Distinguishing quantum operations having few Kraus operators

John Watrous

Institute for Quantum Computing and School of Computer Science
University of Waterloo, Waterloo, Ontario, Canada.

April 18, 2008

Abstract

Entanglement is sometimes helpful in distinguishing between quantum operations, as differences between quantum operations can become magnified when their inputs are entangled with auxiliary systems. Bounds on the dimension of the auxiliary system needed to optimally distinguish quantum operations are known in several situations. For instance, the dimension of the auxiliary space never needs to exceed the dimension of the input space [Smi83, Kit97] of the operations for optimal distinguishability, while no auxiliary system whatsoever is needed to optimally distinguish unitary operations [AKN98, CPR00]. Another bound, which follows from work of R. Timoney [Tim03], is that optimal distinguishability is always possible when the dimension of the auxiliary system is twice the number of operators needed to express the difference between the quantum operations in Kraus form. This paper provides an alternate proof of this fact that is based on concepts and tools that are familiar to quantum information theorists.

1 Introduction

The notion of entanglement is pervasive in the theory of quantum information, often playing a critically important and yet sometimes subtle role in different settings. One such setting concerns the distinguishability of quantum operations, which has been considered in various forms by several authors [Ací01, AKN98, CPR00, DPP01, GLN05, Kit97, KSW06, RW05, Sac05b, Sac05a].

Consider a situation in which two quantum operations Φ_0 and Φ_1 are fixed. A single evaluation of one of the two operations is given, and the goal is to determine which of the two operations it is. This type of problem will be considered in greater generality momentarily, but for the moment assume that Φ_0 and Φ_1 are single-qubit operations. Also assume that a bit $a \in \{0,1\}$, chosen uniformly at random, determines which of the two operations is given, so that it is meaningful to consider the optimal probability with which the given operation is correctly identified.

A natural approach to an instance of this problem is to optimally choose a single-qubit input state ρ so that the output states $\Phi_0(\rho)$ and $\Phi_1(\rho)$ are as far apart as possible (with respect to the trace norm, for instance). Then, some optimal measurement can be applied to the output state $\Phi_a(\rho)$ to obtain information about the bit a.

This, however, is not the most general approach, and is not always optimal. More generally, one may prepare a possibly *entangled* state between the input to the operation and some auxiliary system, and then apply the operation Φ_a to the input system. A multiple-qubit measurement may then be applied to the output and auxiliary systems together to obtain information about a. Indeed

this more general approach can give an improvement in the probability of correctly identifying the bit a in some cases.

For example, consider an instance of the above problem in which Φ_0 is the identity operation, while Φ_1 corresponds to the application of a randomly chosen non-identity Pauli operator:

$$\Phi_1(\rho) = \frac{1}{3}\sigma_x\rho\sigma_x + \frac{1}{3}\sigma_y\rho\sigma_y + \frac{1}{3}\sigma_z\rho\sigma_z.$$

These two quantum operations can be distinguished without error using an entangled input state as follows: any one of the four Bell states is chosen, Φ_a is applied to one of a pair of qubits in this state, and the two qubits are measured with respect to the Bell basis. In case $a = 0$, the result of the measurement obviously agrees with the initially chosen Bell state, while in case $a = 1$, the result of the measurement will correspond to one of the three remaining Bell states, never resulting in the initially chosen state. In this way, the index a can be identified without error, and so Φ_0 and Φ_1 can be distinguished perfectly. Perfect distinguishability of Φ_0 and Φ_1 is, however, not possible with a strategy that does not entangle the input to the operations with an auxiliary system: the optimal probability of correctly guessing a with such a strategy can be shown to be $5/6$.

A related example is discussed later in Section 3 that illustrates that a striking gap can exist between the entangled and non-entangled approaches to this problem. (It is nearly the same as an example that was discussed in [KSW06].) In particular, quantum operations acting on large systems can sometimes be distinguished perfectly using entanglement with an auxiliary system, and yet act nearly identically on inputs not entangled with an auxiliary system. A similar phenomenon arises in the context of approximate randomization of quantum states [HLSW04].

It is, however, not always the case that entanglement with an auxiliary system helps in this problem. While it is easy to construct trivial examples of this sort, there is an interesting general class of examples known: if Φ_0 and Φ_1 are arbitrary *unitary* operations, then optimal distinguishability is possible without an auxiliary system [AKN98, CPR00]. The same fact holds more generally when Φ_0 and Φ_1 are given by $\Phi_0(X) = AXA^*$ and $\Phi_1(X) = BXB^*$ for linear isometries A and B.

In light of these examples, it is natural to ask how large an auxiliary system is needed for optimal distinguishability between various classes of quantum operations. In general, it is known that optimal distinguishability never requires an auxiliary system that is larger than the input space of the operations [Smi83, Kit97], while the example to be discussed in Section 3 shows that the probability to distinguish operations can sometimes shrink with even a small decrease in the size of the auxiliary system from this upper bound.

This paper focuses on a lesser-known (and incomparable) bound: for quantum operations Φ_0 and Φ_1, it is sufficient for optimal distinguishability that the dimension of the auxiliary system is twice the number of Kraus operators needed to express the difference between Φ_0 and Φ_1, which is at most twice the total number of Kraus operators needed to express Φ_0 and Φ_1.

Note that this bound is independent of the size of the systems the quantum operations act upon, and may be viewed as a generalization of the above-mentioned fact that unitary operations require no auxiliary systems for optimal distinguishability. That particular fact, however, is not quite recovered, for the bound obtained only establishes that at most two auxiliary qubits are required in this particular case rather than zero. The bound is also clearly not interesting in the case where the difference between the quantum operations to be distinguished requires a number of Kraus operators that exceeds the dimension of the input space of the operations. Nevertheless, the results hold generally for all quantum operations, and may potentially be of use in understanding quantum operations with few Kraus operators. Recent work on quantum expanders [BATS07,

BASTS07, GE07, Har07, Has07a, Has07b] provides a setting where quantum operations with few Kraus operators are of interest for some applications.

