*B = 0$  and  $A^*A = B^*B \implies \Phi(A)^*\Phi(B) = 0$ , and
  - $AB^* = 0$  and  $AA^* = BB^* \implies \Phi(A)\Phi(B)^* = 0$ ,
and  $\|\Phi(X)\|_1 = \|X\|_1$  for some  $X \in M_n \setminus \{0\}$ .
6.  $\|J(\Phi)\|_1 = n$  and  $\|J(\Phi T_n)\|_1 = n^2$ .
7.  $m \geq n$ , and there exists a positive integer  $r \leq m/n$ , a density matrix  $\sigma \in M_r$ , and isometries  $U, V : \mathbb{C}^n \otimes \mathbb{C}^r \rightarrow \mathbb{C}^m$  for which

$$\Phi(X) = U(X \otimes \sigma)V^* \quad (10)$$

for all  $X \in M_n$ .

8.  $\|\Phi\|_1 = 1$ , and  $\Phi$  has a left inverse  $\Psi : M_m \rightarrow M_n$  with  $\|\Psi\|_1 = 1$ .

If, in addition,  $\Phi$  is positive, then statement 7 holds with  $V = U$ , making  $\Phi$  a quantum channel, and  $\Psi$  may also be taken to be a quantum channel in statement 8 (and hence,  $\Phi$  is a reversible quantum channel).

Before continuing some comments on the theorem are in order. In statement 6, the norm  $\|J(\Phi T_n)\|_1$  appears, but this specific location of the transpose is an arbitrary notational choice. Using the definition of the Choi matrix and properties of the transpose, it may be verified that

$$\|J(\Phi T_n)\|_1 = \|J(T_n \Phi)\|_1 = \|(T_n \otimes \text{id}_n)(J(\Phi))\|_1 = \|(\text{id}_m \otimes T_n)(J(\Phi))\|_1 \quad (11)$$

for any linear map  $\Phi : M_n \rightarrow M_m$ . As per the discussion in Section 2 regarding entanglement negativity, the expressions in Equation (11) can be roughly interpreted as a measure of how entangled  $J(\Phi)$  is. With this interpretation, the characterization given in statement 6 says that  $\Phi$  is a complete trace-norm isometry if and only if its Choi matrix is maximally entangled (and has a particular normalization).

Statements 3, 4, and 5 concern the map  $\Phi$  preserving certain kinds of multiplication. The intuition for these statements comes from the explicit structure given in statement

7. However, in our proof, we show how they follow directly from the assumptions of  $\Phi$  being either a complete or 2-trace-norm isometry. The benefit of these alternative proofs, which we give separately in Proposition 5 below, is that they work in more generality (i.e. in the proposition we only use that the domain is a subspace  $V \subset M_n$ ), and so may be of independent interest. We also note that statement 5 may seem oddly specific, but it is included for being specially suited for proving the theorem in the following section.

Lastly, while we give a complete proof of the above theorem, several equivalences may be deduced from [8], whose title “Isometries for Ky Fan Norms between Matrix Spaces” is self-explanatory of its content. In particular, as a special case of the results therein, an explicit structural characterization of (not necessarily complete) trace-norm isometries taking  $M_n$  into  $M_m$  is given. From this, the explicit structure of complete trace-norm isometries may be deduced by refining this structure, and indeed, this refinement only requires the additional assumption that the map is a 2-trace-norm isometry. Thus, the equivalence of statements 1, 2, and 7 may be viewed as a special case of the main theorem in [8]. Furthermore, the general technique of the proofs we give are in line with those of [8], and with linear norm preserver problems more generally [16]: translating between norm relations and algebraic relations for matrices. (See [17] for a survey of results on isometries of matrix spaces for unitarily invariant norms.)

With this last comment, we begin the proof of Theorem 3 with the following equivalence between a trace-norm relation for a  $2 \times 2$  block-matrix, and statements about how the blocks multiply.

**Proposition 4.** *For matrices  $A, B, C, D \in M_n$ , it holds that*

$$\left\| \begin{pmatrix} A & B \\ C & D \end{pmatrix} \right\|_1 = \|A\|_1 + \|B\|_1 + \|C\|_1 + \|D\|_1, \quad (12)$$

*if and only if*

$$A^*B = AC^* = D^*C = DB^* = 0. \quad (13)$$

*Proof.* In [11, Proposition 6] it was shown that, for any Hilbert-Schmidt orthogonal set of matrices  $\{A_i\}_{i=1}^r$  – all with the same dimensions, not necessarily square – it holds that

$$\left\| \sum_{i=1}^r A_i \right\|_1 = \sum_{i=1}^r \|A_i\|_1, \quad (14)$$

if and only if  $A_i^*A_j = 0$  and  $A_iA_j^* = 0$  for all  $i \neq j$ . The current proposition follows by application of this fact to the set  $\{A \otimes E_{1,1}, B \otimes E_{1,2}, C \otimes E_{2,1}, D \otimes E_{2,2}\} \subset M_n \otimes M_2$ .  $\square$

Next, we prove a proposition containing some of the implications required for Theorem 3, but in more generality. We note that the proof takes inspiration from multiplicative domain proofs for unital and completely positive linear maps on C\*-algebras (see [7] and [3, Theorem 3.18]).

**Proposition 5.** *Let  $V \subset M_n$  be a subspace, and let  $\Phi : V \rightarrow M_n$  be linear.*

1. *If  $\Phi$  is a 2-trace-norm isometry, then for  $A, B \in V$  the following implications hold:*

- $A^*B = 0 \implies \Phi(A)^*\Phi(B) = 0$ , and
- $AB^* = 0 \implies \Phi(A)\Phi(B)^* = 0$ .

2. *If  $\Phi$  is a complete trace-norm isometry, then for  $A, B, C, D \in V$  the following implications hold:*

- $A^*B = C^*D \implies \Phi(A)^*\Phi(B) = \Phi(C)^*\Phi(D)$ , and
- $AB^* = CD^* \implies \Phi(A)\Phi(B)^* = \Phi(C)\Phi(D)^*$ .

*Proof.* First, assume  $\Phi$  is a 2-trace-norm isometry and let  $A, B \in V$ . Assuming  $A^*B = 0$ , we have

$$\left\| \begin{pmatrix} \Phi(A) & \Phi(B) \\ 0 & 0 \end{pmatrix} \right\|_1 = \left\| \begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix} \right\|_1 = \|A\|_1 + \|B\|_1 = \|\Phi(A)\|_1 + \|\Phi(B)\|_1, \quad (15)$$

where the second equality is by Proposition 4. Hence, also by Proposition 4, equality between the first and last expressions implies that  $\Phi(A)^*\Phi(B) = 0$ . Similarly, if  $AB^* = 0$ , then

$$\left\| \begin{pmatrix} \Phi(A) & 0 \\ \Phi(B) & 0 \end{pmatrix} \right\|_1 = \left\| \begin{pmatrix} A & 0 \\ B & 0 \end{pmatrix} \right\|_1 = \|A\|_1 + \|B\|_1 = \|\Phi(A)\|_1 + \|\Phi(B)\|_1, \quad (16)$$

and so  $\Phi(A)\Phi(B)^* = 0$ .

