

Distinguishing a maximally entangled basis using LOCC and shared entanglement

Somshubhro Bandyopadhyay*

Vincent Russo[†]

Abstract

We consider the problem of distinguishing between the elements of a bipartite maximally entangled orthonormal basis using LOCC (local operations and classical communication) and a partially entangled state acting as a resource. We derive an exact formula for the optimum success probability and find that it corresponds to the fully entangled fraction of the resource state. The derivation consists of two steps: First, we consider a relaxation of the problem by replacing LOCC with positive-partial-transpose (PPT) measurements and establish an upper bound on the success probability as the solution of a semidefinite program, and then show that this upper bound is achieved by a teleportation-based LOCC protocol. This further implies that separable and PPT measurements provide no advantage over LOCC for this task.

1 Introduction

Distinguishing between quantum states is a fundamental problem in quantum theory, where the aim is to ascertain the state of a quantum system promised to be in one of a known set of states (see [1, 2, 3, 4] for excellent reviews). The problem may be understood as follows. Let $S_\psi = \{(p_i, |\psi_i\rangle) : i = 1, \dots, n\}$ be a set of quantum states, each state occurring with probability p_i such that $\sum_{i=1}^n p_i = 1$. Now consider a quantum system prepared in a state chosen from S_ψ , but we do not know which one. The objective is to determine which state the system is in by performing a suitable measurement. By measurement we mean a positive operator valued measure (POVM) described by a collection of positive operators satisfying the completeness relation. Now, according to quantum theory, the given states can be perfectly distinguished if and only if they are mutually orthogonal, and when they are not, the best one can do is to perform a measurement which is optimal according to some well-defined distinguishability measure. One such measure is the success probability, the maximum probability that the unknown state is identified correctly and is defined as

$$p(S_\psi) = \sup_{\mathbf{M}} \sum_{i=1}^n p_i \langle \psi_i | M_i | \psi_i \rangle, \quad (1)$$

where $\mathbf{M} = \{M_1, \dots, M_n\}$ is a measurement and the supremum is taken over all measurements. Computing the success probability in general is hard, and exact results have been found only for specific instances of the problem (see [1, 2, 4] for comprehensive discussions).

Local distinguishability

This problem has also been studied within the “distant lab” paradigm in quantum information theory [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 30, 32, 33, 34]. For simplicity, we confine our discussion to bipartite quantum systems of finite dimension $\mathbb{C}^d \otimes \mathbb{C}^d$, where $d \geq 2$. The given state now belongs to a known set of bipartite states $S_\phi = \{(p_i, |\phi_i\rangle) : i = 1, \dots, n\}$ and is shared between two distant observers, Alice and Bob. The goal is the same as before, but the measurements are restricted

*Department of Physical Sciences, Bose Institute, Bidhannagar, Kolkata 700091, India; som@jcbose.ac.in, som.s.bandyopadhyay@gmail.com

[†]Unitary Fund; vincent@unitary.fund

to *local operations and classical communication* (LOCC) [35], wherein Alice and Bob perform measurements on their respective local systems and communicate via classical channels but cannot exchange quantum information. The primary question of interest is how well LOCC can distinguish the given states relative to global measurement (measurement performed on the whole system). For example, if the states $|\phi_i\rangle$ are orthogonal, one would be interested in knowing whether they can be perfectly distinguished by LOCC, as is always possible by a global measurement. One motivation for studying this problem is to find out how much global information encoded in orthogonal states of composite systems is accessible by local means. Another motivation is to explore nonlocal properties that may manifest in this setup.

It turns out that in some instances of the problem, LOCC is optimal, and in some, it is not. For example, two orthogonal pure states can be perfectly distinguished by LOCC¹ irrespective of the number of parties, dimensions, or entanglement [8]. However, this does not always hold for sets of three or more orthogonal states. Notable examples of sets whose members are not perfectly distinguishable by LOCC include the Bell basis [10], orthogonal bases containing entangled states [12], unextendible product bases [7, 13], orthogonal product bases exhibiting nonlocality without entanglement [6, 20, 22, 32] and strong nonlocality without entanglement [33]. Orthogonal states, which are perfectly distinguishable by LOCC, are called locally distinguishable. Otherwise, they are locally indistinguishable. Locally indistinguishable states, product or otherwise, are said to be nonlocal in the sense a global measurement can extract more information about the unknown state than coordinated local measurements alone. These states have also found novel applications in quantum cryptography primitives, such as secret sharing [41] and data hiding [37, 38, 39, 40].

Local (LOCC) distinguishability can be similarly quantified by (local) success probability. Following (1), it is defined as (also, see [36])

$$p_L(S_\phi) = \sup_{\pi \in \text{LOCC}} \sum_{i=1}^n p_i \langle \phi_i | \pi_i | \phi_i \rangle, \quad (2)$$

where $\pi = \{\pi_1, \dots, \pi_n\}$ is an LOCC measurement. Computing the local optimum is notoriously hard even for orthogonal states, for the LOCC class does not admit tractable characterization. Nevertheless, a few results have been found – for the members of the Bell basis, given with probabilities $p_1 \geq p_2 \geq p_3 \geq p_4 > 0$, the success probability is $p_1 + p_2$ [30, 36] and for any three uniformly distributed Bell states, it is $2/3$ [31]; in dimensions $\mathbb{C}^d \otimes \mathbb{C}^d$ for $d \geq 3$, it has been shown that a set of n maximally entangled states can be locally distinguished with success probability at most d/n [17], from which it follows that no more than d maximally entangled states can be perfectly distinguished by LOCC; however, in some state spaces for $d \geq 4$, one can find even smaller locally indistinguishable sets for which $n \leq d$ [27, 28, 29].

Local distinguishability with shared entanglement

By definition, LOCC is a strict subset of all quantum operations that one may perform on a composite system; for example, LOCC can neither create entanglement nor increase entanglement on average. The limitations of LOCC, however, can be overcome with shared entanglement, which is why entanglement is considered a resource for quantum information processing tasks. Naturally, one would like to know how entanglement can help distinguish locally indistinguishable states by LOCC [31, 43, 44, 45, 46, 47, 49, 50].

One of the first questions addressed in this context deals with entanglement cost, which quantifies how much entanglement must be consumed to perfectly distinguish locally indistinguishable states by LOCC [31, 43, 44, 45, 47, 50]. It has been shown that, for example, a $\mathbb{C}^2 \otimes \mathbb{C}^2$ maximally entangled state is necessary and sufficient to perfectly distinguish the members of the Bell basis by LOCC [31]. The LOCC protocol here mimics quantum teleportation [48] and is known as the “teleportation protocol”, where one-half of the unknown state is first teleported using the resource state, followed by a Bell measurement. Likewise, a $\mathbb{C}^d \otimes \mathbb{C}^d$ maximally entangled state is necessary and sufficient to perfectly distinguish a $\mathbb{C}^d \otimes \mathbb{C}^d$ maximally entangled basis for all $d \geq 3$ by LOCC. The proof of this fact follows from a simple application of a result proved in [12]. Exact results, however, are hard to obtain for generic sets of orthonormal states, even if they form a basis. Nevertheless, lower bounds have been found; for example, a lower bound on the entanglement cost of locally distinguishing an arbitrary orthonormal basis, not necessarily maximally entangled, is

¹For two orthogonal mixed states, surprisingly, this is not always true [26, 34].

given by the average entanglement of the basis states [44], assuming the states are all equally probable. In $\mathbb{C}^2 \otimes \mathbb{C}^2$, this lower bound can be improved upon for almost all orthonormal bases [45].

Instead of asking about entanglement cost, one could ask how well locally indistinguishable states can be distinguished by LOCC using shared entanglement as a resource [31, 46, 47, 49, 50]. The present work considers a problem of this kind, so let us discuss the essentials of this problem in some detail.