The above bound follows from a theorem of Timoney [Tim03], whose proof is based on the notion of the Haagerup estimate on the norm of complete boundedness for a class of super-operators on C^*-algebras. This paper provides a different proof based on notions that are familiar in the theory of quantum information. In particular, the well-known *fidelity* function plays a central and simplifying role in the proof. One of the technical parts of the proof, based on a theorem of Barvinok [Bar02], may also be of independent use in quantum information theory: every non-zero output of a positive super-operator, ranging over all density operator inputs, must have a low-rank preimage.

The remainder of the paper is organized as follows. Section 2 reviews background material needed for the paper, including a discussion of super-operator representations and distinguishability. Section 3 gives an example of quantum operations that require a large auxiliary system to be distinguished optimally. The actual bound discussed above on the size of the auxiliary space needed for optimal distinguishability of quantum operations is proved in Section 4.

2 Background

2.1 Basic linear algebra

In this paper the term *complex Euclidean space* refers to any finite dimensional inner product space over the complex numbers $\mathbb{C}$, and we assume that every such space has a fixed orthonormal *standard basis*. For the remainder of this section, let $\mathcal{X}$ and $\mathcal{Y}$ be arbitrary complex Euclidean spaces, and let $\{|a\rangle \,:\, a \in \Sigma\}$ denote the standard basis of $\mathcal{X}$, with Σ being some arbitrary finite, non-empty set.

The space of (linear) operators mapping $\mathcal{X}$ to $\mathcal{Y}$ is denoted $\mathrm{L}(\mathcal{X}, \mathcal{Y})$, while $\mathrm{L}(\mathcal{X})$ is shorthand for $\mathrm{L}(\mathcal{X}, \mathcal{X})$. The adjoint (or Hermitian transpose) of $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is denoted A^*, and the identity element of $\mathrm{L}(\mathcal{X})$ is denoted $\mathbb{1}_{\mathcal{X}}$. If $\mathcal{V}$ is a subspace of $\mathcal{X}$, we let $\Pi_{\mathcal{V}} \in \mathrm{L}(\mathcal{X})$ denote the orthogonal projection onto $\mathcal{V}$. We write $\mathrm{Herm}(\mathcal{X})$ to refer to the set of Hermitian operators on $\mathcal{X}$, $\mathrm{Pos}(\mathcal{X})$ to refer to the set of positive semidefinite operators on $\mathcal{X}$, and $\mathrm{D}(\mathcal{X})$ to refer to the set of density operators on $\mathcal{X}$. The notation $A \geq 0$ also means that A is positive semidefinite, and more generally $A \geq B$ means that $A - B$ is positive semidefinite.

The *spectral norm* of an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is defined as

$$\|A\| = \max\{\|Au\| \,:\, u \in \mathrm{S}(\mathcal{X})\}$$

where $\mathrm{S}(\mathcal{X}) = \{u \in \mathcal{X} \,:\, \|u\| = 1\}$ denotes the unit sphere in $\mathcal{X}$. The *trace norm* of an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is defined as

$$\|A\|_1 = \mathrm{Tr}\sqrt{A^*A}.$$

Equivalently, $\|A\|_1$ is the sum of the singular values of A.

The *fidelity* between positive semidefinite operators $P, Q \in \mathrm{Pos}(\mathcal{X})$ is defined as

$$\mathrm{F}(P, Q) = \left\| \sqrt{P}\sqrt{Q} \right\|_1 = \mathrm{Tr}\sqrt{\sqrt{Q}P\sqrt{Q}}.$$

This function has also been called the *tracial geometric mean* in work of Timoney [Tim07] that is subsequent to the paper [Tim03] that is most closely related to this one.

2.2 Linear super-operators and representations

A linear mapping of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ is a *super-operator*, and the space of all such mappings is denoted $\mathrm{T}(\mathcal{X}, \mathcal{Y})$. As expected, the notation $\mathrm{T}(\mathcal{X})$ is shorthand for $\mathrm{T}(\mathcal{X}, \mathcal{X})$, and $\mathbb{1}_{\mathrm{L}(\mathcal{X})} \in \mathrm{T}(\mathcal{X})$ denotes the identity super-operator.

A super-operator $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is *positive* if $\Phi(P) \in \mathrm{Pos}(\mathcal{Y})$ for every $P \in \mathrm{Pos}(\mathcal{X})$, and is *completely positive* if $\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}$ is positive for every complex Euclidean space $\mathcal{Z}$. Super-operators that are both completely positive and trace-preserving will be called *admissible* super-operators. Such super-operators represents valid *quantum operations* from a system with associated space $\mathcal{X}$ to one with associated space $\mathcal{Y}$.

With respect to the standard basis of $\mathcal{X}$, the *Choi-Jamiołkowski representation* of a super-operator $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is defined as

$$J(\Phi) = \sum_{a,b \in \Sigma} \Phi(|a\rangle\langle b|) \otimes |a\rangle\langle b|.$$

The resulting mapping $J : \mathrm{T}(\mathcal{X}, \mathcal{Y}) \to \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$ is a linear bijection. It is the case that Φ is completely positive if and only if $J(\Phi)$ is positive semidefinite.

Every super-operator $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ can be expressed as

$$\Phi(X) = \sum_{j=1}^{k} A_j X B_j^*$$

for some choice of an integer $k \geq 1$ and operators $A_1, \ldots, A_k, B_1, \ldots, B_k \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$. This expression is called a *Kraus representation* of Φ and the operators $A_1, \ldots, A_k$ and $B_1, \ldots, B_k$ are referred to as *Kraus operators*. The minimal value of k for which such an expression exists is $k = \mathrm{rank}(J(\Phi))$. In case Φ is completely positive one may take $A_j = B_j$ for all $j = 1, \ldots, k$.

Finally, every super-operator $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ can be expressed as

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(AXB^*)$$

for some choice of a complex Euclidean space $\mathcal{Z}$ and operators $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$. In particular, such a representation exists provided that $\dim(\mathcal{Z}) \geq \mathrm{rank}(J(\Phi))$. When Φ is completely positive one may take $A = B$, and such an expression is called a *Stinespring representation* of Φ.

2.3 Distinguishability of quantum operations

The trace distance between quantum states directly relates to their distinguishability. This relation can be simply expressed by referring to the following abstract problem.