Next, assume  $\Phi$  is a complete trace-norm isometry on  $V$ , and let  $A, B, C, D \in V$ . If  $A^*B = C^*D$ , then

$$\begin{pmatrix} A & 0 \\ -C & 0 \end{pmatrix}^* \begin{pmatrix} B & 0 \\ D & 0 \end{pmatrix} = 0. \quad (17)$$

Under the assumption that  $\Phi$  is completely trace-norm isometric,  $\Phi \otimes \text{id}_2$  is a 2-trace-norm isometry, and so, by the 2-trace-norm isometry case, it holds that

$$\begin{pmatrix} \Phi(A) & 0 \\ -\Phi(C) & 0 \end{pmatrix}^* \begin{pmatrix} \Phi(B) & 0 \\ \Phi(D) & 0 \end{pmatrix} = 0, \quad (18)$$

giving  $\Phi(A)^*\Phi(B) = \Phi(C)^*\Phi(D)$ . Similarly, if  $AB^* = CD^*$ , then

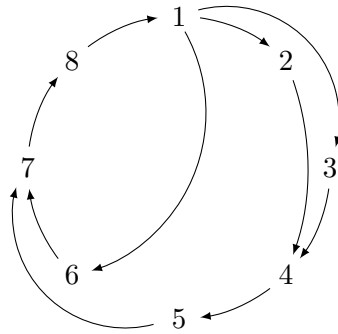
$$\begin{pmatrix} A & -C \\ 0 & 0 \end{pmatrix} \begin{pmatrix} B & D \\ 0 & 0 \end{pmatrix}^* = 0, \quad (19)$$

and again the 2-trace-norm isometry case implies that

$$\begin{pmatrix} \Phi(A) & -\Phi(C) \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \Phi(B) & \Phi(D) \\ 0 & 0 \end{pmatrix}^* = 0, \quad (20)$$

giving  $\Phi(A)\Phi(B)^* = \Phi(C)\Phi(D)^*$ . □

*Proof of Theorem 3.* We prove the implications in the diagram below.



The implications appear in the order:  $1 \Rightarrow 2$ ,  $3 \Rightarrow 4 \Rightarrow 5$ ,  $1 \Rightarrow 6$ ,  $2 \Rightarrow 4$ ,  $1 \Rightarrow 3$ ,  $8 \Rightarrow 1$ ,  $6 \Rightarrow 7$ ,  $7 \Rightarrow 8$ , and  $5 \Rightarrow 7$ . All implications except  $5 \Rightarrow 7$ , which is technically involved, follow essentially immediately from facts already given. The modified statements for the special case when  $\Phi$  is positive are given before the proof of  $5 \Rightarrow 7$ .

The implications that are immediate due to subsequent statements being logically weaker are  $1 \Rightarrow 2$  and  $3 \Rightarrow 4 \Rightarrow 5$ . The implication  $1 \Rightarrow 6$  follows from the norm relations

$$\|J(\text{id}_n)\|_1 = n \text{ and } \|J(T_n)\|_1 = n^2, \quad (21)$$

and  $\Phi$  being a complete trace-norm isometry. The implications  $2 \Rightarrow 4$  and  $1 \Rightarrow 3$  are both the content of Proposition 5, and the implication  $8 \Rightarrow 1$  is straightforward to verify.

For  $6 \Rightarrow 7$ , the norm values of statement 6 imply by Theorem 1 that there exists a positive integer  $r \leq m/n$ , a density matrix  $\sigma \in M_r$ , and isometries  $U, V : \mathbb{C}^r \otimes \mathbb{C}^n \rightarrow \mathbb{C}^m$  for which

$$\frac{1}{n}J(\Phi) = (U \otimes \mathbb{1}_n)(\sigma \otimes \tau_n)(V^* \otimes \mathbb{1}_n). \quad (22)$$

This is equivalent to the required form for  $\Phi$ .

For  $7 \Rightarrow 8$ , define  $\Psi(Y) = \text{Tr}_{M_r}(U^*YV)$  for  $Y \in M_m$ , where  $\text{Tr}_{M_r}$  is the partial trace of  $M_r$ . Using the fact that the trace-norm is non-increasing under partial trace, it may be verified that  $\Psi$  has the required properties.

For the special case when  $\Phi$  is positive, return to the proof of the implication  $6 \Rightarrow 7$ . As  $\Phi$  is Hermiticity preserving, by Remark 2 and Theorem 1, there exists a Hermitian  $H \in M_r$  with  $\|H\|_1 = 1$ , and an isometry  $U : \mathbb{C}^n \otimes \mathbb{C}^r \rightarrow \mathbb{C}^m$  for which  $\Phi(X) = U(X \otimes H)U^*$  for all  $X \in M_n$ . That  $\Phi$  is positive implies  $H \geq 0$ , making  $H$  a density matrix, and giving  $\Phi$  the required form. To see that  $\Psi$  may also be taken to be a quantum channel in statement 8, we define  $\Psi$  as as in the proof of  $7 \Rightarrow 8$  with a slight modification. Fix a density matrix  $\eta \in M_n$ , and set  $\Psi(Y) = \text{Tr}_{M_r}(U^*YU) + \text{Tr}((\mathbb{1}_m - UU^*)Y)\eta$  for all  $Y \in M_m$ . It is routine to verify that  $\Psi$  is a quantum channel and that  $\Psi\Phi = \text{id}_n$ .

Lastly, we show  $5 \Rightarrow 7$ . We will use the assumption in statement 5 to build further facts about how outputs of  $\Phi$  on rank-1 matrices multiply, which we break into a series of claims.

**Claim 1.** For unit vectors  $x_1, x_2, y \in \mathbb{C}^n$  with  $\langle x_1, x_2 \rangle = 0$ , it holds that

$$\Phi(x_1y^*)^*\Phi(x_1y^*) = \Phi(x_2y^*)^*\Phi(x_2y^*) \text{ and } \Phi(yx_1^*)\Phi(yx_1^*)^* = \Phi(yx_2^*)\Phi(yx_2^*)^*. \quad (23)$$

To see the first equality, note that  $x_1 + x_2 \perp x_1 - x_2$ , and so

$$0 = \Phi((x_1 + x_2)y^*)^*\Phi((x_1 - x_2)y^*) \quad (24)$$

$$= \Phi(x_1y^*)^*\Phi(x_1y^*) - \Phi(x_1y^*)^*\Phi(x_2y^*) + \Phi(x_2y^*)^*\Phi(x_1y^*) - \Phi(x_2y^*)^*\Phi(x_2y^*) \quad (25)$$

$$= \Phi(x_1y^*)^*\Phi(x_1y^*) - \Phi(x_2y^*)^*\Phi(x_2y^*), \quad (26)$$

where the second and third term in Equation (25) are 0 by application of statement 5. This gives the desired equality, and it follows similarly that  $\Phi(yx_1^*)\Phi(yx_1^*)^* = \Phi(yx_2^*)\Phi(yx_2^*)^*$ .

**Claim 2.** For any  $x_1, x_2, y_1, y_2 \in \mathbb{C}^n$  with  $\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle = 0$ , it holds that

$$\Phi(x_1y_1^*)^*\Phi(x_2y_2^*) = 0 \text{ and } \Phi(x_1y_1^*)\Phi(x_2y_2^*)^* = 0. \quad (27)$$

For the first equality, assuming without loss of generality that  $x_1, x_2, y_1$ , and  $y_2$  have unit length, Claim 1 gives that  $\Phi(x_1y_1^*)\Phi(x_1y_1^*)^* = \Phi(x_1y_2^*)\Phi(x_1y_2^*)^*$ , and statement 5 gives that  $\Phi(x_1y_2^*)\Phi(x_2y_2^*) = 0$ . These equalities imply the range relations

$$\text{ran}(\Phi(x_1y_1^*)) = \text{ran}(\Phi(x_1y_2^*)) \perp \text{ran}(\Phi(x_2y_2^*)), \quad (28)$$



which imply  $\Phi(x_1y_1^*)^*\Phi(x_2y_2^*) = 0$ . It similarly follows that  $\Phi(x_1y_1^*)\Phi(x_2y_2^*)^* = 0$ .