Let $\mathcal{A}_1 = \mathcal{A}_2 = \mathbb{C}^d$ and $\mathcal{B}_1 = \mathcal{B}_2 = \mathbb{C}^d$ denote the state spaces corresponding to the quantum systems held by Alice and Bob, respectively. Let

$$S_\chi = \{(p_i, |\chi_i\rangle) : i = 1, \dots, n\} \quad (3)$$

be an orthonormal set of locally indistinguishable states, where $|\chi_i\rangle \in \mathcal{A}_1 \otimes \mathcal{B}_1$. Suppose that Alice and Bob wish to distinguish the elements of S_χ using LOCC and a resource state $|\varphi\rangle \in \mathcal{A}_2 \otimes \mathcal{B}_2$. It is easy to see that this boils down to distinguishing between the elements of the set

$$S_{\chi \otimes \varphi} = \{(p_i, |\chi_i\rangle \otimes |\varphi\rangle) : i = 1, \dots, n\} \quad (4)$$

by LOCC, where $|\chi_i\rangle \otimes |\varphi\rangle \in \mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{A}_2 \otimes \mathcal{B}_2$.

Since Alice holds \mathcal{A}_1 and \mathcal{A}_2 and Bob holds \mathcal{B}_1 and \mathcal{B}_2 , LOCC is defined with respect to the bipartition $\mathcal{A} : \mathcal{B}$, where $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ and $\mathcal{B} = \mathcal{B}_1 \otimes \mathcal{B}_2$. This reflects the fact that Alice and Bob may perform joint measurements on the composite systems \mathcal{A} and \mathcal{B} , respectively. So to define the success probability we need to take this into consideration, which requires expressing the states $|\chi_i\rangle \otimes |\varphi\rangle$ as states in $\mathcal{A} \otimes \mathcal{B}$ by swapping the systems \mathcal{B}_1 and \mathcal{A}_2 .

Define the unitary swap operator $U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} : \mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{A}_2 \otimes \mathcal{B}_2 \rightarrow \mathcal{A} \otimes \mathcal{B}$ whose action on product states is given by

$$U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} (|\alpha_1\rangle |\beta_1\rangle |\alpha_2\rangle |\beta_2\rangle) = |\alpha_1\rangle |\alpha_2\rangle |\beta_1\rangle |\beta_2\rangle \quad (5)$$

for all vectors $|\alpha_1\rangle \in \mathcal{A}_1$, $|\alpha_2\rangle \in \mathcal{A}_2$, $|\beta_1\rangle \in \mathcal{B}_1$, $|\beta_2\rangle \in \mathcal{B}_2$.

Let $|\chi_i\rangle \otimes |\varphi\rangle \rightarrow |\xi_i\rangle \in \mathcal{A} \otimes \mathcal{B}$ for each $i = 1, \dots, n$, where $|\xi_i\rangle = U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} (|\chi_i\rangle \otimes |\varphi\rangle)$. Accordingly, the success probability is defined as

$$p_L(S_{\chi \otimes \varphi}) = \sup_{\Pi \in \text{LOCC}} \sum_{i=1}^n p_i \langle \xi_i | \Pi_i | \xi_i \rangle, \quad (6)$$

where $\Pi = \{\Pi_1, \dots, \Pi_n\}$ is an LOCC measurement realized in the bipartition $\mathcal{A} : \mathcal{B}$.

The success probability, defined in (6), has been exactly computed for sets of Bell states and a resource state of the form $|\eta\rangle = a_1 |00\rangle + a_2 |11\rangle$, where $a_1 \geq a_2 \geq 0$ and $a_1^2 + a_2^2 = 1$. For the Bell basis, denoted by S_B , assuming uniform distribution, it is given by [31]

$$p_L(S_{B \otimes \eta}) = \frac{1}{2} (1 + 2a_1 a_2). \quad (7)$$

The success probability is unity if and only if $a_1 = a_2 = 1/\sqrt{2}$, so the Bell basis can be perfectly distinguished if and only if the resource state is maximally entangled. For a set of any three uniformly distributed Bell states, denoted by $S_{B'}$, the success probability turns out to be [31]

$$p_L(S_{B' \otimes \eta}) = \frac{2}{3} (1 + a_1 a_2). \quad (8)$$

Observe that one still requires a maximally entangled state as a resource to perfectly distinguish three Bell states by LOCC. In some sense, this is counter-intuitive because one would have expected the entanglement cost in this case to be less than that for the Bell basis. Besides these two examples, recently, the local optimum with shared entanglement has been computed for a family of noisy Bell states, which shows, yet again, the optimum value (i.e., the global optimum) is achieved with a maximally entangled resource [50].

The formulas in (7) and (8) are not just ordinary functions of the Schmidt coefficients a_1 and a_2 . In particular, the one in (7) is the fully entangled fraction of the resource state $|\eta\rangle$, defined as [51]

$$F(\eta) = \max_{|\Psi\rangle} \langle \Psi | \eta | \Psi \rangle, \quad (9)$$

where $\eta = |\eta\rangle\langle\eta|$, and the maximum is taken over all maximally entangled states $|\Psi\rangle$. So we can write (7) simply as

$$p_L(S_{B\otimes\eta}) = F(\eta). \quad (10)$$

Therefore, how well the Bell basis can be distinguished using LOCC and shared entanglement as a resource is given by how close the resource state is to a maximally entangled state. Likewise, one may also express (8) as a function of $F(\eta)$.

Note that, besides the fully entangled fraction, one may also express (7) and (8) as a simple function of the entanglement of $|\eta\rangle$ quantified by an entanglement measure such as negativity $N(\eta) = a_1 a_2$ [52].

Problem statement

Let $\{|\Psi_1\rangle, \dots, |\Psi_{d^2}\rangle\}$ be an orthonormal, maximally entangled basis of $\mathcal{A}_1 \otimes \mathcal{B}_1$. Without loss of generality, we assume that

$$|\Psi_1\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle |i\rangle \quad (11)$$

is the standard maximally entangled state. The remaining states can be written as

$$|\Psi_j\rangle = (\mathbf{1}_{\mathcal{A}_1} \otimes U_j) |\Psi_1\rangle \quad (12)$$

for some unitary operator $U_j \in U(\mathcal{B}_1)$ for each $j = 2, \dots, d^2$, where $U(\mathcal{B}_1)$ denotes the set of unitary operators acting on \mathcal{B}_1 . Since $\langle\Psi_i|\Psi_j\rangle = \delta_{ij}$ for all $i, j = 1, \dots, d^2$, the unitary operators obey the relation $\text{Tr}(U_i^\dagger U_j) = d\delta_{ij}$ for $i, j = 1, \dots, d^2$, where $U_1 = \mathbf{1}_{\mathcal{B}_1}$.

Define the set

$$S_\Psi = \left\{ \left(\frac{1}{d^2}, |\Psi_k\rangle \right) : k = 1, \dots, d^2 \right\}. \quad (13)$$

This set is locally indistinguishable [12, 17] with the local optimum given by $p_L(S_\Psi) = 1/d$ [17, 28].

In this paper, we consider the problem of distinguishing between the elements of S_Ψ using LOCC and a resource state

$$|\tau\rangle = \sum_{i=1}^d a_i |i\rangle |i\rangle \in \mathcal{A}_2 \otimes \mathcal{B}_2, \quad (14)$$

where $\{a_i\}$ are the ordered Schmidt coefficients ($a_1 \geq a_2 \geq \dots \geq a_d \geq 0$) satisfying $\sum_{i=1}^d a_i^2 = 1$. Note that the resource state is entangled as long as two or more Schmidt coefficients are positive.

The set of interest is, therefore,

$$S_{\Psi\otimes\tau} = \left\{ \left(\frac{1}{d^2}, |\Psi_k\rangle \otimes |\tau\rangle \right) : k = 1, \dots, d^2 \right\}. \quad (15)$$

We wish to find out how well the elements of $S_{\Psi\otimes\tau}$ can be distinguished by LOCC. Since this problem is defined in the bipartition $\mathcal{A} : \mathcal{B}$ with $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ and $\mathcal{B} = \mathcal{B}_1 \otimes \mathcal{B}_2$, we first let $|\Psi_k\rangle \otimes |\tau\rangle \rightarrow |\Phi_k\rangle \in \mathcal{A} \otimes \mathcal{B}$, where $|\Phi_k\rangle = U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} (|\Psi_k\rangle \otimes |\tau\rangle)$ for each $k = 1, \dots, d^2$, and define the success probability as

$$p_L(S_{\Psi\otimes\tau}) = \sup_{\Pi \in \text{LOCC}} \frac{1}{d^2} \sum_{i=1}^{d^2} \langle \Phi_i | \Pi_i | \Phi_i \rangle, \quad (16)$$

where $\Pi = \{\Pi_1, \dots, \Pi_{d^2}\}$ is an LOCC measurement realized the bipartition $\mathcal{A} : \mathcal{B}$.