Problem 1 (*Distinguishing quantum states*)**.** Quantum states $\rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})$ are fixed, and a bit $a \in \{0, 1\}$ is chosen uniformly at random. The goal is to guess the value of a with probability as large as possible by means of a measurement of a single copy of ρ_a.

The optimal probability to correctly guess a is precisely

$$\frac{1}{2} + \frac{1}{4} \left\| \rho_0 - \rho_1 \right\|_1.$$

Indeed, any measurement performed on ρ_0 and ρ_1 will result in probability mass functions p_0 and p_1 for which $\left\| p_0 - p_1 \right\|_1 \leq \left\| \rho_0 - \rho_1 \right\|_1$, and moreover equality is achieved by a two-outcome (projective) measurement.

As briefly discussed in the introduction, we may consider a similar problem for quantum operations rather than states.

Problem 2 (*Distinguishing quantum operations).* Quantum operations $\Phi_0, \Phi_1 \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ are fixed, and a bit $a \in \{0,1\}$ is chosen uniformly at random. The goal is to guess the value of a with probability as large as possible by means of a process involving just a single evaluation of the operation Φ_a.

The super-operator norm that is most relevant to this problem is sometimes known as the *diamond norm*. It is defined as follows.

Definition 3. Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces. For every $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, we define the *super-operator trace norm* of Φ as

$$\|\Phi\|_1 \stackrel{\text{def}}{=} \max\{\|\Phi(X)\|_1 : X \in \mathrm{L}(\mathcal{X}),\ \|X\|_1 \leq 1\},$$

and we define the *diamond norm* of Φ as

$$\|\Phi\|_\diamond \stackrel{\text{def}}{=} \left\|\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})}\right\|_1.$$

Let us note that for a given super-operator $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, we have

$$\|\Phi\|_1 = \max\{\|\Phi(uv^*)\|_1 : u, v \in \mathrm{S}(\mathcal{X})\}$$

and therefore

$$\|\Phi\|_\diamond = \max\left\{\left\|(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(uv^*)\right\|_1 : u, v \in \mathrm{S}(\mathcal{X} \otimes \mathcal{X})\right\}.$$

It holds that

$$\|\Phi\|_\diamond = \left\|\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}\right\|_1$$

for any choice of $\mathcal{Z}$ whose dimension is at least that of $\mathcal{X}$.

The diamond norm, first used in the setting of quantum information by Kitaev [Kit97], has precisely the same relationship to the problem of distinguishing quantum operations as the trace norm has to distinguishing quantum states. Specifically, the quantity $\|\Phi_0 - \Phi_1\|_\diamond$ represents the maximal ℓ_1-distance between two probability distributions resulting from *interactive measurements* of the operations Φ_0 and Φ_1, where an interactive measurement refers to the process of preparing a state, evaluating a quantum operation on part of that state, and measuring the result. In particular, the optimal probability to correctly guess the value of the bit a in the problem above is

$$\frac{1}{2} + \frac{1}{4}\|\Phi_0 - \Phi_1\|_\diamond.$$

Roughly speaking, the inclusion of the tensor factor $\mathbb{1}_{\mathrm{L}(\mathcal{X})}$ in the definition of the diamond norm accounts for the use of an auxiliary space in a process that attempts to distinguish between super-operators. It should be appreciated, however, that the diamond norm happens to be very robust and possesses nice properties that also contribute to its use for this application.

The diamond norm is closely related to the *norm of complete boundedness*, which plays an important role in operator theory [Pau02] and is sometimes referenced in quantum information theory. Specifically, it holds that $\|\Phi\|_\diamond = \|\Phi^*\|_{\mathrm{cb}}$ for any super-operator $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, where $\Phi^* \in \mathrm{T}(\mathcal{Y}, \mathcal{X})$ denotes the adjoint super-operator to Φ. It must be kept in mind, however, that the norm of complete boundedness (as it is most commonly defined) gives an appropriate way to measure distance between quantum operations in the so-called *Heisenberg picture* formulation of quantum information and not in the more common *Schrödinger picture* formulation; for it is the quantity $\|\Phi_0 - \Phi_1\|_\diamond = \|\Phi_0^* - \Phi_1^*\|_{\mathrm{cb}}$ and not $\|\Phi_0 - \Phi_1\|_{\mathrm{cb}}$ that directly relates to the distinguishability of Φ_0 and Φ_1 in the sense discussed above.

3 An illustrative example

A simple example was presented in the introduction illustrating the use of entanglement to distinguish admissible super-operators. In that example, the use of an entangled input allows perfect distinguishability of two quantum operations that can be distinguished correctly with probability at most $5/6$ without the use of entangled inputs. In this section we present a class of examples that show a more striking difference between strategies that entangle inputs with an auxiliary system and those that do not. A similar example appears in [KSW06].

Let $\mathcal{X}$ be a complex Euclidean space and let $n = \dim(\mathcal{X})$. Define admissible super-operators $\Phi_0, \Phi_1 \in \mathrm{T}(\mathcal{X})$ as follows:

$$\Phi_0(X) = \frac{1}{n+1}\left((\operatorname{Tr} X)\mathbb{1}_{\mathcal{X}} + X^{\mathsf{T}}\right),$$

$$\Phi_1(X) = \frac{1}{n-1}\left((\operatorname{Tr} X)\mathbb{1}_{\mathcal{X}} - X^{\mathsf{T}}\right).$$

Here, X^{T} denotes transposition with respect to the standard basis of $\mathcal{X}$. It is clear from the definitions that both Φ_0 and Φ_1 are trace-preserving, while complete positivity follows from a calculation of the Choi-Jamiołkowski representations of these super-operators:

$$J(\Phi_0) = \frac{2}{n+1}\Pi_{\mathcal{X}\circledcirc\mathcal{X}} \quad \text{and} \quad J(\Phi_1) = \frac{2}{n-1}\Pi_{\mathcal{X}\circledcirc\mathcal{X}},$$

where $\mathcal{X} \circledcirc \mathcal{X}$ and $\mathcal{X} \circledcirc \mathcal{X}$ are the symmetric and antisymmetric subspaces of $\mathcal{X} \otimes \mathcal{X}$, respectively.