**Claim 3.** For unit vectors  $x_1, x_2, y_1, y_2 \in \mathbb{C}^n$  with  $\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle = 0$ , it holds that

$$\Phi(x_1y_1^*)^*\Phi(x_1y_2^*) = \Phi(x_2y_1^*)^*\Phi(x_2y_2^*), \text{ and } \Phi(x_1y_1^*)\Phi(x_2y_1^*)^* = \Phi(x_1y_2^*)\Phi(x_2y_2^*)^*. \quad (29)$$

For the first equality,  $x_1 + x_2 \perp x_1 - x_2$ , so Claim 2 implies

$$0 = \Phi((x_1 + x_2)y_1^*)^*\Phi((x_1 - x_2)y_2^*) \quad (30)$$

$$= \Phi(x_1y_1^*)^*\Phi(x_1y_2^*) - \Phi(x_1y_1^*)^*\Phi(x_2y_2^*) + \Phi(x_2y_1^*)^*\Phi(x_1y_2^*) - \Phi(x_2y_1^*)^*\Phi(x_2y_2^*) \quad (31)$$

$$= \Phi(x_1y_1^*)^*\Phi(x_1y_2^*) - \Phi(x_2y_1^*)^*\Phi(x_2y_2^*), \quad (32)$$

where we have used Claim 2 to determine that  $\Phi(x_1y_1^*)^*\Phi(x_2y_2^*) = \Phi(x_2y_1^*)^*\Phi(x_1y_2^*) = 0$ . It may be similarly reasoned that  $\Phi(x_1y_1^*)\Phi(x_2y_1^*)^* = \Phi(x_1y_2^*)\Phi(x_2y_2^*)^*$ .

We now use Claims 1 to 3 to construct the explicit structure of  $\Phi$  by examining how it acts on elementary matrices. By Claim 1 it holds that

$$\Phi(E_{1,1})^*\Phi(E_{1,1}) = \Phi(E_{a,1})^*\Phi(E_{a,1}) \text{ and } \Phi(E_{1,1})\Phi(E_{1,1})^* = \Phi(E_{1,b})\Phi(E_{1,b})^* \quad (33)$$

for all  $1 \leq a, b \leq n$ , and hence there exists partial isometries

$$U_a : \text{ran}(\Phi(E_{1,1})) \rightarrow \text{ran}(\Phi(E_{a,1})), \text{ and } V_b : \text{ran}(\Phi(E_{1,1})^*) \rightarrow \text{ran}(\Phi(E_{1,b})^*) \quad (34)$$

for which  $\Phi(E_{a,1}) = U_a\Phi(E_{1,1})$  and  $\Phi(E_{1,b}) = \Phi(E_{1,1})V_b^*$  (where  $U_1$  and  $V_1$  may be taken to be the orthogonal projections onto  $\text{ran}(\Phi(E_{1,1}))$  and  $\text{ran}(\Phi(E_{1,1})^*)$  respectively). Note as well that, statement 5 gives that  $\Phi(E_{a,1})^*\Phi(E_{a',1}) = \Phi(E_{1,b})\Phi(E_{1,b'})^* = 0$  for  $a \neq a'$  and  $b \neq b'$ , and hence the sets of partial isometries  $\{U_a\}_{a=1}^n, \{V_b\}_{b=1}^n$  have mutually orthogonal ranges.

Next, we claim that for all  $1 \leq a, b \leq n$  it holds that  $\Phi(E_{a,b}) = U_a\Phi(E_{1,1})V_b^*$ . In the previous claim this fact is established when at least one of  $a$  and  $b$  is 1, so we may assume that both  $a, b \geq 2$ . In this case, Claim 3 implies that

$$\Phi(E_{1,1})^*\Phi(E_{1,b}) = \Phi(E_{a,1})^*\Phi(E_{a,b}), \quad (35)$$

and so

$$\Phi(E_{1,1})^*\Phi(E_{1,1})V_b^* = \Phi(E_{1,1})^*U_a^*\Phi(E_{a,b}). \quad (36)$$

As  $\text{ran}(U_a^*) = \text{ran}(\Phi(E_{1,1}))$  we may cancel the  $\Phi(E_{1,1})^*$  from the left-side of the above equation to get that  $\Phi(E_{1,1})V_b^* = U_a^*\Phi(E_{a,b})$  (alternatively, we may multiply on the left by the pseudo-inverse of  $\Phi(E_{1,1})^*$ ). Finally, we have  $\text{ran}(U_a) = \text{ran}(E_{a,b})$ , as  $\Phi(E_{a,b})^*\Phi(E_{a,b}) = \Phi(E_{a,1})^*\Phi(E_{a,1})$ , and so

$$\Phi(E_{a,b}) = U_aU_a^*\Phi(E_{a,b}) = U_a\Phi(E_{1,1})V_b^*, \quad (37)$$

as required.

The last step is to show that the structure we have just deduced for  $\Phi$  is the same as that in statement 7. Let  $\Phi(E_{1,1}) = \sum_{i=1}^r s_i x_i y_i^*$  be a singular value decomposition. Define  $\sigma = \sum_{i=1}^r s_i E_{i,i} \in M_r$ , which is clearly positive, and define matrices  $U, V : \mathbb{C}^n \otimes \mathbb{C}^r \rightarrow \mathbb{C}^m$  to act as

$$U(e_a \otimes e_i) = U_a x_i, \text{ and } V(e_b \otimes e_j) = V_b y_j. \quad (38)$$

We may verify that these are in fact isometries:

$$\langle U(e_b \otimes e_j), U(e_a \otimes e_i) \rangle = \langle U_b x_j, U_a x_i \rangle = \delta_{a,b} \langle x_j, x_i \rangle = \delta_{a,b} \delta_{i,j}, \quad (39)$$

where we have used that  $U_a$  and  $U_b$  have orthogonal ranges for  $a \neq b$ . Hence,  $U$  is an isometry as it sends an orthonormal basis to an orthonormal set. The same proof shows that  $V$  is an isometry. Finally, we have that

$$\Phi(E_{a,b}) = U_a \Phi(E_{1,1}) V_b^* = \sum_{i=1}^r s_i U_a x_i y_i^* V_b^* = \sum_{i=1}^r s_i U(E_{a,b} \otimes E_{i,i}) V^* = U(E_{a,b} \otimes \sigma) V^*. \quad (40)$$

Hence,  $\Phi$  has the desired form, and the last thing we need is that  $\text{Tr}(\sigma) = 1$ . The final assumption is that there exists  $X \in M_n \setminus \{0\}$  with  $\|\Phi(X)\|_1 = \|X\|_1$ . This gives

$$\|X\|_1 = \|\Phi(X)\|_1 = \|U(X \otimes \sigma) V^*\|_1 = \|X\|_1 \text{Tr}(\sigma), \quad (41)$$

and hence  $\text{Tr}(\sigma) = 1$  as desired.  $\square$

**Remark 6.** Consider an additional special case of Theorem 3 when  $\Phi$  is Hermiticity preserving. As in the proof of the case when  $\Phi$  is positive, there exists a positive integer  $r \leq m/n$ , a Hermitian  $H \in M_r$ , and an isometry  $U : \mathbb{C}^n \otimes \mathbb{C}^r \rightarrow \mathbb{C}^m$  for which  $\Phi(X) = U(X \otimes H)U^*$  for all  $X \in M_n$ . If  $m < 2n$ , then necessarily  $r = 1$  and hence  $H = \pm 1$ . It follows that either  $\Phi$  or  $-\Phi$  is a reversible quantum channel. If  $m \geq 2n$ , then by considering the Hahn decomposition of  $H$ , one may verify that this form is equivalent to the statement that there exists reversible quantum channels  $\Phi_0, \Phi_1 : M_n \rightarrow M_m$  with orthogonal ranges and a number  $r \in [0, 1]$  for which

$$\Phi = r\Phi_0 - (1-r)\Phi_1. \quad (42)$$

## 4 Characterization of linear maps whose multiplicity maps have maximal norm

We now prove the main result. As mentioned in the introduction, the inequality in Equation (43) below is known in more generality in  $C^*$ -algebras [3, Exercise 3.10].

**Theorem 7.** *Let  $\Phi : M_n \rightarrow M_m$  be linear with  $\|\Phi\|_1 = 1$ . It holds that*

$$\|\Phi \otimes \text{id}_k\|_1 \leq k, \quad (43)$$

with equality if and only if  $n, m \geq k$ , and for any pair of unit vectors  $u, v \in \mathbb{C}^n \otimes \mathbb{C}^k$  satisfying

$$\|(\Phi \otimes \text{id}_k)(uv^*)\|_1 = k \quad (44)$$

(of which at least one such pair must exist), the following statements hold:

1.  $u$  and  $v$  are maximally entangled; i.e. they decompose as

$$u = \sqrt{\frac{1}{k}} \sum_{a=1}^k u_a \otimes e_a \text{ and } v = \sqrt{\frac{1}{k}} \sum_{b=1}^k v_b \otimes e_b \quad (45)$$

for orthonormal sets  $\{u_a\}_{a=1}^k, \{v_b\}_{b=1}^k \subset \mathbb{C}^n$ .