Our objective is to compute the local optimum defined in (16) and find an LOCC protocol achieving the same value. As far as we are aware, this problem remains open in all state spaces $\mathbb{C}^d \otimes \mathbb{C}^d$ for $d \geq 3$. We are particularly interested in knowing whether an expression similar to (10) holds for $p_L(S_{\Psi\otimes\tau})$ as well.

Overview of results

The main result of the paper is the following:

Theorem 1. *The success probability for distinguishing the elements of $S_{\Psi \otimes \tau}$ by LOCC is given by*

$$p_L(S_{\Psi \otimes \tau}) = F(\tau), \quad (17)$$

where $F(\tau)$ is the fully entangled fraction of $|\tau\rangle$, defined as the maximum overlap between $|\tau\rangle$ and a maximally entangled state, and given by the formula [51]

$$F(\tau) = \frac{1}{d} \left(\sum_{i=1}^d a_i \right)^2 \in \left[\frac{1}{d}, 1 \right]. \quad (18)$$

The optimum value is achieved by a teleportation-based LOCC protocol.

Remark 1. Since $\frac{1}{d} \leq F(\tau) \leq 1$, it holds that $\frac{1}{d} \leq p_L(S_{\Psi \otimes \tau}) \leq 1$, where each of the left and right inequalities become equality for product and maximally entangled $|\tau\rangle$, respectively.

Remark 2. Theorem 1 holds for any maximally entangled basis of $\mathbb{C}^d \otimes \mathbb{C}^d$. Our proof, as we will see, is representation independent.

Remark 3. One may also express the success probability as a function of the negativity of the resource state $N(\tau)$ using the relation $F(\tau) = \frac{1}{d} [1 + 2N(\tau)]$.

To prove Theorem 1 we will proceed as follows. First we will consider a relaxation of our problem by replacing LOCC with positive-partial-transpose (PPT) measurements (these are measurements whose operators are positive under partial transposition). The (PPT) success probability is defined as

$$p_{\text{PPT}}(S_{\Psi \otimes \tau}) = \sup_{\Omega \in \text{PPT}} \frac{1}{d^2} \sum_{i=1}^{d^2} \langle \Phi_i | \Omega_i | \Phi_i \rangle, \quad (19)$$

where $\Omega = \{\Omega_1, \dots, \Omega_{d^2}\}$ is a PPT measurement on $\mathcal{A} \otimes \mathcal{B}$.

Following [28], we will formulate our PPT distinguishability problem as a semidefinite program (SDP) and solve the dual problem to obtain an upper bound on $p_{\text{PPT}}(S_{\Psi \otimes \tau})$.

Lemma 1. *An upper bound on the success probability for distinguishing the elements of $S_{\Psi \otimes \tau}$ by any PPT measurement is given by*

$$p_{\text{PPT}}(S_{\Psi \otimes \tau}) \leq F(\tau). \quad (20)$$

Since LOCC is a strict subset of PPT measurements, we have the following corollary.

Corollary 1. *For the given set of states $S_{\Psi \otimes \tau}$, it holds that*

$$p_L(S_{\Psi \otimes \tau}) \leq p_{\text{PPT}}(S_{\Psi \otimes \tau}) \leq F(\tau). \quad (21)$$

The next result shows that the upper bound in Corollary 1 is also a lower bound on $p_L(S_{\Psi \otimes \tau})$.

Lemma 2. *The success probability for distinguishing the elements of $S_{\Psi \otimes \tau}$ by LOCC is bounded below by*

$$p_L(S_{\Psi \otimes \tau}) \geq F(\tau). \quad (22)$$

We will prove Lemma 2 by presenting an LOCC protocol that distinguishes between the elements of $S_{\Psi \otimes \tau}$ with probability $F(\tau)$. The protocol here is based on quantum teleportation.

Since the lower bound in Lemma 2 matches the upper bound in Corollary 1, this completes the proof of Theorem 1. Furthermore,

$$p_L(S_{\Psi \otimes \tau}) = p_{\text{PPT}}(S_{\Psi \otimes \tau}) = F(\tau), \quad (23)$$

which shows that, even though $\text{LOCC} \subset \text{PPT}$, the LOCC optimum equals the PPT optimum. Thus PPT measurements (hence, separable measurements) provide no advantage in distinguishing a maximally entangled basis using shared entanglement.

The rest of the paper is arranged as follows. In section 2, we discuss the SDP formulation of distinguishing a set of states by PPT measurements, including ours. We prove Lemma 1 in section 3 and Lemma 2 in section 4. We conclude in section 5 with a brief summary of results and a discussion on open problems.

2 PPT distinguishability as a semidefinite program

The problem of distinguishing a set of states by PPT measurements can be cast as a semidefinite program [28] and, thereby, can be solved for many problems of interest. This, coupled with the fact that LOCC \subset PPT has yielded exact results [28, 29, 31, 34, 50], no-go results [27, 34], and useful bounds [28, 34] for local (in)distinguishability problems that were once thought to be intractable.

Let \mathcal{X} and \mathcal{Y} represent d -dimensional state spaces for $d \geq 2$. Let $\text{Pos}(\mathcal{X})$, $\text{Pos}(\mathcal{Y})$, and $\text{Pos}(\mathcal{X} \otimes \mathcal{Y})$ denote the sets of positive semidefinite operators acting on \mathcal{X} , \mathcal{Y} , and $\mathcal{X} \otimes \mathcal{Y}$, respectively. An operator $P \in \text{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is PPT if $T_{\mathcal{X}}(P) \in \text{Pos}(\mathcal{X} \otimes \mathcal{Y})$, where $T_{\mathcal{X}}$ represents partial transposition taken in the standard basis of \mathcal{X} (note that, as far as the definition of PPT is concerned, partial transposition could be taken with respect to any one of the state spaces \mathcal{X} or \mathcal{Y}).

Denote the set of all PPT operators acting on $\mathcal{X} \otimes \mathcal{Y}$ by $\text{PPT}(\mathcal{X} : \mathcal{Y})$. The set $\text{PPT}(\mathcal{X} : \mathcal{Y})$ is a closed, convex cone. A PPT measurement is defined by a collection of measurement operators $\{P_1, \dots, P_n\}$, where $P_i \in \text{PPT}(\mathcal{X} : \mathcal{Y})$ for each $i = 1, \dots, n$.

For a given ensemble $\mathcal{E} = \{(p_i, \rho_i) : i = 1, \dots, n\}$, where ρ_i are density operators on $\mathcal{X} \otimes \mathcal{Y}$, the problem of finding $p_{\text{PPT}}(\mathcal{E})$ can be expressed as a semidefinite program [28]:

Primal problem	Dual problem
maximize: $\sum_{i=1}^n p_i \text{Tr}(\rho_i P_i)$	minimize: $\text{Tr}(H)$
subject to: $\sum_{i=1}^n P_i = \mathbf{1}_{\mathcal{X} \otimes \mathcal{Y}}$	subject to: $H - p_k \rho_k \in \text{PPT}(\mathcal{X} : \mathcal{Y})$
$P_k \in \text{PPT}(\mathcal{X} : \mathcal{Y})$	$H \in \text{Herm}(\mathcal{X} \otimes \mathcal{Y})$
$(k = 1, \dots, n)$	$(k = 1, \dots, n)$

where $\text{Herm}(\mathcal{X} \otimes \mathcal{Y})$ is the set of Hermitian operators acting on $\mathcal{X} \otimes \mathcal{Y}$.