These two operations can be distinguished perfectly, provided that a sufficiently large auxiliary quantum system is used. To see this, consider these operations applied to half of the maximally entangled state

$$\xi = \frac{1}{n}\sum_{a,b\in\Sigma} |a\rangle\langle b| \otimes |a\rangle\langle b| \in \mathrm{D}(\mathcal{X}\otimes\mathcal{X}).$$

We have

$$(\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\xi) = \frac{2}{n(n+1)}\Pi_{\mathcal{X}\circledcirc\mathcal{X}} \quad \text{and} \quad (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\xi) = \frac{2}{n(n-1)}\Pi_{\mathcal{X}\circledcirc\mathcal{X}}.$$

As $\mathcal{X} \circledcirc \mathcal{X}$ and $\mathcal{X} \circledcirc \mathcal{X}$ are orthogonal, it holds that

$$\left\| (\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\xi) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\xi) \right\|_1 = 2.$$

This implies that the density operators $(\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\xi)$ and $(\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\xi)$, and therefore the super-operators Φ_0 and Φ_1, can be distinguished without error.

Now suppose $\mathcal{W}_k$ represents an auxiliary space of dimension k, where $1 \leq k \leq n$. It is clear by convexity that the quantity

$$\left\| (\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)})(\rho) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)})(\rho) \right\|_1$$

is maximized for $\rho = uu^*$, where $u \in \mathcal{X} \otimes \mathcal{W}_k$ is a unit vector. Fix such a vector u, and write

$$u = \sum_{j=1}^{k} \sqrt{p_j}\, x_j \otimes w_j$$

for $\{x_1, \ldots, x_k\} \subset \mathcal{X}$ and $\{w_1, \ldots, w_k\} \subset \mathcal{W}_k$ orthonormal sets and $p_1, \ldots, p_k \geq 0$. Noting that

$$\begin{aligned}
&(\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)})(uu^*) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)})(uu^*) \\
&\qquad = \frac{2}{n^2 - 1} \sum_{j=1}^{k} p_j \left(n \overline{x_j} x_j^{\mathsf{T}} - \mathbb{1}_{\mathcal{X}} \right) \otimes w_j w_j^* + \frac{2n}{n^2 - 1} \sum_{i \neq j} \sqrt{p_i p_j}\, \overline{x_j} x_i^{\mathsf{T}} \otimes w_i w_j^*
\end{aligned}$$

provides a simple upper bound:

$$\left\| (\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)})(uu^*) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)})(uu^*) \right\|_1 \leq \frac{4}{n+1} + \frac{2n}{n^2 - 1}(k-1).$$

This inequality is obviously not tight for some values of k; but it nevertheless shows that any significant decrease in the size of the auxiliary space results in a significant error in distinguishing these super-operators. In particular, by taking $k = 1$ we see that the quantum operations Φ_0 and Φ_1 act nearly identically on input states that are not entangled with an auxiliary system.

4 The main result

This section contains a proof of the bound discussed in the introduction. A formal statement of this result is given in the following theorem.

Theorem 4. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $\Phi_0, \Phi_1 \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be admissible super-operators, and let $k = \operatorname{rank}(J(\Phi_0 - \Phi_1))$. Then for any complex Euclidean space $\mathcal{W}$ with $\dim(\mathcal{W}) \geq 2k$ there exists a unit vector $u \in \mathcal{X} \otimes \mathcal{W}$ such that*

$$\left\| (\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W})})(uu^*) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W})})(uu^*) \right\|_1 = \| \Phi_0 - \Phi_1 \|_\diamond .$$

Before proceeding to the proof of this theorem, let us briefly discuss its interpretation in terms of the super-operator distinguishability problem.

We suppose that we are given admissible super-operators Φ_0 and Φ_1 mapping $\mathrm{L}(\mathcal{X})$ to $\mathrm{L}(\mathcal{Y})$, and that these super-operators are to be distinguished in the sense of the abstract problem discussed previously. Let $k = \operatorname{rank}(J(\Phi_0 - \Phi_1))$, which is at most the sum of the number of Kraus operators needed to express Φ_0 and Φ_1.

We know that the optimal probability to distinguish the super-operators, by which we mean the optimal probability to correctly identify Φ_a for $a \in \{0, 1\}$ chosen uniformly, is

$$\frac{1}{2} + \frac{1}{4} \| \Phi_0 - \Phi_1 \|_\diamond .$$

The theorem implies it is possible to achieve this probability of success by preparing some pure state $u \in \mathcal{X} \otimes \mathcal{W}$ for $\mathcal{W}$ corresponding to an auxiliary system of dimension at most $2k$, applying Φ_a to this state, and measuring the result. This is because an optimally chosen measurement correctly distinguishes between the states $(\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W})})(uu^*)$ and $(\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W})})(uu^*)$ with probability

$$\frac{1}{2} + \frac{1}{4} \left\| (\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W})})(uu^*) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W})})(uu^*) \right\|_1 = \frac{1}{2} + \frac{1}{4} \| \Phi_0 - \Phi_1 \|_\diamond .$$

The proof of Theorem 4 is split into three subsections. The first subsection establishes a fact about the rank of an input density operator to a positive super-operator required to yield a given output. The second subsection relates the super-operator trace norm and diamond norm to the maximum output fidelity of completely positive super-operators. Finally, the third subsection combines these facts to prove the main theorem.

4.1 A theorem on the minimum rank of a preimage

Let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be a positive super-operator. Define

$$\mathrm{Out}(\Phi) \stackrel{\text{def}}{=} \{\Phi(\rho) \,:\, \rho \in \mathrm{D}(\mathcal{X})\}$$

to be the set of all outputs of Φ ranging over all density operator inputs, and for a given operator $P \in \mathrm{Out}(\Phi)$ let us consider the set

$$\{\rho \in \mathrm{D}(\mathcal{X}) \,:\, \Phi(\rho) = P\}. \tag{1}$$

In this section we prove that this set must include at least one density operator ρ that satisfies $\mathrm{rank}(\rho) \leq \mathrm{rank}(P)$, provided that $P \neq 0$. (We really only need this fact for completely positive Φ, but the proof goes through for all positive Φ.)