2. Defining isometries  $U, V : \mathbb{C}^k \rightarrow \mathbb{C}^n$  as

$$U = \sum_{a=1}^k u_a e_a^* \text{ and } V = \sum_{b=1}^k v_b e_b^*, \quad (46)$$

there exists a complete trace-norm isometry  $\Psi : T_n(UM_kV^*) \rightarrow M_m$ , where

$$T_n(UM_kV^*) = \{(UXV^*)^\top : X \in M_k\}, \quad (47)$$

for which  $\Phi(X) = \Psi(X^\top)$  for all  $X \in UM_kV^*$ .

*Proof.* Letting  $u, v \in \mathbb{C}^n \otimes \mathbb{C}^k$  be unit vectors, we will first show that

$$\|(\Phi \otimes \text{id}_k)(uv^*)\|_1 \leq k, \quad (48)$$

which will prove Equation (43). We may assume without loss of generality that  $u$  and  $v$  have decompositions of the form

$$u = \sum_{a=1}^r \alpha_a u_a \otimes e_a, \text{ and } v = \sum_{b=1}^r \beta_b v_b \otimes e_b, \quad (49)$$

for  $r \leq \min(k, n)$ , unit vectors  $\alpha, \beta \in \mathbb{C}^r$  with non-negative entries, and orthonormal sets  $\{u_a\}_{a=1}^r, \{v_b\}_{b=1}^r \subset \mathbb{C}^n$ . We have

$$\|(\Phi \otimes \text{id}_k)(uv^*)\|_1 = \left\| \sum_{a,b=1}^r \alpha_a \beta_b \Phi(u_a v_b^*) \otimes E_{a,b} \right\|_1 \quad (50)$$

$$\leq \sum_{a,b=1}^r \alpha_a \beta_b \|\Phi(u_a v_b^*)\|_1 \quad (51)$$

$$\leq \sum_{a,b=1}^r \alpha_a \beta_b \|u_a v_b^*\|_1 \quad (52)$$

$$= \sum_{a,b=1}^r \alpha_a \beta_b \quad (53)$$

$$= \langle 1_r, \alpha \rangle \langle 1_r, \beta \rangle \quad (54)$$

$$\leq \|1_r\|^2 \|\alpha\| \|\beta\| \quad (55)$$

$$= r \quad (56)$$

$$\leq k \quad (57)$$

where  $1_r \in \mathbb{C}^r$  is the vector of all ones. Hence, it holds that  $\|\Phi \otimes \text{id}_k\|_1 \leq k$ .

We now examine equality conditions. Suppose that  $\|(\Phi \otimes \text{id}_k)(uv^*)\|_1 = k$  for unit vectors  $u, v \in \mathbb{C}^n \otimes \mathbb{C}^k$  with decompositions as in Equation (49). First, we may conclude that  $r = k$ , and hence  $k \leq n$ . Furthermore, equality in the application of Cauchy-Schwarz in Equation (55) implies that  $\alpha = \beta = \sqrt{\frac{1}{k}} 1_k$ , and so  $u$  and  $v$  are maximally entangled.

Thus, defining the isometries  $U, V : \mathbb{C}^k \rightarrow \mathbb{C}^n$  as in Equation (46), it holds that

$$\left\| \sum_{a,b=1}^k \Phi(U E_{a,b} V^*) \otimes E_{a,b} \right\|_1 = k^2, \quad (58)$$

and this is equivalent to the more general fact that

$$\left\| \sum_{a,b=1}^k \Phi(x_a y_b^*) \otimes E_{a,b} \right\|_1 = k^2, \quad (59)$$

for any orthonormal bases  $\{x_a\}_{a=1}^k \subset \text{ran}(U)$  and  $\{y_b\}_{b=1}^k \subset \text{ran}(V)$ . As  $\|\Phi\|_1 = 1$ , the above implies that  $\|\Phi(x_a y_b^*)\|_1 = 1$  for all  $1 \leq a, b \leq k$ . By looking at  $2 \times 2$  block-submatrices, it also implies that, for any unit vectors  $x_1, x_2 \in \text{ran}(U)$  and  $y_1, y_2 \in \text{ran}(V)$  with  $\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle = 0$ , it holds that

$$\left\| \begin{pmatrix} \Phi(x_1 y_1^*) & \Phi(x_1 y_2^*) \\ \Phi(x_2 y_1^*) & \Phi(x_2 y_2^*) \end{pmatrix} \right\|_1 = 4. \quad (60)$$

As each block has trace-norm 1, the above  $2 \times 2$  block matrix has trace-norm equal to the sum of the trace-norms of the blocks. Proposition 4 then implies the relations

$$\Phi(x_1 y_1^*)^* \Phi(x_1 y_2^*) = \Phi(x_1 y_1^*) \Phi(x_2 y_1^*)^* = 0 \quad (61)$$

for any  $x_1, x_2 \in \text{ran}(U)$  and  $y_1, y_2 \in \text{ran}(V)$  with  $\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle = 0$ .

This may be written in a more suggestive way: for  $A, B \in UM_k V^*$  rank-1, the following implications hold:

- (i)  $A^* B = 0$  and  $A^* A = B^* B \implies \Phi(A) \Phi(B)^* = 0$ , and
- (ii)  $AB^* = 0$  and  $AA^* = BB^* \implies \Phi(A)^* \Phi(B) = 0$ .

These implications are very similar to statement 5 in Theorem 3, but the adjoints appear in different locations. We may remedy this by defining  $\Psi : T_n(UM_k V^*) \rightarrow M_m$  as  $\Psi = \Phi T_n$ , where  $T_n$  is the transpose. We claim that, for  $A, B \in T_n(UM_k V^*)$  rank-1, the following implications hold:

- (a)  $A^* B = 0$  and  $A^* A = B^* B \implies \Psi(A)^* \Psi(B) = 0$ , and
- (b)  $AB^* = 0$  and  $AA^* = BB^* \implies \Psi(A) \Psi(B)^* = 0$ .

We will prove that (ii)  $\implies$  (a), with (i)  $\implies$  (b) being similar. Let  $A^\top, B^\top \in T_n(UM_k V^*)$  be rank-1. The statements  $(A^\top)^* B^\top = 0$  and  $(A^\top)^* A^\top = (B^\top)^* B^\top$  are equivalent to  $AB^* = 0$  and  $AA^* = BB^*$ , so (ii) implies that  $\Phi(A)^* \Phi(B) = 0$ , which is in turn equivalent to  $\Psi(A^\top)^* \Psi(B^\top) = 0$ .

Thus, by Theorem 3,  $\Psi = \Phi T_n$  is a complete trace-norm isometry on  $T_n(UM_k V^*)$ , as required.<sup>3</sup>  $\square$

As a corollary to Theorems 3 and 7, we provide two characterizations of the set of linear maps  $\Phi : M_n \rightarrow M_m$  satisfying  $\|\Phi\|_1 = n \|\Phi\|_1$ .

**Corollary 8.** *Let  $\Phi : M_n \rightarrow M_m$  be linear with  $m \geq n$ . The following are equivalent.*

1.  $\|\Phi\|_1 = 1$  and  $\|\Phi\|_1 = n$ .
2.  $\|J(\Phi)\|_1 = n^2$  and  $\|J(\Phi T_n)\|_1 = n$ .
3. There exists a complete trace-norm isometry  $\Psi : M_n \rightarrow M_m$  for which  $\Phi = \Psi T_n$ .