Let ω denote the solution of the dual problem. By the weak duality theorem, it holds that $p_{\text{PPT}}(\mathcal{E}) \leq \omega$. Thus, every feasible solution of the dual problem provides an upper bound on $p_{\text{PPT}}(\mathcal{E})$.

Distinguishing the elements of $S_{\Psi \otimes \tau}$ by PPT measurements: SDP formulation

Following the above prescription, the primal and dual problems for distinguishing the elements of $S_{\Psi \otimes \tau}$ by a PPT measurement are the following:

Primal problem	Dual problem
maximize: $\frac{1}{d^2} \sum_{i=1}^{d^2} \langle \Phi_i \Omega_i \Phi_i \rangle$	minimize: $\text{Tr}(H)$
subject to: $\sum_{i=1}^{d^2} \Omega_i = \mathbf{1}_{\mathcal{A} \otimes \mathcal{B}}$	subject to: $H - \Phi_k / d^2 \in \text{PPT}(\mathcal{A} : \mathcal{B})$
$\Omega_k \in \text{PPT}(\mathcal{A} : \mathcal{B})$	$H \in \text{Herm}(\mathcal{A} \otimes \mathcal{B})$
$(k = 1, \dots, d^2)$	$(k = 1, \dots, d^2)$

where $\Phi_k = |\Phi_k\rangle \langle \Phi_k|$ and $\text{Herm}(\mathcal{A} \otimes \mathcal{B})$ is the set of Hermitian operators acting on $\mathcal{A} \otimes \mathcal{B}$.

Therefore, any $H \in \text{Herm}(\mathcal{A} \otimes \mathcal{B})$ for which the constraint of the dual problem is satisfied, it holds that

$$p_{\text{PPT}}(S_{\Psi \otimes \tau}) \leq \text{Tr}(H). \quad (24)$$

So if we could find an appropriate H , we would immediately obtain an upper bound on the local optimum $p_L(S_{\Psi \otimes \tau})$ as $p_L(S_{\Psi \otimes \tau}) \leq p_{\text{PPT}}(S_{\Psi \otimes \tau})$.

3 Proof of Lemma 1

Our objective is to find an $H \in \text{Herm}(\mathcal{A} \otimes \mathcal{B})$ that satisfies the dual feasibility condition

$$\text{T}_{\mathcal{A}} \left(H - \Phi_k / d^2 \right) = \text{T}_{\mathcal{A}}(H) - \frac{1}{d^2} \text{T}_{\mathcal{A}}(\Phi_k) \in \text{Pos}(\mathcal{A} \otimes \mathcal{B}), \quad k = 1, \dots, d^2, \quad (25)$$

and for which $\text{Tr}(H) = F(\tau)$. Once an appropriate H is found, the proof will then follow from (24).

Let \mathbb{H} be a Hermitian operator of the form

$$\mathbb{H} = \sum_{i=1}^m h_{1i} \otimes h_{2i} \in \text{Herm}(\mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{A}_2 \otimes \mathcal{B}_2), \quad (26)$$

where $h_{1i} \in \text{Herm}(\mathcal{A}_1 \otimes \mathcal{B}_1)$ and $h_{2i} \in \text{Herm}(\mathcal{A}_2 \otimes \mathcal{B}_2)$ for each $i = 1, \dots, m$. We will use the following lemma to find a feasible solution of the dual problem.

Lemma 3. *Suppose \mathbb{H} is a Hermitian operator of the form (26) such that*

$$(\text{T}_{\mathcal{A}_1} \otimes \text{T}_{\mathcal{A}_2}) \left(\mathbb{H} - \frac{1}{d^2} \Psi_k \otimes \tau \right) \in \text{Pos}(\mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{A}_2 \otimes \mathcal{B}_2) \quad (27)$$

for each $k = 1, \dots, d^2$, where $\Psi_k = |\Psi_k\rangle \langle \Psi_k|$ and $\tau = |\tau\rangle \langle \tau|$. Then the dual feasibility condition (25) is satisfied for

$$H = U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} \mathbb{H} U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger \in \text{Herm}(\mathcal{A} \otimes \mathcal{B}). \quad (28)$$

The proof is given in the appendix.

First observe that the equality

$$\text{Tr}(H) = \text{Tr}(\mathbb{H}) \quad (29)$$

follows immediately from (28).

Therefore, to prove Lemma 1 it is sufficient to find an \mathbb{H} of the form (26) such that (27) is satisfied for all $k = 1, \dots, d^2$, and for which $\text{Tr}(\mathbb{H}) = F(\tau)$.

Define a operator

$$\mathbb{H} = \frac{1}{d^3} \mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1} \otimes \left[\tau + 2 \sum_{i,j=1, i < j}^d a_i a_j \text{T}_{\mathcal{A}_2}(\psi_{ij}^-) \right] \in \text{Herm}(\mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{A}_2 \otimes \mathcal{B}_2), \quad (30)$$

where $\psi_{ij}^- = |\psi_{ij}^- \rangle \langle \psi_{ij}^-|$, $|\psi_{ij}^- \rangle = \frac{1}{\sqrt{2}} (|i\rangle |j\rangle - |j\rangle |i\rangle)$, and $\text{T}_{\mathcal{A}_2}$ denotes the partial transposition of with respect to the standard basis of \mathcal{A}_2 .

Observe that \mathbb{H} has the form (26), and a simple calculation shows

$$\text{Tr}(\mathbb{H}) = \frac{1}{d} \left(1 + 2 \sum_{i,j=1, i < j}^d a_i a_j \right) = F(\tau), \quad (31)$$

where the second equality follows from (18). We now prove that the positivity condition (27) is satisfied.

First, observe that

$$\begin{aligned} (\text{T}_{\mathcal{A}_1} \otimes \text{T}_{\mathcal{A}_2}) \left[\mathbb{H} - \frac{1}{d^2} (\Psi_k \otimes \tau) \right] &= (\text{T}_{\mathcal{A}_1} \otimes \text{T}_{\mathcal{A}_2}) \mathbb{H} - \frac{1}{d^2} (\text{T}_{\mathcal{A}_1} \otimes \text{T}_{\mathcal{A}_2}) (\Psi_k \otimes \tau) \\ &= \frac{1}{d^3} \mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1} \otimes \left[\text{T}_{\mathcal{A}_2}(\tau) + 2 \sum_{i,j=1, i < j}^d a_i a_j \psi_{ij}^- \right] - \frac{1}{d^2} \text{T}_{\mathcal{A}_1}(\Psi_k) \otimes \text{T}_{\mathcal{A}_2}(\tau) \\ &= \frac{1}{d^3} \Psi_k \otimes \text{T}_{\mathcal{A}_2}(\tau) + \mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1} \otimes \frac{2}{d^3} \sum_{i,j=1, i < j}^d a_i a_j \psi_{ij}^-, \end{aligned} \quad (32)$$

where

$$Y_k = \mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1} - d\mathbb{T}_{\mathcal{A}_1}(\Psi_k). \quad (33)$$

We will now evaluate the RHS of (32).

A straightforward calculation reveals

$$\mathbb{T}_{\mathcal{A}_2}(\tau) = \sum_{i=1}^d a_i^2 \psi_{ii} + \sum_{i,j=1, i<j}^d a_i a_j \psi_{ij}^+ - \sum_{i,j=1, i<j}^d a_i a_j \psi_{ij}^-, \quad (34)$$

where $\psi_{ii} = |\psi_{ii}\rangle \langle \psi_{ii}|$, $|\psi_{ii}\rangle = |i\rangle |i\rangle$ and $\psi_{ij}^+ = |\psi_{ij}^+\rangle \langle \psi_{ij}^+|$, $|\psi_{ij}^+\rangle = \frac{1}{\sqrt{2}}(|i\rangle |j\rangle + |j\rangle |i\rangle)$. Let

$$\Gamma = \sum_{i=1}^d a_i^2 \psi_{ii} + \sum_{i,j=1, i<j}^d a_i a_j \psi_{ij}^+ \quad (35)$$

which is clearly positive semidefinite (since $a_i \geq 0$ for all $i = 1, \dots, d$, and $\{\psi_{ii}\}$ and $\{\psi_{ij}^+\}$ are density operators) and write (34) in a compact form

$$\mathbb{T}_{\mathcal{A}_2}(\tau) = \Gamma - \sum_{i,j=1, i<j}^d a_i a_j \psi_{ij}^-. \quad (36)$$

Using (36) in (32) and simplifying, we get

$$(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) \left[\mathbb{H} - \frac{1}{d^2} (\Psi_k \otimes \tau) \right] = \frac{1}{d^3} Y_k \otimes \Gamma + \frac{2}{d^3} \sum_{i,j=1, i<j}^d a_i a_j \left(\mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1} - \frac{1}{2} Y_k \right) \otimes \psi_{ij}^-. \quad (37)$$

Since Γ and the density operators $\{\psi_{ij}^-\}$, both being independent of k , are positive semidefinite, it suffices to prove that Y_k and $\left(\mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1} - \frac{1}{2} Y_k \right)$ are positive semidefinite for each $k = 1, \dots, d^2$.