The basic idea of the proof is as follows. We observe that the above set (1) is a nonempty, compact, and convex, and therefore has at least one extreme point. Assuming that P is nonzero, it may be argued that any such extreme point must have rank at most that of P. The proof below is based on the proof of Proposition 13.1 in Chapter II of Barvinok [Bar02], with some minor refinements possible given the particular assumptions at hand.

Theorem 5. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be a positive super-operator. Then for every choice of $P \in \mathrm{Out}(\Phi)$ with $P \neq 0$ there exists a density operator $\rho \in \mathrm{D}(\mathcal{X})$ such that*

1. *$\Phi(\rho) = P$, and*
2. *$\mathrm{rank}(\rho) \leq \mathrm{rank}(P)$.*

Proof. Let $n = \dim(\mathcal{X})$, $m = \dim(\mathcal{Y})$, and $k = \mathrm{rank}(P)$. Using a spectral decomposition of P we may write

$$P = \sum_{i=1}^{k} y_i y_i^*$$

for some orthogonal collection $\{y_1, \ldots, y_k\} \subset \mathcal{Y}$. Define $\mathcal{U} = \mathrm{span}\{y_1, \ldots, y_k\}$.

Next, viewing spaces of Hermitian operators as real vector spaces, we define a real linear mapping

$$\Psi : \mathrm{Herm}(\mathcal{X}) \to \mathrm{Herm}(\mathcal{U}) \oplus \mathbb{R}$$

as follows. For each $X \in \mathrm{Herm}(\mathcal{X})$ we define $\Psi(X) = (Y, \lambda)$, for

$$\begin{aligned} Y &= \Pi_{\mathcal{U}} \Phi(X) \Pi_{\mathcal{U}}, \\ \lambda &= \mathrm{Tr}\left[(\mathbb{1}_{\mathcal{X}} - \Pi_{\mathcal{U}})\, \Phi(X)\right]. \end{aligned}$$

Given that $\mathrm{Herm}(\mathcal{U}) \oplus \mathbb{R}$ is a (k^2+1)-dimensional real vector space, it holds that

$$\ker(\Psi) = \{X \in \mathrm{Herm}(\mathcal{X}) \,:\, \Psi(X) = (0,0)\}$$

is a subspace of $\mathrm{Herm}(\mathcal{X})$ having dimension at least $n^2 - \left(k^2+1\right)$.

For every choice of $\rho \in \mathrm{D}(\mathcal{X})$ it holds that $\Phi(\rho) = P$ if and only if $\Psi(\rho) = (P, 0)$, and therefore

$$\{\rho \in \mathrm{D}(\mathcal{X}) \,:\, \Phi(\rho) = P\} = \{\rho \in \mathrm{D}(\mathcal{X}) \,:\, \Psi(\rho) = (P,0)\}.$$

This set is non-empty, compact, and convex, and we may therefore choose an extreme point ρ from this set. To complete the proof, it suffices to prove that $r = \mathrm{rank}(\rho) \leq k$.

Using a spectral decomposition of ρ we may write

$$\rho = \sum_{i=1}^{r} p_i x_i x_i^*$$

for $p_1, \ldots, p_r > 0$ and $\{x_1, \ldots, x_r\}$ orthogonal unit vectors in $\mathcal{X}$. Let $\mathcal{V} = \operatorname{span}\{x_1, \ldots, x_r\}$ and let $\mathcal{A} \subseteq \operatorname{Herm}(\mathcal{X})$ be the subspace defined as

$$\mathcal{A} = \{X \in \operatorname{Herm}(\mathcal{X}) : \operatorname{im}(X) \subseteq \mathcal{V},\ \operatorname{Tr}(X) = 0\}.$$

Equivalently, $\mathcal{A}$ is the subspace containing all traceless Hermitian operators of the form

$$X = \sum_{1 \leq i,j \leq r} \alpha_{i,j} x_i x_j^*.$$

Observe that $\dim(\mathcal{A}) = r^2 - 1$ (again, as a real vector space).

Consider the intersection of the subspaces $\ker(\Psi)$ and $\mathcal{A}$, and suppose $X \in \ker(\Psi) \cap \mathcal{A}$ is any element of this intersection. Our goal will be to prove that $X = 0$, and therefore that the intersection $\ker(\Psi) \cap \mathcal{A}$ is trivial. To this end, assume toward contradiction that $X \neq 0$. As X is Hermitian and $\operatorname{im}(X) \subseteq \mathcal{V}$, we have that

$$\pm X \leq \|X\| \, \Pi_{\mathcal{V}}.$$

Given that $\delta \Pi_{\mathcal{V}} \leq \rho$ for $\delta = \min(p_1, \ldots, p_r) > 0$, it follows that $\pm \varepsilon X \leq \rho$ for $\varepsilon = \delta / \|X\|$. Because X is traceless, this implies that $\rho \pm \varepsilon X \in \mathrm{D}(\mathcal{X})$. Finally, given that $X \in \ker(\Psi)$, we have $\Psi(\rho \pm \varepsilon X) = (P, 0)$, which is equivalent to $\Phi(\rho \pm \varepsilon X) = P$.

At this point we have proved that

$$\Phi(\rho - \varepsilon X) = \Phi(\rho) = \Phi(\rho + \varepsilon X),$$

and we have that ρ, $\rho - \varepsilon X$ and $\rho + \varepsilon X$ are distinct density operators. Given that

$$\rho = \frac{1}{2}(\rho - \varepsilon X) + \frac{1}{2}(\rho + \varepsilon X)$$

and that ρ was chosen to be an extreme point in the set $\{\rho \in \mathrm{D}(\mathcal{X}) : \Phi(\rho) = P\}$, we have arrived at a contradiction. It is therefore established that the subspaces $\ker(\Psi)$ and $\mathcal{A}$ have a trivial intersection.

