Indistinguishability of bipartite states by positive-partial-transpose operations in the many-copy scenario

Yinan Li,[1,*] Xin Wang,[1,†] and Runyao Duan[1,2,‡]

[1]*Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, New South Wales 2007, Australia*

[2]*UTS-AMSS Joint Research Laboratory for Quantum Computation and Quantum Information Processing, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China*

A bipartite subspace S is called strongly positive-partial-transpose (PPT) unextendible if for every positive integer k, there is no PPT operator supporting on the orthogonal complement of $S^{\otimes k}$. We show that a subspace is strongly PPT unextendible if it contains a PPT-definite operator (a positive semidefinite operator whose partial transpose is positive definite). Based on these, we are able to propose a simple criterion for verifying whether a set of bipartite orthogonal quantum states is indistinguishable by PPT operations in the many-copy scenario. Utilizing this criterion, we further point out that any entangled pure state and its orthogonal complement cannot be distinguished by PPT operations in the many-copy scenario. On the other hand, we investigate that the minimum dimension of strongly PPT-unextendible subspaces in an $m \otimes n$ system is $m + n - 1$, which involves a generalization of the result that non-positive-partial-transpose subspaces can be as large as any entangled subspace [N. Johnston, Phys. Rev. A **87**, 064302 (2013)].

I. INTRODUCTION

One fascinating phenomenon of quantum mechanics is the quantum nonlocality, that is, there exist some global quantum operations on a composite system that cannot be implemented by the owners of the subsystems using local operations and classical communication (LOCC) only. A general strategy to study quantum nonlocality is to consider what kind of information processing tasks cannot be achieved by LOCC. Roughly speaking, if a certain task is accomplished with different optimal global and local efficiencies, then we can construct a class of quantum operations that cannot be realized by LOCC. There is no doubt that the discrimination of orthogonal quantum states is an effective one and it has received considerable attention in the past decades. See Refs. [1–23] for a partial list.

It is well-known that orthogonal quantum states can be perfectly distinguished if globe operations are permitted. And the setup of local distinguishability of quantum states is simple: two or more spatially separated observers share a composite quantum system prepared in one of many known mutually orthogonal quantum states. Their goal is to identify the unknown states by LOCC. When we only need to distinguish two orthogonal multipartite pure states, the perfect local discrimination can always be achieved [2]. Nevertheless, if we have more than two states to distinguish, they cannot be perfectly distinguished by LOCC if one or more states are entangled [4]. This phenomenon is percipient since entanglement has been shown to ensure difficulty in state discrimination [10]. On the other hand, it has been shown that there exist sets of orthogonal product states that cannot be discriminated perfectly by LOCC [1,24,25].

However, the local indistinguishability might be overcome in the many-copy scenario, which is the case that multiple copies of quantum states are provided. A simple example would be four 2⊗2 Bell states, which can be perfectly distinguished within two copies [6], while they are indistinguishable with a single copy [5,6,8]. In fact, it has been shown that N orthogonal pure states can always be perfectly distinguished by LOCC when $N - 1$ copies of the unknown state are provided [16]. This suggests that the available copies of the unknown state play a crucial role in local distinguishability. However, it turns out that there exist two orthogonal quantum states, one of which is necessarily mixed, that are locally indistinguishable in the many-copy scenario [16]. Thus, the local indistinguishability of orthogonal quantum states is more robust in mixed states for it persists even in the domain of multiple copies, whereas in the case of pure states it does not.

Proving local indistinguishability is hard even in the bipartite case, since our knowledge about LOCC is limited. To circumvent the difficulty, one approach is to show the indistinguishability by operations that completely preserve the positivity of the partial transpose [denoted as positive-partial-transpose (PPT) operations], and local indistinguishability automatically follows since the set of all LOCC operations will also preserve the positivity of the partial transpose. The advantage of this approach is that the set of PPT operations enjoys a tractable mathematical structure. It has been shown that the bipartite maximally entangled state and the normalized projection onto its orthogonal complement cannot be distinguished by PPT operations in the many-copy scenario [26]. On the other hand, the notion of PPT plays a significant role in quantum information theory. It has been used to provide some convenient criteria for the separability of quantum states [27–29], and to study the problem of entanglement distillation, pure state transformation, and communication over quantum channels (e.g., [30–36]).

In this paper, we contribute a simple criterion for verifying indistinguishability of bipartite quantum states by PPT opera-

─────────
*yinan.li@student.uts.edu.au
†xin.wang-8@student.uts.edu.au
‡runyao.duan@uts.edu.au

tions in the many-copy scenario. This criterion is based on the observation that if the support of some state is strongly PPT unextendible, then any set of orthogonal states containing such a state cannot be distinguished by PPT operations in the many-copy scenario. Here we say a subspace S of some bipartite Hilbert space is *strongly PPT unextendible* if for any positive integer k, there is no PPT state whose support is a subspace of the orthogonal complement of $S^{\otimes k}$. And this concept is a natural generalization of the concept of *strongly unextendible subspace*, introduced in Ref. [37]. To observe strong PPT unextendibility, one evidence is the so-called PPT-definite operator, which is a positive semidefinite operator whose partial transpose is positive definite. In fact, the existence of PPT-definite operators can be observed efficiently by semidefinite programming (SDP) [38], which is a powerful tool in quantum information theory with many applications (e.g., [39–46]). As an application, we show that any entangled pure states and the normalized projector onto their orthogonal complement cannot be distinguished by PPT operations in the many-copy scenario, which is a far-reaching extension of one of the main results in Ref. [26]. Meanwhile, we show that the minimum dimension of strongly PPT-unextendible subspaces in a $m \otimes n$ system is $m + n - 1$, which extends the result on the minimum dimension of the PPT-unextendible subspace in Ref. [47].