To calculate Y_k , we need to first compute $\mathbb{T}_{\mathcal{A}_1}(\Psi_k)$. This requires expressing $|\Psi_k\rangle$ in an orthonormal product basis of the form $\{|\mu_i\rangle | \nu_j\rangle\}_{i,j=1}^d$, where $\{|\mu_i\rangle\}_{i=1}^d$ and $\{|\nu_j\rangle\}_{j=1}^d$ are the orthonormal bases of \mathcal{A}_1 and \mathcal{B}_1 respectively, and then taking the partial transpose in the basis of \mathcal{A}_1 . For our purpose, it will be convenient to take this product basis as the Schmidt basis of $|\Psi_k\rangle$ for each k (note that the Schmidt basis, in general, will be different for different $|\Psi_k\rangle$). We therefore write $|\Psi_k\rangle$ in the Schmidt form

$$|\Psi_k\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |\alpha_k^i\rangle |\beta_k^i\rangle, \quad (38)$$

where $\{|\alpha_k^1\rangle, \dots, |\alpha_k^d\rangle\}$ and $\{|\beta_k^1\rangle, \dots, |\beta_k^d\rangle\}$ are orthonormal bases of \mathcal{A}_1 and \mathcal{B}_1 , respectively. It holds that

$$\mathbb{T}_{\mathcal{A}_1}(\Psi_k) = \frac{1}{d} \left[\sum_i \zeta_k^{ii} + \sum_{i,j=1, i<j}^d \zeta_k^{ij+} - \sum_{i,j=1, i<j}^d \zeta_k^{ij-} \right], \quad (39)$$

where $\zeta_k^{ii} = |\zeta_k^{ii}\rangle \langle \zeta_k^{ii}|$, $|\zeta_k^{ii}\rangle = |\alpha_k^i\rangle |\beta_k^i\rangle$; $\zeta_k^{ij\pm} = |\zeta_k^{ij\pm}\rangle \langle \zeta_k^{ij\pm}|$, $|\zeta_k^{ij\pm}\rangle = \frac{1}{\sqrt{2}} \left(|\alpha_k^i\rangle |\beta_k^j\rangle \pm |\alpha_k^j\rangle |\beta_k^i\rangle \right)$.

Now decomposing $\mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1}$ as

$$\mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1} = \sum_{i=1}^d \zeta_k^{ii} + \sum_{i,j=1, i<j}^d \zeta_k^{ij+} + \sum_{i,j=1, i<j}^d \zeta_k^{ij-} \quad (40)$$

and using (40) and (39) in (33), we get

$$Y_k = 2 \sum_{i,j=1, i<j}^d \zeta_k^{ij-}, \quad (41)$$

which is positive semidefinite. Similarly, from (40) and (41), we get

$$\left(\mathbf{1}_{\mathcal{A}_1 \otimes \mathcal{B}_1} - \frac{1}{2} Y_k \right) = \sum_{i=1}^d \zeta_k^{ii} + \sum_{i,j=1, i<j}^d \zeta_k^{ij+}, \quad (42)$$

which is also positive semidefinite.

The above analysis clearly holds for any $k \in \{1, \dots, d^2\}$, and so we have proved (27) for all $k = 1, \dots, d^2$. This completes the proof of Lemma 1.

4 Proof of Lemma 2

The LOCC protocol for distinguishing the elements of $S_{\Psi \otimes \tau}$ is based on quantum teleportation. But before we describe the protocol, it will be helpful to understand how states transform under teleportation.

Recall that in the standard teleportation protocol of a d -dimensional quantum state, the teleportation channel is taken to be the maximally entangled state $|\Psi_1\rangle$ given by (11), Alice performs her measurement in the canonical maximally entangled basis, communicates her outcome to Bob via a classical channel, and Bob applies a unitary correction chosen from a fixed set of unitary operators. Note that the unitary operator that Bob applies depends on the outcome of Alice's measurement; in particular, there is an one-to-one correspondence between Alice's outcome and Bob's unitary correction.

Suppose Alice wants to teleport a quantum state, say, $|\varphi\rangle \in \mathbb{C}^d$, but instead of $|\Psi_1\rangle$ they share a maximally entangled state $|\Psi_x\rangle \in \mathcal{A}_1 \otimes \mathcal{B}_1$, where $|\Psi_x\rangle = (\mathbf{1}_{\mathcal{A}_1} \otimes V_x) |\Psi_1\rangle$ for some unitary operator $V_x \in U(\mathcal{B}_1)$. It is easy to check that if they carry out all the steps of the standard protocol prescribed for $|\Psi_1\rangle$, Bob will end up with the state $|\varphi_x\rangle = V_x |\varphi\rangle$. Therefore, in order to reproduce the teleportation input correctly Bob needs to apply another unitary correction V_x^{-1} on $|\varphi_x\rangle$.

Now suppose that Alice and Bob do not know the identity of $|\Psi_x\rangle$ but only that it belongs to a known set, i.e., $|\Psi_x\rangle \in \{|\Psi_{x_1}\rangle, \dots, |\Psi_{x_n}\rangle\}$, where $|\Psi_{x_i}\rangle = (\mathbf{1}_{\mathcal{A}_1} \otimes V_{x_i}) |\Psi_1\rangle$. It then follows that $|\varphi_x\rangle \in \{|\varphi_{x_1}\rangle, \dots, |\varphi_{x_n}\rangle\}$, where $|\varphi_{x_i}\rangle = V_{x_i} |\varphi\rangle$. In this case, the input state cannot be exactly reproduced at Bob's end because they do not know which maximally entangled state they shared.

This can be extended to teleportation of an entangled system. Suppose the state Alice wants to teleport is $|\Theta\rangle \in \mathcal{A}'' \otimes \mathcal{A}'$, where $\mathcal{A}' = \mathcal{A}'' = \mathbb{C}^d$. Once again assume that the teleportation channel is $|\Psi_x\rangle$. Then at the end of the standard protocol, assuming Alice performs her measurement on the composite system $\mathcal{A}' \otimes \mathcal{A}_1$, they will end up sharing $|\Theta_x\rangle \in \mathcal{A}'' \otimes \mathcal{B}_1$, where $|\Theta_x\rangle = (\mathbf{1}_{\mathcal{A}''} \otimes V_x) |\Theta\rangle$. Moreover, if $|\Psi_x\rangle \in \{|\Psi_{x_1}\rangle, \dots, |\Psi_{x_n}\rangle\}$, then $|\Theta_x\rangle \in \{|\Theta_{x_1}\rangle, \dots, |\Theta_{x_n}\rangle\}$, where $|\Theta_{x_i}\rangle = (\mathbf{1}_{\mathcal{A}''} \otimes V_{x_i}) |\Theta\rangle$.