Now, given that $\ker(\Psi)$ and $\mathcal{A}$ are subspaces of $\operatorname{Herm}(\mathcal{X})$ with

$$\begin{aligned} \dim(\ker(\Psi)) &\geq n^2 - \left(k^2 + 1\right), \\ \dim(\mathcal{A}) &= r^2 - 1, \\ \dim(\ker(\Psi) \cap \mathcal{A}) &= 0, \end{aligned}$$

we have $n^2 - \left(k^2 + 1\right) + \left(r^2 - 1\right) \leq n^2$, and therefore $r^2 \leq k^2 + 2$. As r and k are positive integers, we conclude that $r \leq k$, which completes the proof. □

Remark 6. Note that the assumption $P \neq 0$ is necessary because a density operator cannot have zero rank. It of course follows easily from the positivity of Φ that if $\Phi(\rho) = 0$ for some density operator ρ, then this is so for some ρ having rank 1. This fact also happens to be revealed by the above proof, which really only uses the assumption that $P \neq 0$ at the very end. In particular, if $k = 0$, the inequality $r^2 \leq k^2 + 2$ only implies that $r \leq 1$.

4.2 Distinguishability and maximum output fidelity

We now relate the super-operator trace norm and diamond norm to the fidelity of outputs of completely positive super-operators, maximized over various sets. Let us begin with two definitions.

Definition 7. For every complex Euclidean space $\mathcal{X}$ and integer $k \geq 1$, define

$$\mathrm{D}_k(\mathcal{X}) \stackrel{\text{def}}{=} \{\rho \in \mathrm{D}(\mathcal{X}) \,:\, \mathrm{rank}(\rho) \leq k\}.$$

Definition 8. Suppose $\mathcal{X}$ and $\mathcal{Y}$ are complex Euclidean spaces and $\Psi_1, \Psi_2 \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ are completely positive super-operators. For each $k \geq 1$ define

$$\mathrm{F}_{\max}^{(k)}(\Psi_1, \Psi_2) \stackrel{\text{def}}{=} \max\left\{\mathrm{F}(\Psi_1(\rho_1), \Psi_2(\rho_2)) \,:\, \rho_1, \rho_2 \in \mathrm{D}_k(\mathcal{X})\right\}.$$

We also write $\mathrm{F}_{\max}(\Psi_1, \Psi_2) = \mathrm{F}_{\max}^{(n)}(\Psi_1, \Psi_2)$ for $n = \dim(\mathcal{X})$, which allows for a maximization over all density operators ρ_1 and ρ_2 in the above equation.

We will also require the following lemma, proved in [RW05]. A short proof is included for completeness.

Lemma 9. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $P, Q \in \mathrm{Pos}(\mathcal{X})$. Assume that $u, v \in \mathcal{X} \otimes \mathcal{Y}$ satisfy $\mathrm{Tr}_{\mathcal{Y}}(uu^*) = P$ and $\mathrm{Tr}_{\mathcal{Y}}(vv^*) = Q$. Then $\mathrm{F}(P, Q) = \|\mathrm{Tr}_{\mathcal{X}}(uv^*)\|_1$.*

Proof. For any choice of $Y \in \mathrm{L}(\mathcal{Y})$ we have

$$\|Y\|_1 = \max_U |\mathrm{Tr}(UY)|$$

where the maximization is over all unitary operators $U \in \mathrm{L}(\mathcal{Y})$, and therefore

$$\|\mathrm{Tr}_{\mathcal{X}}(uv^*)\|_1 = \max_U |\mathrm{Tr}\left(U \,\mathrm{Tr}_{\mathcal{X}}(uv^*)\right)| = \max_U |v^*\left(\mathbb{1}_{\mathcal{X}} \otimes U\right)u|.$$

As U ranges over all possible unitary operators on $\mathcal{Y}$, the vector $(\mathbb{1}_{\mathcal{X}} \otimes U)u$ ranges over all purifications of P in $\mathcal{X} \otimes \mathcal{Y}$. The above quantity is therefore equal to $\mathrm{F}(P, Q)$ by Uhlmann's Theorem (q.v. Theorem 9.4 in [NC00]). □

Now, the relation between distinguishability and maximum output fidelity that will established is given by the following theorem (cf. Corollary 2.2 of [Tim07]).

Theorem 10. *Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be complex Euclidean spaces, let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be an arbitrary super-operator, and suppose that $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ satisfy $\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(AXB^*)$ for all $X \in \mathrm{L}(\mathcal{X})$. Define completely positive super-operators $\Psi_A, \Psi_B \in \mathrm{T}(\mathcal{X}, \mathcal{Z})$ as*

$$\Psi_A(X) = \mathrm{Tr}_{\mathcal{Y}}(AXA^*),$$
$$\Psi_B(X) = \mathrm{Tr}_{\mathcal{Y}}(BXB^*),$$

for all $X \in \mathrm{L}(\mathcal{X})$. Then for all $k \geq 1$ it holds that

$$\mathrm{F}_{\max}^{(k)}(\Psi_A, \Psi_B) = \left\|\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)}\right\|_1,$$

where $\mathcal{W}_k$ is any complex Euclidean space with dimension k.

Remark 11. Note that it is the space $\mathcal{Y}$ that is traced-out in the definition of Ψ_A and Ψ_B, rather than the space $\mathcal{Z}$.

Proof. Let us fix $k \geq 1$ and let $\mathcal{W}_k$ be a complex Euclidean space of dimension k. For any choice of $u, v \in \mathcal{X} \otimes \mathcal{W}_k$ we have

$$\begin{aligned}
&\left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)})(uv^*) \right\|_1 \\
&\qquad = \left\| \mathrm{Tr}_{\mathcal{Z}} \left[(A \otimes \mathbb{1}_{\mathcal{W}_k}) uv^* (B^* \otimes \mathbb{1}_{\mathcal{W}_k}) \right] \right\|_1 \\
&\qquad = \mathrm{F}\left(\mathrm{Tr}_{\mathcal{Y} \otimes \mathcal{W}_k} \left((A \otimes \mathbb{1}_{\mathcal{W}_k}) uu^* (A^* \otimes \mathbb{1}_{\mathcal{W}_k}) \right), \mathrm{Tr}_{\mathcal{Y} \otimes \mathcal{W}_k} \left((B \otimes \mathbb{1}_{\mathcal{W}_k}) vv^* (B^* \otimes \mathbb{1}_{\mathcal{W}_k}) \right) \right) \\
&\qquad = \mathrm{F}\left(\Psi_A(\mathrm{Tr}_{\mathcal{W}_k}(uu^*)), \Psi_B(\mathrm{Tr}_{\mathcal{W}_k}(vv^*)) \right),
\end{aligned}$$

where the second equality is by Lemma 9. Given that $\dim(\mathcal{W}_k) = k$, it holds that

$$\left\{ \mathrm{Tr}_{\mathcal{W}_k}(uu^*) \,:\, u \in \mathrm{S}\left(\mathcal{X} \otimes \mathcal{W}_k\right) \right\} = \mathrm{D}_k\left(\mathcal{X}\right).$$