*In the above, if  $\Phi$  is Hermiticity preserving so is  $\Psi$ , and if  $\Phi$  is positive then so is  $\Psi$  (and hence is a reversible quantum channel).*

*Proof.* It is immediate that 3  $\implies$  1 and 3  $\implies$  2. That 1  $\implies$  3 is given by Theorem 7, and that 2  $\implies$  3 is given by Theorem 3. For the special cases, since  $\Psi = \Phi T_n$ , if  $\Phi$  is Hermiticity preserving so is  $\Psi$ , as it is a composition of Hermiticity preserving maps. The same logic applies if  $\Phi$  is positive; with  $\Psi$  being a reversible quantum channel following from the positive case of Theorem 3.  $\square$

<sup>3</sup>Note that Theorem 3 as stated only applies to maps whose domain is all of  $M_n$ . Here, the domain of  $\Psi$  is  $T_n(UM_k V^*) = \overline{V} M_k U^\top \subset M_n$ , so technically we are applying Theorem 3 to conclude that the linear map  $X \mapsto \Psi(V^\top X \overline{U})$  is a complete trace-norm isometry on  $M_k$ . However, this is equivalent to  $\Psi$  being a complete trace-norm isometry on  $T_n(UM_k V^*)$ .

## 5 A uniqueness result for the Werner-Holevo channels in single-shot quantum channel discrimination

A fundamental operational task in quantum information is to determine which quantum channel, from a set of possible channels, is acting on a system. The simplest version of this task is *single-shot quantum channel discrimination*, where the goal is to determine which of two channels is acting on a system given only a single use. Various aspects of this task have been extensively studied (see e.g. [11, 18–25]). For completeness, we give a description of the task below. Proofs of all facts summarized may be found in [9, Chapter 3].

Single-shot quantum channel discrimination may be formulated as a single-player game specified by a triple  $(\lambda, \Gamma_0, \Gamma_1)$ , where  $\lambda \in [0, 1]$  and  $\Gamma_0, \Gamma_1 : M_n \rightarrow M_m$  are quantum channels. In the game, the player knows a description of the triple  $(\lambda, \Gamma_0, \Gamma_1)$ , and the game proceeds as follows:

1. The referee samples a bit  $\alpha \in \{0, 1\}$  with probability  $p(0) = \lambda$ ,  $p(1) = 1 - \lambda$ .
2. The player is given a single use of the channel  $\Gamma_\alpha$ ; i.e. the player gives a quantum state on the input system of their choice to the referee, who then returns the output of  $\Gamma_\alpha$ .
3. The player must guess  $\alpha$  (after say, making a measurement on the output).

The goal of the player is to maximize the probability that they guess  $\alpha$  correctly.

Ultimately, all the player can do is prepare an input state to  $\Gamma_\alpha$  then try to discriminate the two possible outputs. In the most unconstrained version of the game, the player is free to use an auxiliary system; i.e. they can prepare a bipartite quantum state  $\rho \in M_n \otimes M_k$  then discriminate the outputs  $(\Gamma_\alpha \otimes \text{id}_k)(\rho)$ . Due to the Holevo-Helstrom theorem for single-shot quantum state discrimination [26, 27], the optimal probability of success given a choice of state  $\rho \in M_n \otimes M_k$  is

$$\frac{1}{2} + \frac{1}{2} \|\lambda(\Gamma_0 \otimes \text{id}_k)(\rho) - (1 - \lambda)(\Gamma_1 \otimes \text{id}_k)(\rho)\|_1. \quad (62)$$

Thus, for a fixed auxiliary system of dimension  $k$ , the optimal success probability of winning the game is given by the optimization of the above expression over density matrices, which reduces to

$$\frac{1}{2} + \frac{1}{2} \|\lambda\Gamma_0 \otimes \text{id}_k - (1 - \lambda)\Gamma_1 \otimes \text{id}_k\|_{1,H}, \quad (63)$$

where, for  $\Psi : M_n \rightarrow M_m$ ,

$$\|\Psi\|_{1,H} = \max\{\|\Psi(H)\|_1 : H \in M_n, \|H\|_1 = 1, H = H^*\}. \quad (64)$$

Hence, the optimal value over unconstrained strategies, which amounts to optimizing Equation (63) over  $k \geq 1$ , is given by

$$\frac{1}{2} + \frac{1}{2} \|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1. \quad (65)$$

A natural question to ask in this setting is: What channel discrimination games (with system input size  $n$ ) have the maximum possible gap between the optimal performance with and without entanglement? By Equations (63) and (65), this amounts to characterizing the games  $(\lambda, \Gamma_0, \Gamma_1)$ , where  $\Gamma_0, \Gamma_1 : M_n \rightarrow M_m$ , with maximal gap between the norms

$$\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_{1,H} \quad \text{and} \quad \|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1. \quad (66)$$

In this section we make partial progress towards answering this question. We apply the results of the previous section to characterize the games (with input space  $M_n$ ) that have maximal gap between the norms  $\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1$  and  $\|\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|\|_1$ . As it generically holds that

$$0 \leq \|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1 \leq \|\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|\|_1 \leq 1, \quad (67)$$

and  $\|\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|\|_1 \leq n\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1$ , the maximum possible gap occurs when

$$1 = \|\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|\|_1 = n\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1. \quad (68)$$

Operationally, the above relations say that the game can be won with certainty using arbitrary entanglement, but is hard to win without entanglement, with the upper bound on unentangled performance given by  $\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1$  being as small as possible given that the game can be won with certainty.

As detailed in [9, Example 3.36], the Werner-Holevo channels [28] provide a well-known family of channel discrimination games satisfying Equation (68). For  $n \geq 2$ , we denote them as  $\Phi_n^{(0)}, \Phi_n^{(1)} : M_n \rightarrow M_n$ , and they are defined to act as

$$\Phi_n^{(0)}(X) = \frac{1}{n+1}(\text{Tr}(X)\mathbb{1}_n + X^\top), \text{ and } \Phi_n^{(1)}(X) = \frac{1}{n-1}(\text{Tr}(X)\mathbb{1}_n - X^\top) \quad (69)$$

for all  $X \in M_n$ . For the probability  $\lambda_n = \frac{n+1}{2n}$ , it holds that

$$\lambda_n\Phi_n^{(0)} - (1 - \lambda_n)\Phi_n^{(1)} = \frac{1}{n}T_n, \quad (70)$$

and as such

$$1 = \|\|\lambda_n\Phi_n^{(0)} - (1 - \lambda_n)\Phi_n^{(1)}\|\|_1 = n\|\lambda_n\Phi_n^{(0)} - (1 - \lambda_n)\Phi_n^{(1)}\|_1. \quad (71)$$

Thus, for  $n \geq 2$  the triple  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$  is an example of a channel discrimination game satisfying Equation (68).<sup>4</sup> We now apply the result of the previous section to show that the game specified by the triple  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$  is in some sense the unique game (with channels having domain  $M_n$ ) satisfying Equation (68).

**Theorem 9.** *Let  $m \geq n$ ,  $\Gamma_0, \Gamma_1 : M_n \rightarrow M_m$  be quantum channels,  $\lambda \in (0, 1)$  be a probability, and let  $\Phi_n^{(0)}, \Phi_n^{(1)} : M_n \rightarrow M_n$  be the Werner-Holevo channels as given in Equation (69). It holds that*

$$1 = \|\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|\|_1 = n\|\lambda\Gamma_0 - (1 - \lambda)\Gamma_1\|_1 \quad (72)$$

if and only if:

- For  $m < 2n$ , there exists a reversible quantum channel  $\Psi : M_n \rightarrow M_m$  for which either  $(\lambda, \Gamma_0, \Gamma_1) = (\lambda_n, \Psi\Phi_n^{(0)}, \Psi\Phi_n^{(1)})$ , or  $(\lambda, \Gamma_0, \Gamma_1) = (1 - \lambda_n, \Psi\Phi_n^{(1)}, \Psi\Phi_n^{(0)})$ .
- For  $m \geq 2n$ , there exists  $r \in [0, 1]$  and two reversible channels  $\Psi_0, \Psi_1 : M_n \rightarrow M_m$  with orthogonal ranges for which  $\lambda = r\lambda_n + (1 - r)(1 - \lambda_n)$ , and

$$\lambda\Gamma_0 = r\lambda_n\Psi_0\Phi_n^{(0)} + (1 - r)(1 - \lambda_n)\Psi_1\Phi_n^{(1)}, \quad (73)$$

and

$$(1 - \lambda)\Gamma_1 = r(1 - \lambda_n)\Psi_0\Phi_n^{(1)} + (1 - r)\lambda_n\Psi_1\Phi_n^{(0)}. \quad (74)$$

<sup>4</sup>While the Werner-Holevo channels were originally introduced in [28] for other reasons, in the setting of quantum channel discrimination, they may be intuitively viewed as a way of smuggling the transpose into the problem, with the properties of the resulting game being inherited from norm properties of the transpose.