We now come to the LOCC protocol for distinguishing the elements of $S_{\Psi \otimes \tau}$. The first step is teleportation of one half of the resource state $|\tau\rangle$ using the unknown state, say, $|\Psi_i\rangle \in \{|\Psi_1\rangle, \dots, |\Psi_{d^2}\rangle\}$ following the standard protocol. Noting that $|\Psi_i\rangle$ has the form (12), the initial state can be written as

$$|\Psi_i\rangle \otimes |\tau\rangle = (\mathbf{1}_{\mathcal{A}_1} \otimes U_i) |\Psi_1\rangle \otimes |\tau\rangle \in \mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{A}_2 \otimes \mathcal{B}_2. \quad (43)$$

Now they complete all the steps of the standard protocol (Alice performs her measurement on $\mathcal{A}_1 \otimes \mathcal{A}_2$, informs Bob about the outcome, who applies the prescribed unitary correction on \mathcal{B}_1). From our previous discussion, we know that this results in Bob holding the state

$$|\gamma_i\rangle = (\mathbf{1}_{\mathcal{B}_2} \otimes U_i) |\tau\rangle \in \mathcal{B}_2 \otimes \mathcal{B}_1. \quad (44)$$

Therefore, after teleportation, Bob holds one of $\{|\gamma_1\rangle, \dots, |\gamma_{d^2}\rangle\} \subset \mathcal{B}_2 \otimes \mathcal{B}_1$. The inner product between any pair of states is found to be

$$\langle \gamma_i | \gamma_j \rangle = \sum_{k=1}^d a_k^2 \langle k | U_i^\dagger U_j | k \rangle. \quad (45)$$

As one would expect, the states $|\gamma_i\rangle$ are not all mutually orthogonal unless $|\tau\rangle$ is maximally entangled, in which case we have $a_k^2 = 1/d$ for $k = 1, \dots, d$, and $\langle \gamma_i | \gamma_j \rangle = \frac{1}{d} \text{Tr}(U_i^\dagger U_j) = \delta_{ij}$.

Now observe that the elements of $\{|\Psi_1\rangle, \dots, |\Psi_{d^2}\rangle\}$ are in one-to-one correspondence with that of $\{|\gamma_1\rangle, \dots, |\gamma_{d^2}\rangle\}$, i.e., if the unknown state was $|\Psi_i\rangle$, Bob's state is guaranteed to be $|\gamma_i\rangle$. Therefore, the "teleportation" step of the protocol induces the map $|\Psi_i\rangle \rightarrow |\gamma_i\rangle$ for each $i = 1, \dots, d^2$, and consequently, the problem is mapped onto that of distinguishing between the elements of $\{|\gamma_1\rangle, \dots, |\gamma_{d^2}\rangle\}$, each given with probability $1/d^2$ (since the unknown state $|\Psi_i\rangle$ was selected with probability $1/d^2$).

To distinguish between the states $|\gamma_i\rangle$ Bob performs a measurement in the orthonormal, maximally entangled basis $\{|\Psi_1\rangle, \dots, |\Psi_{d^2}\rangle\} \subset \mathcal{B}_2 \otimes \mathcal{B}_1$, where the basis vectors are defined as $|\Psi_i\rangle = (\mathbf{1}_{\mathcal{B}_2} \otimes U_i) |\Psi_1\rangle$. The outcome of this measurement is now identified as the unknown state that they initially shared. The success probability for this is given by

$$\begin{aligned}
p &= \frac{1}{d^2} \sum_{i=1}^{d^2} |\langle \Psi_i | \gamma_i \rangle|^2 \\
&= \frac{1}{d^2} \sum_{i=1}^{d^2} \left| \langle \Psi_1 | (\mathbf{1}_{\mathcal{B}_2} \otimes U_i^\dagger) (\mathbf{1}_{\mathcal{B}_2} \otimes U_i) |\tau\rangle \right|^2 \\
&= \frac{1}{d^2} \sum_{i=1}^{d^2} |\langle \Psi_1 | \tau \rangle|^2 \\
&= |\langle \Psi_1 | \tau \rangle|^2 = \frac{1}{d} \left(\sum_{i=1}^d a_i \right)^2 = F(\tau).
\end{aligned} \tag{46}$$

This completes the proof.

5 Conclusions

One of the central questions in local distinguishability of quantum states is how well a given set of locally indistinguishable states can be distinguished using LOCC and shared entanglement as a resource. In this paper, we considered the problem of locally distinguishing the elements of a bipartite maximally entangled orthonormal basis using a partially entangled state acting as a resource. In particular, our objective was to find an expression for the success probability, which quantifies how well the basis states can be distinguished in an entanglement-assisted LOCC setup. This has been solved for the Bell basis in $\mathbb{C}^2 \otimes \mathbb{C}^2$ [31] but remained open in all higher dimensions. Here, we solved this problem for any maximally entangled orthonormal basis in dimensions $\mathbb{C}^d \otimes \mathbb{C}^d$, where $d \geq 3$. Assuming the basis states are uniformly distributed, we derived an exact formula for the success probability. This formula corresponds to the fully entangled fraction of the resource state. So, how well the elements of a maximally entangled basis can be locally distinguished using shared entanglement is determined by how close the resource state is to a maximally entangled state.

To derive our formula, we proceeded as follows. First, we established an upper bound on the success probability using the SDP formulation of distinguishing quantum states by PPT measurements [28] and then showed that this upper bound is achievable by LOCC. The LOCC protocol here is based on quantum teleportation. One further concludes that, for distinguishing maximally entangled states with shared entanglement, PPT measurements provide no advantage over LOCC, even though LOCC is a strict subset of PPT measurements.

We now briefly mention a couple of open problems. Let $S \subset \mathbb{C}^d \otimes \mathbb{C}^d$ for $d \geq 2$ be an orthonormal set of maximally entangled states. Such a set is locally indistinguishable whenever $d + 1 \leq |S| \leq d^2$ [17]. In addition, locally indistinguishable sets with $|S| \leq d$ also exist for $d \geq 4$ [28, 29]. A fundamental question is whether a maximally entangled state is always necessary to perfectly distinguish an orthonormal set of maximally entangled states known to be locally indistinguishable. This question is completely solved for $d = 2$ [31] but remains open in higher dimensions except when S is a basis of $\mathbb{C}^d \otimes \mathbb{C}^d$. One could attempt to answer this question in higher dimensions by computing the entanglement cost or the success probability within the framework of entanglement-assisted LOCC as discussed in this paper or earlier works

[31, 44, 45, 47, 50]. The latter approach, which involves computing the success probability, as we did in this paper for $|S| = d^2$, could be fruitful as one could directly check whether the resource state needs to be maximally entangled or not by setting the success probability to unity.

Acknowledgement. We thank Tathagata Gupta and Shayeef Murshid for helpful comments.

Appendix: Proof of Lemma 3

To prove Lemma 3 we will use the following result. Let $\text{Lin}(\mathcal{H} \otimes \mathcal{H}')$ denote the set of linear operators on $\mathcal{H} \otimes \mathcal{H}'$, where \mathcal{H} and \mathcal{H}' are finite-dimensional state spaces.

Lemma 4. *Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_1 = \mathcal{Y}_2 = \mathbb{C}^d$, where $d \geq 2$. For any pair of linear operators $\Lambda \in \text{Lin}(\mathcal{X}_1 \otimes \mathcal{Y}_1)$ and $\Xi \in \text{Lin}(\mathcal{X}_2 \otimes \mathcal{Y}_2)$, it holds that*

$$U_{\mathcal{Y}_1 \leftrightarrow \mathcal{X}_2} [(\text{T}_{\mathcal{X}_1} \otimes \text{T}_{\mathcal{X}_2})(\Lambda \otimes \Xi)] U_{\mathcal{Y}_1 \leftrightarrow \mathcal{X}_2}^\dagger = \text{T}_{\mathcal{X}} [U_{\mathcal{Y}_1 \leftrightarrow \mathcal{X}_2} (\Lambda \otimes \Xi) U_{\mathcal{Y}_1 \leftrightarrow \mathcal{X}_2}^\dagger], \quad (47)$$

where $U_{\mathcal{Y}_1 \leftrightarrow \mathcal{X}_2}$ is the unitary swap operator defined similarly as in (5) and $\mathcal{X} = \mathcal{X}_1 \otimes \mathcal{X}_2$.