This implies that

$$\begin{aligned}
\left\| \Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)} \right\|_1 &= \max \left\{ \left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)})(uv^*) \right\|_1 \,:\, u, v \in \mathrm{S}\left(\mathcal{X} \otimes \mathcal{W}_k\right) \right\} \\
&= \max \left\{ \mathrm{F}\left(\Psi_A(\rho_A), \Psi_B(\rho_B) \right) \,:\, \rho_A, \rho_B \in \mathrm{D}_k\left(\mathcal{X}\right) \right\} \\
&= \mathrm{F}_{\max}^{(k)}(\Psi_A, \Psi_B)
\end{aligned}$$

as required. □

The following corollary, which corresponds to the case $k = \dim(\mathcal{X})$ in the previous theorem, is of special interest. This fact is implicit in [KW00] and appears (as an exercise) in [KSV02].

Corollary 12. *Suppose that $\Phi \in \mathrm{T}\left(\mathcal{X}, \mathcal{Y}\right)$ and $\Psi_A, \Psi_B \in \mathrm{T}\left(\mathcal{X}, \mathcal{Z}\right)$ are as in Theorem 10. Then*

$$\mathrm{F}_{\max}(\Psi_A, \Psi_B) = \left\| \Phi \right\|_\diamond.$$

4.3 Optimal distinguishability with small auxiliary systems

Now we combine the results of the previous two subsections to bound the size of the auxiliary space needed to optimally distinguish quantum operations. First we prove the following theorem.

Theorem 13. *Let $\Phi \in \mathrm{T}\left(\mathcal{X}, \mathcal{Y}\right)$ be a super-operator, let $k = \mathrm{rank}(J(\Phi))$, and let $\mathcal{W}_k$ be a complex Euclidean space having dimension k. Then*

$$\left\| \Phi \right\|_\diamond = \left\| \Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)} \right\|_1.$$

Proof. As $\mathrm{rank}(J(\Phi)) = k$, we may write $\Phi(X) = \mathrm{Tr}_{\mathcal{W}_k}\left(AXB^*\right)$ for $A, B \in \mathrm{L}\left(\mathcal{X}, \mathcal{Y} \otimes \mathcal{W}_k\right)$. By Corollary 12, $\left\| \Phi \right\|_\diamond = \mathrm{F}_{\max}(\Psi_A, \Psi_B)$ for $\Psi_A, \Psi_B \in \mathrm{T}\left(\mathcal{X}, \mathcal{W}_k\right)$ defined as

$$\begin{aligned}
\Psi_A(X) &= \mathrm{Tr}_{\mathcal{Y}}\left(AXA^*\right), \\
\Psi_B(X) &= \mathrm{Tr}_{\mathcal{Y}}\left(BXB^*\right).
\end{aligned}$$

Let $\rho_A, \rho_B \in \mathrm{D}\left(\mathcal{X}\right)$ be density operators that achieve this maximum fidelity:

$$\mathrm{F}_{\max}(\Psi_A, \Psi_B) = \mathrm{F}(\Psi_A(\rho_A), \Psi_B(\rho_B)).$$

The operators $\Psi_A(\rho_A)$ and $\Psi_B(\rho_B)$ are contained in $\mathrm{Pos}\,(\mathcal{W}_k)$, and therefore have rank at most k. By Theorem 5 there must therefore exist density operators $\xi_A, \xi_B \in \mathrm{D}\,(\mathcal{X})$ having rank at most k such that $\Psi_A(\xi_A) = \Psi_A(\rho_A)$ and $\Psi_B(\xi_B) = \Psi_B(\rho_B)$. Thus

$$\mathrm{F}_{\max}^{(k)}(\Psi_A, \Psi_B) \geq \mathrm{F}(\Psi_A(\xi_A), \Psi_B(\xi_B)) = \mathrm{F}(\Psi_A(\rho_A), \Psi_B(\rho_B)) = \mathrm{F}_{\max}(\Psi_A, \Psi_B).$$

The reverse inequality obviously holds, and so by Theorem 10 and Corollary 12 we have

$$\|\Phi\|_\diamond = \mathrm{F}_{\max}(\Psi_A, \Psi_B) = \mathrm{F}_{\max}^{(k)}(\Psi_A, \Psi_B) = \left\| \Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_k)} \right\|_1$$

as required. □

Before completing the proof Theorem 4, we need one more lemma. It is similar to Lemma 2.4 in [RW05], but is slightly more general. We need this lemma because the value of the super-operator trace norm is not always achieved by a density operator input, even when the super-operator is the difference between admissible super-operators [Wat05].