**Remark 10.** Theorem 9 may be interpreted as saying that the game  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$  uniquely satisfies Equation (72) in the following sense: Any game  $(\lambda, \Gamma_0, \Gamma_1)$ , whose channels have domain  $M_n$  and satisfy Equation (72), is constructed out of, and is reducible by the player to, the game  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$  in a way that perfectly preserves success probabilities. Indeed, mathematically, one can check that

$$\|\lambda(\Gamma_0 \otimes \text{id}_k)(X) - (1 - \lambda)(\Gamma_1 \otimes \text{id}_k)(X)\|_1 \quad (75)$$

$$= \|\lambda_n(\Phi_n^{(0)} \otimes \text{id}_k)(X) - (1 - \lambda_n)(\Phi_n^{(1)} \otimes \text{id}_k)(X)\|_1 \quad (76)$$

for all integers  $k \geq 1$  and matrices  $X \in M_n \otimes M_k$ . Operationally, the construction/reduction of such games  $(\lambda, \Gamma_0, \Gamma_1)$  in terms of  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$  goes as follows.

- For the case  $m < 2n$ , the construction and reduction are natural; up to a reversible quantum channel (which the player can undo) and a relabeling of the channels (which the player knows), the game  $(\lambda, \Gamma_0, \Gamma_1)$  is exactly the game  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$ .
- For the case  $m \geq 2n$ , the relation between  $(\lambda, \Gamma_0, \Gamma_1)$  and  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$  is less clear, though it can be thought of as a convex combination of relabelings of the game  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$ , where the player is able to detect which labeling is being used. Specifically, with probability  $r$ ,  $\Gamma_0$  acts as  $\Phi_n^{(0)}$  and  $\Gamma_1$  acts as  $\Phi_n^{(1)}$ , and with probability  $(1 - r)$  the labels are reversed. As  $\Psi_0$  and  $\Psi_1$  have orthogonal ranges, the player is able to measure which labelling is being used without disturbance. Once this is done, the situation from the players perspective is now the same as in the case  $m < 2n$ , and they may act accordingly.

Before proving Theorem 9, we prove a lemma regarding the uniqueness of certain decompositions of Hermiticity preserving maps into differences of completely positive maps.

**Lemma 11.** *Let  $\Phi : M_n \rightarrow M_m$  be Hermiticity preserving,  $\Psi_0, \Psi_1 : M_n \rightarrow M_m$  be completely positive and satisfy*

$$\Phi = \Psi_0 - \Psi_1 \text{ and } \|\Phi\|_1 = \|\Psi_0\|_1 + \|\Psi_1\|_1, \quad (77)$$

and let  $u \in \mathbb{C}^n \otimes \mathbb{C}^n$  be a unit vector satisfying  $\|\Phi\|_1 = \|(\Phi \otimes \text{id}_n)(uu^*)\|_1$ . It follows that

$$\|\Psi_0\|_1 = \|(\Psi_0 \otimes \text{id}_n)(uu^*)\|_1 \text{ and } \|\Psi_1\|_1 = \|(\Psi_1 \otimes \text{id}_n)(uu^*)\|_1, \quad (78)$$

and for any other completely positive maps  $\Psi'_0, \Psi'_1 : M_n \rightarrow M_m$  satisfying the conditions in Equation (77),

$$(\Psi'_0 \otimes \text{id}_n)(uu^*) = (\Psi_0 \otimes \text{id}_n)(uu^*) \text{ and } (\Psi'_1 \otimes \text{id}_n)(uu^*) = (\Psi_1 \otimes \text{id}_n)(uu^*). \quad (79)$$

Hence, if such a  $u$  exists with full Schmidt-rank, the completely positive maps  $\Psi_0, \Psi_1$  satisfying Equation (77) are unique (if they exist).

*Proof.* We have

$$\|\Phi\|_1 = \|(\Phi \otimes \text{id}_n)(uu^*)\|_1 \quad (80)$$

$$= \|(\Psi_0 \otimes \text{id}_n)(uu^*) - (\Psi_1 \otimes \text{id}_n)(uu^*)\|_1 \quad (81)$$

$$\leq \|(\Psi_0 \otimes \text{id}_n)(uu^*)\|_1 + \|(\Psi_1 \otimes \text{id}_n)(uu^*)\|_1 \quad (82)$$

$$\leq \|\Psi_0\|_1 + \|\Psi_1\|_1 \quad (83)$$

$$= \|\Phi\|_1. \quad (84)$$

Hence, all inequalities are equalities, and therefore  $\|\Psi_0\|_1 = \|(\Psi_0 \otimes \text{id}_n)(uu^*)\|_1$  and  $\|\Psi_1\|_1 = \|(\Psi_1 \otimes \text{id}_n)(uu^*)\|_1$ .

Next, as  $\Psi_0$  and  $\Psi_1$  are completely positive, it holds that  $(\Psi_0 \otimes \text{id}_n)(uu^*) \geq 0$  and  $(\Psi_1 \otimes \text{id}_n)(uu^*) \geq 0$ , and so equality in Equation (82) implies that

$$(\Phi \otimes \text{id}_n)(uu^*) = (\Psi_0 \otimes \text{id}_n)(uu^*) - (\Psi_1 \otimes \text{id}_n)(uu^*) \quad (85)$$

is the Hahn decomposition of  $(\Phi \otimes \text{id}_n)(uu^*)$ .<sup>5</sup> Thus, for any other completely positive maps  $\Psi'_0, \Psi'_1 : M_n \rightarrow M_m$  satisfying the hypotheses,

$$(\Phi \otimes \text{id}_n)(uu^*) = (\Psi'_0 \otimes \text{id}_n)(uu^*) - (\Psi'_1 \otimes \text{id}_n)(uu^*) \quad (86)$$

is also the Hahn decomposition of  $(\Phi \otimes \text{id}_n)(uu^*)$ . Equation (79) therefore follows by the uniqueness of the Hahn decomposition.

Finally, if  $u \in \mathbb{C}^n \otimes \mathbb{C}^n$  has full Schmidt-rank, then a linear map  $\Gamma : M_n \rightarrow M_m$  is uniquely specified by the matrix  $(\Gamma \otimes \text{id}_n)(uu^*)$ , and so Equation (79) implies the uniqueness of the pair  $\Psi_0$  and  $\Psi_1$  (assuming such a pair exists).  $\square$

*Proof of Theorem 9.* In both cases the ‘‘if’’ part is a matter of verifying Equation (76), where the case  $m \geq 2n$  requires use of the fact that  $\Psi_0$  and  $\Psi_1$  have orthogonal ranges.

Thus, assume we have a channel discrimination triple  $(\lambda, \Gamma_0, \Gamma_1)$  satisfying Equation (72). By Corollary 8, the norm relation implies

$$\lambda\Gamma_0 - (1 - \lambda)\Gamma_1 = \frac{1}{n}\Psi T_n, \quad (87)$$

for  $\Psi : M_n \rightarrow M_m$  a Hermiticity preserving complete trace-norm isometry. Remark 6 gives the following structure for  $\Psi$ :

- If  $m < 2n$ , either  $\Psi$  or  $-\Psi$  is a reversible quantum channel.
- If  $m \geq 2n$ , there exists  $r \in [0, 1]$  and  $\Psi_0, \Psi_1 : M_n \rightarrow M_m$  reversible quantum channels with orthogonal ranges for which  $\Psi = r\Psi_0 - (1 - r)\Psi_1$ .