Proof. Let $\{|x_i\rangle : i = 1, \dots, d\}$ be the standard basis of \mathcal{X}_1 and \mathcal{X}_2 and $\{|y_i\rangle : i = 1, \dots, d\}$ be the standard bases of \mathcal{Y}_1 and \mathcal{Y}_2 . Linear operators Λ acting on $\mathcal{X}_1 \otimes \mathcal{Y}_1$ and Ξ on $\mathcal{X}_2 \otimes \mathcal{Y}_2$ can be written as

$$\Lambda = \sum_{a,b,c,e} q_{ab}^{ce} |x_a\rangle \langle x_b| \otimes |y_c\rangle \langle y_e|, \quad (48)$$

$$\Xi = \sum_{\alpha,\beta,\gamma,\delta} q_{\alpha\beta}^{\gamma\delta} |x_\alpha\rangle \langle x_\beta| \otimes |y_\gamma\rangle \langle y_\delta|. \quad (49)$$

Therefore,

$$\Lambda \otimes \Xi = \sum_{a,b,c,e,\alpha,\beta,\gamma,\delta} q_{ab}^{ce} q_{\alpha\beta}^{\gamma\delta} |x_a\rangle \langle x_b| \otimes |y_c\rangle \langle y_e| \otimes |x_\alpha\rangle \langle x_\beta| \otimes |y_\gamma\rangle \langle y_\delta|. \quad (50)$$

Let us now compute the LHS of (47). First,

$$\begin{aligned} (\text{T}_{\mathcal{X}_1} \otimes \text{T}_{\mathcal{X}_2})(\Lambda \otimes \Xi) &= \text{T}_{\mathcal{X}_1}(\Lambda) \otimes \text{T}_{\mathcal{X}_2}(\Xi), \\ &= \sum_{a,b,c,e,\alpha,\beta,\gamma,\delta} q_{ab}^{ce} q_{\alpha\beta}^{\gamma\delta} |x_b\rangle \langle x_a| \otimes |y_c\rangle \langle y_e| \otimes |x_\beta\rangle \langle x_\alpha| \otimes |y_\gamma\rangle \langle y_\delta|. \end{aligned} \quad (51)$$

Next, swapping \mathcal{Y}_1 and \mathcal{X}_2 gives

$$\begin{aligned} \text{LHS of (47)} &= \sum_{a,b,c,e,\alpha,\beta,\gamma,\delta} q_{ab}^{ce} q_{\alpha\beta}^{\gamma\delta} |x_b\rangle \langle x_a| \otimes |x_\beta\rangle \langle x_\alpha| \otimes |y_c\rangle \langle y_e| \otimes |y_\gamma\rangle \langle y_\delta|, \\ &= \sum_{a,b,c,e,\alpha,\beta,\gamma,\delta} q_{ab}^{ce} q_{\alpha\beta}^{\gamma\delta} |x_b x_\beta\rangle \langle x_a x_\alpha| \otimes |y_c y_\gamma\rangle \langle y_e y_\delta|. \end{aligned} \quad (52)$$

We now compute the RHS of (47).

$$\begin{aligned} \text{T}_{\mathcal{X}} [U_{\mathcal{Y}_1 \leftrightarrow \mathcal{X}_2} (\Lambda \otimes \Xi) U_{\mathcal{Y}_1 \leftrightarrow \mathcal{X}_2}^\dagger] &= \text{T}_{\mathcal{X}} \left(\sum_{a,b,c,e,\alpha,\beta,\gamma,\delta} q_{ab}^{ce} q_{\alpha\beta}^{\gamma\delta} |x_a\rangle \langle x_b| \otimes |x_\alpha\rangle \langle x_\beta| \otimes |y_c\rangle \langle y_e| \otimes |y_\gamma\rangle \langle y_\delta| \right), \\ &= \text{T}_{\mathcal{X}} \left(\sum_{a,b,c,e,\alpha,\beta,\gamma,\delta} q_{ab}^{ce} q_{\alpha\beta}^{\gamma\delta} |x_a x_\alpha\rangle \langle x_b x_\beta| \otimes |y_c y_\gamma\rangle \langle y_e y_\delta| \right), \\ &= \sum_{a,b,c,e,\alpha,\beta,\gamma,\delta} q_{ab}^{ce} q_{\alpha\beta}^{\gamma\delta} |x_b x_\beta\rangle \langle x_a x_\alpha| \otimes |y_c y_\gamma\rangle \langle y_e y_\delta|. \end{aligned} \quad (53)$$

From (52) and (53), we see that

$$\text{LHS of (47)} = \text{RHS of (47)}. \quad (54)$$

□

Proof of Lemma 3

Suppose that

$$(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) \left(\mathbb{H} - \frac{1}{d^2} \Psi_k \otimes \tau \right) \in \text{Pos}(\mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{A}_2 \otimes \mathcal{B}_2), \quad k = 1, \dots, d^2, \quad (55)$$

where \mathbb{H} is a Hermitian operator of the form given by (26).

Since swapping subsystems does not affect the positivity of an operator, it holds that

$$U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} \left[(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) \left(\mathbb{H} - \frac{1}{d^2} \Psi_k \otimes \tau \right) \right] U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger \in \text{Pos}(\mathcal{A} \otimes \mathcal{B}), \quad k = 1, \dots, d^2. \quad (56)$$

The operator in (56) can be expanded as

$$\begin{aligned} U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} \left[(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) \left(\mathbb{H} - \frac{1}{d^2} \Psi_k \otimes \tau \right) \right] U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger &= U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} [(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) \mathbb{H}] U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger \\ &\quad - \frac{1}{d^2} U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} [(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) (\Psi_k \otimes \tau)] U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger. \end{aligned} \quad (57)$$

We now apply Lemma 4 to each term on the RHS of (57). For the first term, we get

$$U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} [(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) \mathbb{H}] U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger = \mathbb{T}_{\mathcal{A}} \left(U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} \mathbb{H} U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger \right), \quad (58)$$

and for the second

$$\frac{1}{d^2} U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} [(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) (\Psi_k \otimes \tau)] U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger = \frac{1}{d^2} \mathbb{T}_{\mathcal{A}} (\Phi_k), \quad k = 1, \dots, d^2, \quad (59)$$

where to arrive at (59) we have used $\Phi_k = U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} (\Psi_k \otimes \tau) U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger$.

Now using (58) and (59), we can write (57) as

$$U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} \left[(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) \left(\mathbb{H} - \frac{1}{d^2} \Psi_k \otimes \tau \right) \right] U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger = \mathbb{T}_{\mathcal{A}} \left(U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} \mathbb{H} U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger - \Phi_k / d^2 \right). \quad (60)$$

Since the LHS of (60) is positive semidefinite [see (56)], the RHS must also be so, i.e.,

$$\mathbb{T}_{\mathcal{A}} \left(U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} \mathbb{H} U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger - \Phi_k / d^2 \right) \in \text{Pos}(\mathcal{A} \otimes \mathcal{B}), \quad k = 1, \dots, d^2. \quad (61)$$

Defining H as

$$H = U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2} \mathbb{H} U_{\mathcal{B}_1 \leftrightarrow \mathcal{A}_2}^\dagger \in \text{Herm}(\mathcal{A} \otimes \mathcal{B}), \quad (62)$$

(61) takes the form

$$\mathbb{T}_{\mathcal{A}} \left(H - \Phi_k / d^2 \right) \in \text{Pos}(\mathcal{A} \otimes \mathcal{B}), \quad k = 1, \dots, d^2. \quad (63)$$

Thus the feasibility condition of the dual problem is satisfied for an H defined in (62), provided the operator $(\mathbb{T}_{\mathcal{A}_1} \otimes \mathbb{T}_{\mathcal{A}_2}) \left(\mathbb{H} - \frac{1}{d^2} \Psi_k \otimes \tau \right)$ is positive semidefinite. This completes the proof.

References

- [1] A. Chefles, Quantum state discrimination, *Contemp. Phys.* **41**, 401 (2000).
- [2] S. M. Barnett and S. Croke, Quantum state discrimination, *Adv. Opt. Photon.* **1**, 238 (2009).
- [3] J. A. Bergou, Discrimination of quantum states, *Journal of Modern Optics*, **57**, 160 (2010).