Lemma 14. *Let $\Phi = \Phi_0 - \Phi_1$ for completely positive super-operators $\Phi_0, \Phi_1 \in \mathrm{T}\,(\mathcal{X}, \mathcal{Y})$, and let $\mathcal{Q}$ be a complex Euclidean space with dimension 2. Then there exists a unit vector $u \in \mathcal{X} \otimes \mathcal{Q}$ such that*

$$\left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Q})})(uu^*) \right\|_1 \geq \|\Phi\|_1 .$$

Proof. Let $X \in \mathrm{L}\,(\mathcal{X})$ be an operator with $\|X\|_1 = 1$ that satisfies $\|\Phi\|_1 = \|\Phi(X)\|_1$, and define

$$Y = \frac{1}{2} X \otimes |0\rangle\langle 1| + \frac{1}{2} X^* \otimes |1\rangle\langle 0| \in \mathrm{Herm}\,(\mathcal{X} \otimes \mathcal{Q}).$$

Here, we assume the standard basis of $\mathcal{Q}$ is $\{|0\rangle, |1\rangle\}$. Then $\|Y\|_1 = \|X\|_1 = 1$ and

$$\begin{aligned}
\left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Q})})(Y) \right\|_1 &= \frac{1}{2} \left\| \Phi(X) \otimes |0\rangle\langle 1| + \Phi(X^*) \otimes |1\rangle\langle 0| \right\|_1 \\
&= \frac{1}{2} \left\| \Phi(X) \otimes |0\rangle\langle 1| + \Phi(X)^* \otimes |1\rangle\langle 0| \right\|_1 \\
&= \|\Phi(X)\|_1 \\
&= \|\Phi\|_1 .
\end{aligned}$$

The second equality follows from the condition that $\Phi = \Phi_0 - \Phi_1$ for Φ_0 and Φ_1 completely positive, which is equivalent to $\Phi(X^*) = \Phi(X)^*$ for all $X \in \mathrm{L}\,(\mathcal{X})$.

Now, because Y is Hermitian, we may consider a spectral decomposition

$$Y = \sum_i \lambda_i u_i u_i^* .$$

By the triangle inequality, it holds that

$$\|\Phi\|_1 = \left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Q})})(Y) \right\|_1 \leq \sum_i |\lambda_i| \left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Q})})(u_i u_i^*) \right\|_1 .$$

As $\|Y\|_1 = 1$, we have $\sum_i |\lambda_i| = 1$, and thus

$$\left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Q})})(u_i u_i^*) \right\|_1 \geq \|\Phi\|_1$$

for some index i. Setting $u = u_i$ for any such choice of i completes the proof. □

Finally we have all of the facts that we require to prove Theorem 4. The proof follows.

Proof of Theorem 4. By Theorem 13 it follows that

$$\|\Phi_0 - \Phi_1\|_\diamond = \left\| \Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{V})} - \Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{V})} \right\|_1$$

for any complex Euclidean space $\mathcal{V}$ having dimension at least k. By Lemma 14 there exists a unit vector $u \in \mathcal{X} \otimes \mathcal{V} \otimes \mathcal{Q}$ such that

$$\left\| (\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{V}\otimes\mathcal{Q})})(uu^*) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{V}\otimes\mathcal{Q})})(uu^*) \right\|_1 \geq \|\Phi_0 - \Phi_1\|_\diamond ,$$

where $\mathcal{Q}$ is any space with dimension 2. The reverse inequality holds due to a general property of the diamond norm. Taking $\mathcal{W} = \mathcal{V} \otimes \mathcal{Q}$ establishes the theorem. □

Acknowledgments

I thank David Kribs and Vern Paulsen for bringing the work of Timoney to my attention, and Gus Gutoski for helpful comments. This work was supported by Canada's NSERC and the Canadian Institute for Advanced Research (CIFAR).

References

[Ací01] A. Acín. Statistical distinguishability between unitary operations. *Physical Review Letters*, 87(17):177901, 2001.

[AKN98] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.

[Bar02] A. Barvinok. *A Course in Convexity*, volume 54 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[BASTS07] A. Ben-Aroya, O. Schwartz, and A. Ta-Shma. An explicit construction of quantum expanders. Available as arXiv.org e-print 0709.0911, 2007.

[BATS07] A. Ben-Aroya and A. Ta-Shma. Quantum expanders and the quantum entropy difference problem. Available as arXiv.org e-print quant-ph/0702129, 2007.

[CPR00] A. Childs, J. Preskill, and J. Renes. Quantum information and precision measurement. *Journal of Modern Optics*, 47(2–3):155–176, 2000.

[DPP01] G. D'Ariano, P. Presti, and M. Paris. Using entanglement improves the precision of quantum measurements. *Physical Review Letters*, 87(27):270404, 2001.

[GE07] D. Gross and J. Eisert. Quantum Margulis expanders. Available as arXiv.org e-print 0710.0651, 2007.

[GLN05] A. Gilchrist, N. Langford, and M. Nielsen. Distance measures to compare real and ideal quantum processes. *Physical Review A*, 71:062310, 2005.

[Har07] A. Harrow. Quantum expanders from any classical Cayley graph expander. Available as arXiv.org e-print 0709.1142, 2007.

[Has07a] M. Hastings. Entropy and entanglement in quantum ground states. *Physical Review B*, 76:035114, 2007.

[Has07b] M. Hastings. Random unitaries give quantum expenders. *Physical Review A*, 76:032315, 2007.

[HLSW04] P. Hayden, D. Leung, P. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004.

[Kit97] A. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[KSV02] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[KSW06] D. Kretschmann, D. Schlingemann, and R. Werner. The information-disturbance tradeoff and the continuity of Stinespring's representation. Available as arXiv.org e-print quant-ph/0605009, 2006.

[KW00] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof system. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, pages 608–617, 2000.

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

[Pau02] V. Paulsen. *Completely Bounded Maps and Operator Algebras*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2002.

[RW05] B. Rosgen and J. Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Proceedings of the 20th Annual Conference on Computational Complexity*, pages 344–354, 2005.

[Sac05a] M. Sacchi. Entanglement can enhance the distinguishability of entanglement-breaking channels. *Physical Review A*, 72:014305, 2005.

[Sac05b] M. Sacchi. Optimal discrimination of quantum operations. *Physical Review A*, 71:062340, 2005.

[Smi83] R. Smith. Completely bounded maps between C^*-algebras. *Journal of the London Mathematical Society*, 2(1):157–166, 1983.

[Tim03] R. Timoney. Computing the norms of elementary operators. *Illinois Journal of Mathematics*, 47(4):1207–1226, 2003.

[Tim07] R. Timoney. Some formulae for norms of elementary operators. *Journal of Operator Theory*, 57(1):121–145, 2007.

[Wat05] J. Watrous. Notes on super-operator norms induced by Schatten norms. *Quantum Information and Computation*, 5(1):58–68, 2005.