In what follows we will work with the form of  $\Psi$  in the case  $m \geq 2n$ , as the case  $m < 2n$  can be subsumed by the case  $r = 0$  or  $r = 1$  when  $m \geq 2n$ , even though it is not possible for two reversible channels  $\Psi_0, \Psi_1 : M_n \rightarrow M_m$  to have orthogonal ranges when  $m < 2n$ .

Observe the following facts:

- $\frac{1}{n}\Psi T_n$  is Hermiticity preserving and decomposes as a difference of CP maps as given in Equation (87),
- $\|\frac{1}{n}\Psi T_n\|_1 = 1 = \|\lambda\Gamma_0\|_1 + \|(1 - \lambda)\Gamma_1\|_1$ , and
- $\|\frac{1}{n}\Psi T_n\|_1 = \|\frac{1}{n}(\Psi T_n \otimes \text{id}_n)(\tau_n)\|_1$ , where  $\tau_n = \frac{1}{n} \sum_{a,b=1}^n E_{a,b} \otimes E_{a,b} \in M_n \otimes M_n$  is the canonical maximally entangled state.

When taken together these facts imply, by Lemma 11, that Equation (87) is the *unique* decomposition of  $\frac{1}{n}\Psi T_n$  into a difference of CP maps with the above properties. In the remainder of the proof, we will exhibit a (seemingly) different decomposition of  $\frac{1}{n}\Psi T_n$ , verify that it also satisfies the assumptions of Lemma 11, then conclude that the two decompositions are necessarily the same.

<sup>5</sup>The Hahn decomposition of a Hermitian matrix  $H \in M_n$  is the unique decomposition of  $H$  as a difference  $H = P - Q$  with  $P, Q \geq 0$  and  $PQ = 0$ . For  $H$  Hermitian and  $P, Q \geq 0$ , it holds that  $H = P - Q$  is the Hahn decomposition of  $H$  if and only if  $\|H\|_1 = \|P\|_1 + \|Q\|_1$ .



Note that  $\frac{1}{n}T_n = \lambda_n \Phi_0^{(n)} - (1 - \lambda_n) \Phi_1^{(n)}$ , and hence

$$\frac{1}{n} \Psi T_n = (r \Psi_0 - (1 - r) \Psi_1) (\lambda_n \Phi_0^{(n)} - (1 - \lambda_n) \Phi_1^{(n)}) \quad (88)$$

$$= [r \lambda_n \Psi_0 \Phi_0^{(n)} + (1 - r)(1 - \lambda_n) \Psi_1 \Phi_1^{(n)}] - [(1 - r) \lambda_n \Psi_1 \Phi_0^{(n)} + r(1 - \lambda_n) \Psi_0 \Phi_1^{(n)}]. \quad (89)$$

The maps in the square brackets are completely positive, and satisfy

$$\left\| r \lambda_n \Psi_0 \Phi_0^{(n)} + (1 - r)(1 - \lambda_n) \Psi_1 \Phi_1^{(n)} \right\|_1 + \left\| (1 - r) \lambda_n \Psi_1 \Phi_0^{(n)} + r(1 - \lambda_n) \Psi_0 \Phi_1^{(n)} \right\|_1 \quad (90)$$

$$= r \lambda_n + (1 - r)(1 - \lambda_n) + (1 - r) \lambda_n + r(1 - \lambda_n) = 1. \quad (91)$$

Hence, by the uniqueness clause of Lemma 11, Equations (73) and (74) hold.

When  $m < 2n$ , either  $r = 0$  or  $r = 1$ , in which case either

$$(\lambda, \Gamma_0, \Gamma_1) = (\lambda_n, \Psi_0 \Phi_n^{(0)}, \Psi_0 \Phi_n^{(1)}), \text{ or } (\lambda, \Gamma_0, \Gamma_1) = (1 - \lambda_n, \Psi_1 \Phi_n^{(1)}, \Psi_1 \Phi_n^{(0)}), \quad (92)$$

as required.  $\square$

## 6 Discussion

The canonical example of a linear map  $\Phi : M_n \rightarrow M_m$  satisfying  $\|\Phi\|_1 = 1$  and

$$\|\Phi \otimes \text{id}_k\|_1 = k \quad (93)$$

is the matrix transpose, and we have proven that, up to an equivalence, the transpose is the *unique* map satisfying the above equation. We have applied this result in the setting of single-shot quantum channel discrimination to prove that a channel discrimination game  $(\lambda, \Gamma_0, \Gamma_1)$  (with input dimension  $n$ ) satisfies the norm relation

$$1 = \|\lambda \Gamma_0 - (1 - \lambda) \Gamma_1\|_1 = n \|\lambda \Gamma_0 - (1 - \lambda) \Gamma_1\|_1 \quad (94)$$

if and only if it is in some sense equivalent to the game  $(\lambda_n, \Phi_n^{(0)}, \Phi_n^{(1)})$ , where  $\Phi_n^{(0)}, \Phi_n^{(1)}$  are the Werner-Holevo channels, and  $\lambda_n = \frac{n+1}{2n}$ .

The uniqueness result for the Werner-Holevo channel discrimination game is almost, but not quite, a characterization of channel discrimination games with maximal gap between the optimal performance of entangled and unentangled strategies. Characterizing such games requires an understanding of the maximal gap between  $\|\Phi\|_{1,H}$  and  $\|\Phi\|_1$  for Hermiticity preserving linear maps  $\Phi : M_n \rightarrow M_m$ . For example, is it true that  $\|\Phi\|_1 \leq n \|\Phi\|_{1,H}$ ? More generally, is it true that

$$\|\Phi \otimes \text{id}_k\|_{1,H} \leq k \|\Phi\|_{1,H} \quad (95)$$

It is not so clear if the proof of the inequality in Theorem 7 can be adapted to this situation. It seems reasonable to conjecture that some inequality of the above form holds, and that the transpose will uniquely saturate the inequality.

Another natural question is whether the characterization of linear maps  $\Phi : M_n \rightarrow M_m$  for which  $\|\Phi\|_1 = 1$  and  $\|\Phi \otimes \text{id}_k\|_1 = k$  holds approximately. E.g. if  $\|\Phi\|_1 = 1$  and  $\|\Phi\|_1 \geq n - \epsilon$ , then is  $\Phi$  necessarily close in some sense to the transpose (followed by a complete trace-norm isometry)?

## Acknowledgements

We thank John Watrous, Vern Paulsen, and Chi-Kwong Li for helpful discussions and comments. This work was supported by NSERC, the Ontario Graduate Scholarship, and the Queen Elizabeth II Graduate Scholarship in Science and Technology.

## A Duality of the operator norm and trace-norm

Let  $\|\cdot\|$  denote the operator norm for matrices, as well as the induced operator norm for linear maps of matrices, i.e. for linear  $\Phi : M_n \rightarrow M_m$ ,

$$\|\Phi\| = \max\{\|\Phi(X)\| : X \in M_n, \|X\| = 1\}. \quad (96)$$

For  $A, B \in M_n$ , we denote the Hilbert-Schmidt inner product as  $\langle A, B \rangle = \text{Tr}(A^*B)$ , and for a linear map  $\Phi : M_n \rightarrow M_m$ , we use  $\Phi^*$  to denote the adjoint of  $\Phi$  with respect to this inner-product. That is,  $\Phi^* : M_m \rightarrow M_n$  is the unique linear map satisfying

$$\langle A, \Phi(B) \rangle = \langle \Phi^*(A), B \rangle \quad (97)$$

for all  $A \in M_m$  and  $B \in M_n$ .