- [4] J. Bae and L-C. Kwek, Quantum state discrimination and its applications, *J. Phys. A: Math. Theor.* **48**, 083001 (2015).
- [5] A. Peres and W. K. Wootters, Optimal detection of quantum information, *Phys. Rev. Lett.* **66**, 1119 (1991).
- [6] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Quantum nonlocality without entanglement, *Phys. Rev. A* **59**, 1070 (1999).
- [7] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Unextendible product bases and bound entanglement, *Phys. Rev. Lett.* **82**, 1070 (1999).
- [8] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local distinguishability of multipartite orthogonal quantum states, *Phys. Rev. Lett.* **85**, 4972 (2000).
- [9] S. Virmani, M. F. Sacchi, M. B. Plenio, D. Markham, Optimal local discrimination of two multipartite pure states, *Phys. Lett. A* **288**, 62 (2001).
- [10] S. Ghosh, G. Kar, A. Roy, A. Sen (De), and U. Sen, Distinguishability of Bell states, *Phys. Rev. Lett.* **87**, 277902 (2001).
- [11] J. Walgate and L. Hardy, Nonlocality, asymmetry, and distinguishing bipartite states, *Phys. Rev. Lett.* **89**, 147901 (2002).
- [12] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Local indistinguishability: More nonlocality with less entanglement, *Phys. Rev. Lett.* **90**, 047902 (2003).
- [13] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Unextendible product bases, uncompletable product bases and bound entanglement, *Commun. Math. Phys.* **238**, 379 (2003).
- [14] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Distinguishability of maximally entangled states, *Phys. Rev. A* **70**, 022304 (2004).
- [15] H. Fan, Distinguishability and indistinguishability by local operations and classical communication, *Phys. Rev. Lett.* **92**, 177905 (2004).
- [16] J. Watrous, Bipartite subspaces having no bases distinguishable by local operations and classical communication, *Phys. Rev. Lett.* **95**, 080505 (2005).
- [17] M. Nathanson, Distinguishing bipartite orthogonal states by LOCC: Best and worst cases, *Journal of Mathematical Physics* **46**, 062103 (2005).
- [18] W. K. Wootters, Distinguishing unentangled states with an unentangled measurement, *Int. J. Quantum Inf.* **4**, 219 (2006).
- [19] M. Hayashi, D. Markham, M. Muraio, M. Owari, and S. Virmani, Bounds on entangled orthogonal state discrimination using local operations and classical communication, *Phys. Rev. Lett.* **96**, 040501 (2006).
- [20] J. Niset and N. J. Cerf, Multipartite nonlocality without entanglement in many dimensions, *Phys. Rev. A* **74**, 052103 (2006).
- [21] R. Y. Duan, Y. Feng, Z. F. Ji, and M. S. Ying, Distinguishing arbitrary multipartite basis unambiguously using local operations and classical communication, *Phys. Rev. Lett.* **98**, 230502 (2007).
- [22] Y. Feng and Y.-Y. Shi, Characterizing locally indistinguishable orthogonal product states, *IEEE Trans. Inf. Theory* **55**, 2799 (2009).
- [23] R. Y. Duan, Y. Feng, Y. Xin, and M. S. Ying, Distinguishability of quantum states by separable operations, *IEEE Trans. Inf. Theory* **55**, 1320 (2009).
- [24] J. Calsamiglia, J. I. de Vicente, R. Muñoz-Tapia, E. Bagan, Local discrimination of mixed states, *Phys. Rev. Lett.* **105**, 080504 (2010).

- [25] S. Bandyopadhyay, S. Ghosh and G. Kar, LOCC distinguishability of unilaterally transformable quantum states, [New J. Phys. **13**, 123013 \(2011\)](#).
- [26] S. Bandyopadhyay, More nonlocality with less purity, [Phys. Rev. Lett. **106**, 210402 \(2011\)](#).
- [27] N. Yu, R. Duan, and M. Ying, Four locally indistinguishable ququad-ququad orthogonal maximally entangled states, [Phys. Rev. Lett. **109**, 020506 \(2012\)](#).
- [28] A. Cosentino, Positive-partial-transpose-indistinguishable states via semidefinite programming, [Phys. Rev. A **87**, 012321 \(2013\)](#).
- [29] A. Cosentino and V. Russo, Small sets of locally indistinguishable orthogonal maximally entangled states, [Quantum Information and Computation **14**, 1098 \(2014\)](#).
- [30] S. Bandyopadhyay and M. Nathanson, Tight bounds on the distinguishability of quantum states under separable measurements, [Phys. Rev. A **88**, 052313 \(2013\)](#).
- [31] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, Limitations on separable measurements by convex optimization, [IEEE Trans. Inf. Theory **61**, 3593 \(2015\)](#).
- [32] S. Halder, Several nonlocal sets of multipartite pure orthogonal product states, [Phys. Rev. A **98**, 022303 \(2018\)](#).
- [33] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, Strong quantum nonlocality without entanglement, [Phys. Rev. Lett. **122**, 040403 \(2019\)](#).
- [34] N. Yu, R. Duan, and M. Ying, Distinguishability of quantum states by positive operator-valued measures with positive partial transpose, [IEEE Trans. Inf. Theory **60**, 2069 \(2014\)](#).
- [35] E. Chitambar, D. Leung, L. Mancinska, M. Ozols, and A. Winter, Everything you always wanted to know about LOCC (but were afraid to ask), [Commun. Math. Phys. **328**, 303 \(2014\)](#).
- [36] M. Navascués, Pure state estimation and the characterization of entanglement, [Phys. Rev. Lett. **100**, 070503 \(2008\)](#).
- [37] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Hiding bits in Bell states, [Phys. Rev. Lett. **86**, 5807 \(2001\)](#).
- [38] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, Quantum data hiding, [IEEE Trans. Inf. Theory **48**, 580 \(2002\)](#).
- [39] T. Eggeling, and R. F. Werner, Hiding classical data in multipartite quantum states, [Phys. Rev. Lett. **89**, 097905 \(2002\)](#).
- [40] W. Matthews, S. Wehner, A. Winter, Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding, [Commun. Math. Phys. **291**, 831 \(2009\)](#).
- [41] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, [Phys. Rev. A **78**, 042309 \(2008\)](#).
- [42] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, [Rev. Mod. Phys. **81**, 865 \(2009\)](#).
- [43] S. M. Cohen, Understanding entanglement as resource: Locally distinguishing unextendible product bases, [Phys. Rev. A **77**, 012304 \(2008\)](#).
- [44] S. Bandyopadhyay, G. Brassard, S. Kimmel, and W. K. Wootters, Entanglement cost of nonlocal measurements, [Phys. Rev. A **80**, 012313 \(2009\)](#).
- [45] S. Bandyopadhyay, R. Rahaman, and W. K. Wootters, Entanglement cost of two-qubit orthogonal measurements, [J. Phys. A: Math. Theor. **43**, 455303 \(2010\)](#).

- [46] S. Bandyopadhyay, S. Halder, and M. Nathanson, Entanglement as a resource for local state discrimination in multipartite systems, [Phys. Rev. A **94**, 022311 \(2016\)](#).
- [47] S. Bandyopadhyay, S. Halder, and M. Nathanson, Optimal resource states for local state discrimination, [Phys. Rev. A **97**, 022314 \(2018\)](#).
- [48] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, [Phys. Rev. Lett. **70**, 1895 \(1993\)](#).
- [49] B. Lovitz and N. Johnston, Entangled subspaces and generic local state discrimination with pre-shared entanglement, [arXiv:2010.02876 2020](#).
- [50] S. Bandyopadhyay and V. Russo, Entanglement cost of discriminating noisy Bell states by local operations and classical communication, [Phys. Rev. A **104**, 032429 \(2021\)](#).
- [51] M. Horodecki and P. Horodecki, Reduction criterion of separability and limits for a class of distillation protocols, [Phys. Rev. A **59**, 4206 \(1999\)](#).
- [52] G. Vidal and R. F. Werner, Computable measure of entanglement, [Phys. Rev. A **65**, 032314 \(2002\)](#).