For our purposes, the “duality” of the trace-norm and operator norm may be summarized by the following: For any matrix  $A \in M_n$ , it holds that

$$\|A\|_1 = \max\{|\langle X, A \rangle| : X \in M_n, \|X\| \leq 1\}, \quad (98)$$

and

$$\|A\| = \max\{|\langle X, A \rangle| : X \in M_n, \|X\|_1 \leq 1\}. \quad (99)$$

A direct implication of these expressions is that, for any linear  $\Phi : M_n \rightarrow M_m$ , it holds that

$$\|\Phi\|_1 = \|\Phi^*\| \text{ and } \|\Phi\| = \|\Phi^*\|_1. \quad (100)$$

The above relations enable interconversion of facts about the trace-norm and facts about the operator norm. For example, the statement

$$\|\Phi \otimes \text{id}_k\|_1 \leq k\|\Phi\|_1 \text{ for all linear maps } \Phi : M_n \rightarrow M_m \quad (101)$$

is equivalent to the statement

$$\|\Phi \otimes \text{id}_k\| \leq k\|\Phi\| \text{ for all linear } \Phi : M_n \rightarrow M_m. \quad (102)$$

This is why [3, Exercise 3.10], which directly generalizes the statement in Equation (102) to arbitrary linear maps between unital  $C^*$ -algebras, is referenced in the introduction as a generalization of the statement in Equation (101). Similarly, our main result characterizing the linear maps  $\Phi : M_n \rightarrow M_m$  for which  $\|\Phi \otimes \text{id}_k\|_1 = k\|\Phi\|_1$ , may also be translated into a characterization of such maps for which  $\|\Phi \otimes \text{id}_k\| = k\|\Phi\|$ .

## References

- [1] R. Smith. Completely Bounded Maps between  $C^*$ -Algebras. *Journal of the London Mathematical Society*, s2-27(1):157–166, 1983. DOI: [10.1112/jlms/s2-27.1.157](https://doi.org/10.1112/jlms/s2-27.1.157).
- [2] J. Tomiyama. Recent Development of the Theory of Completely Bounded Maps between  $C^*$ -Algebras. *Publications of the Research Institute for Mathematical Sciences*, 19(3):1283–1303, 1983. DOI: [10.2977/prims/1195182030](https://doi.org/10.2977/prims/1195182030).

- [3] V. Paulsen. *Completely Bounded Maps and Operator Algebras*. Cambridge University Press, Cambridge, 2003. DOI: [10.1017/CBO9780511546631](https://doi.org/10.1017/CBO9780511546631).
- [4] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1):1–8, 1996. DOI: [10.1016/S0375-9601\(96\)00706-2](https://doi.org/10.1016/S0375-9601(96)00706-2).
- [5] G. Vidal and R. F. Werner. Computable measure of entanglement. *Physical Review A*, 65(3):032314, 2002. DOI: [10.1103/PhysRevA.65.032314](https://doi.org/10.1103/PhysRevA.65.032314).
- [6] J. Tomiyama. On the transpose map of matrix algebras. *Proceedings of the American Mathematical Society*, 88(4):635–638, 1983. DOI: [10.1090/S0002-9939-1983-0702290-4](https://doi.org/10.1090/S0002-9939-1983-0702290-4).
- [7] M.-D. Choi. A Schwarz inequality for positive linear maps on  $C^*$ -algebras. *Illinois Journal of Mathematics*, 18(4):565–574, 1974. ISSN 0019-2082. URL <https://projecteuclid.org/euclid.ijm/1256051007>.
- [8] C.-K. Li, Y.-T. Poon, and N.-S. Sze. Isometries for Ky Fan Norms between Matrix Spaces. *Proceedings of the American Mathematical Society*, 133(2):369–377, 2005. DOI: [10.1090/S0002-9939-04-07510-0](https://doi.org/10.1090/S0002-9939-04-07510-0).
- [9] J. Watrous. The Theory of Quantum Information. <https://cs.uwaterloo.ca/~watrous/TQI>, 2017.
- [10] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975. DOI: [10.1016/0024-3795\(75\)90075-0](https://doi.org/10.1016/0024-3795(75)90075-0).
- [11] D. Puzzuoli and J. Watrous. Ancilla Dimension in Quantum Channel Discrimination. *Annales Henri Poincaré*, 18(4):1153–1184, 2017. DOI: [10.1007/s00023-016-0537-y](https://doi.org/10.1007/s00023-016-0537-y).
- [12] A. Jenčová. Reversibility conditions for quantum operations. *Reviews in Mathematical Physics*, 24(07):1250016, 2012. DOI: [10.1142/S0129055X1250016X](https://doi.org/10.1142/S0129055X1250016X).
- [13] D. Sutter, M. Berta, and M. Tomamichel. Multivariate Trace Inequalities. *Communications in Mathematical Physics*, 352(1):37–58, 2017. DOI: [10.1007/s00220-016-2778-5](https://doi.org/10.1007/s00220-016-2778-5).
- [14] R. Kadison. Isometries of Operator Algebras. *Annals of Mathematics*, 54(2):325–338, 1951. DOI: [10.2307/1969534](https://doi.org/10.2307/1969534).
- [15] W.-S. Cheung, C.-K. Li, and Y.-T. Poon. Isometries between matrix algebras. *Journal of the Australian Mathematical Society*, 77(1):1–16, 2004. DOI: [10.1017/S1446788700010119](https://doi.org/10.1017/S1446788700010119).
- [16] C.-K. Li and S. Pierce. Linear Preserver Problems. *The American Mathematical Monthly*, 108(7):591–605, 2001. DOI: [10.2307/2695268](https://doi.org/10.2307/2695268).
- [17] J.-T. Chan, C.-K. Li, and N.-S. Sze. Isometries for unitarily invariant norms. *Linear Algebra and its Applications*, 399:53–70, 2005. DOI: [10.1016/j.laa.2004.05.017](https://doi.org/10.1016/j.laa.2004.05.017).
- [18] A. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997. DOI: [10.1070/RM1997v052n06ABEH002155](https://doi.org/10.1070/RM1997v052n06ABEH002155).
- [19] A. Kitaev, A. Shen, and M. Vyalı. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002. DOI: [10.1090/gsm/047](https://doi.org/10.1090/gsm/047).
- [20] M. Sacchi. Optimal discrimination of quantum operations. *Physical Review A*, 71(6):062340, 2005. DOI: [10.1103/PhysRevA.71.062340](https://doi.org/10.1103/PhysRevA.71.062340).
- [21] M. Sacchi. Entanglement can enhance the distinguishability of entanglement-breaking channels. *Physical Review A*, 72(1):014305, 2005. DOI: [10.1103/PhysRevA.72.014305](https://doi.org/10.1103/PhysRevA.72.014305).
- [22] B. Rosgen. Distinguishing short quantum computations. In *Proceedings of the 25th International Symposium on Theoretical Aspects of Computer Science*, pages 597–608, 2008. DOI: [10.4230/LIPIcs.STACS.2008.1322](https://doi.org/10.4230/LIPIcs.STACS.2008.1322).

- [23] J. Watrous. Distinguishing quantum operations having few Kraus operators. *Quantum Information and Computation*, 8(9):819–833, 2008. ISSN 1533-7146. URL <http://www.rintonpress.com/journals/qiconline.html#v8n89>.
- [24] M. Piani and J. Watrous. All Entangled States are Useful for Channel Discrimination. *Physical Review Letters*, 102(25):250501, 2009. DOI: [10.1103/PhysRevLett.102.250501](https://doi.org/10.1103/PhysRevLett.102.250501).
- [25] A. Jenčová and M. Plávala. Conditions for optimal input states for discrimination of quantum channels. *Journal of Mathematical Physics*, 57(12):122203, 2016. DOI: [10.1063/1.4972286](https://doi.org/10.1063/1.4972286).
- [26] C. Helstrom. Detection theory and quantum mechanics. *Information and Control*, 10(3):254–291, 1967. DOI: [10.1016/S0019-9958\(67\)90302-6](https://doi.org/10.1016/S0019-9958(67)90302-6).
- [27] A. Holevo. An analog of the theory of statistical decisions in noncommutative probability theory. *Transactions of the Moscow Mathematical Society*, 26:133–149, 1972. ISSN 0077-1554. URL <https://zbmath.org/?q=an:0289.62007>.
- [28] R. F. Werner and A. S. Holevo. Counterexample to an additivity conjecture for output purity of quantum channels. *Journal of Mathematical Physics*, 43(9):4353–4357, 2002. DOI: [10.1063/1.1498491](https://doi.org/10.1063/1.1498491).