II. PRELIMINARIES

We review some notation and definitions. In the following, we will use symbols such as $\mathcal{A}$ (or $\mathcal{A}'$) and $\mathcal{B}$ (or $\mathcal{B}'$) to denote (finite-dimensional) Hilbert spaces associated with Alice and Bob, respectively. The dimension of $\mathcal{A}$ and $\mathcal{B}$ are denoted by $d_\mathcal{A}$ and $d_\mathcal{B}$. We say two subspaces S_1 and S_2 of some Hilbert space are orthogonal, denoted by $S_1 \perp S_2$, if for any $|\psi_1\rangle \in S_1$ and $|\psi_2\rangle \in S_2$, $\langle\psi_1|\psi_2\rangle = 0$. The orthogonal complement of a subspace S is denoted by $S^\perp = \{|\psi\rangle : \langle\psi|\phi\rangle = 0, \forall |\phi\rangle \in S\}$. The space of all linear operators over $\mathcal{A}$ is denoted by $\mathcal{L}(\mathcal{A})$. For convenience, we use $\lambda_{\max}(X)$ and $\lambda_{\min}(X)$ to denote the maximum eigenvalue and the minimum eigenvalue of some operator $X \in \mathcal{L}(\mathcal{A})$. A quantum state is characterized by its density operator $\rho \in \mathcal{L}(\mathcal{A})$, which is a positive semidefinite operator with trace unity. The support of ρ, denoted by supp(ρ), is defined to be the space spanned by the eigenvectors of ρ with positive eigenvalues. We say a positive semidefinite operator X is supporting on some subspace S of $\mathcal{A}$, if supp(X) is a subspace of S.

A bipartite positive semidefinite operator $E_{AB} \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$ is said to be PPT if $E_{AB}^{T_B}$ is positive semidefinite, where the action of partial transpose (with respect to B) is defined as $(|i_A\rangle\langle k_A| \otimes |j_B\rangle\langle l_B|)^{T_B} = |i_A\rangle\langle k_A| \otimes |l_B\rangle\langle j_B|$. Moreover, a PPT operator $E_{AB} \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$ is said to be *PPT-definite* if $E_{AB}^{T_B}$ is positive definite.

In this paper, the PPT operations used for distinguishing a set of n orthogonal quantum states $\{\rho_1, \ldots, \rho_n\}$ can be defined as an n-tuple of operators, $(M_k)_{k=1,\ldots,n}$, where $M_k \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$ is PPT for $k = 1, \ldots, n$ and $\sum_{k=1}^n M_k = \mathbb{1}_{\mathcal{A} \otimes \mathcal{B}}$. Then $\{\rho_1, \ldots, \rho_n\}$ is said to be:

(i) *Perfectly distinguishable by PPT operations*, if there exist $(M_k)_{k=1,\ldots,n}$, where $M_k \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$ is PPT for $k = 1, \ldots, n$ and $\sum_{k=1}^n M_k = \mathbb{1}_{\mathcal{A} \otimes \mathcal{B}}$, such that Tr($M_i \rho_j$) = δ_{ij}, for any $1 \leqslant i, j \leqslant n$.

(ii) *Unambiguously distinguishable by PPT operations*, if there exist $(M_k)_{k=1,\ldots,n}$, where $M_k \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$ is PPT for $k = 1, \ldots, n$ and $\sum_{k=1}^n M_k = \mathbb{1}_{\mathcal{A} \otimes \mathcal{B}}$, such that Tr($M_i \rho_j$) = $p_i \delta_{ij}, p_i > 0$ for any $1 \leqslant i, j \leqslant n$.

(iii) *Indistinguishable by PPT operations*, if it is not unambiguously distinguishable by PPT operation.

These definitions can be naturally generalized when multiple copies are provided. In addition, we would say a set of orthogonal quantum states $\{\rho_1, \ldots, \rho_n\}$ is indistinguishable by PPT operations in the many-copy scenario, if for any positive integer k, $\{\rho_1^{\otimes k}, \ldots, \rho_n^{\otimes k}\}$ is indistinguishable by PPT operations.

In the end, we say a bipartite subspace S of $\mathcal{A} \otimes \mathcal{B}$ is PPT extendible, if there exists a PPT operator $\sigma \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$, such that σ is supporting on the orthogonal complement of S. S is said to be PPT unextendible if it is not PPT extendible, and to be strongly PPT unextendible if for any positive integer k, $S^{\otimes k}$ is not PPT extendible.

III. MAIN RESULTS

A. Indistinguishability by PPT operations

The main result of this paper is a sufficient criterion for verifying the PPT indistinguishability of orthogonal quantum states:

Theorem 1. For a set of orthogonal bipartite quantum states $\{\rho_1, \ldots, \rho_n\}$, if there is a PPT-definite operator supporting on the support of some ρ_k, then $\{\rho_1, \ldots, \rho_n\}$ is indistinguishable by PPT operations in the many-copy scenario.

To prove this theorem, we first show the following lemma.

Lemma 2. For a set of orthogonal quantum states $\{\rho_1, \ldots, \rho_n\}$, if there exists $k \in \{1, \ldots, n\}$ such that supp(ρ_k) is strongly PPT unextendible, then S is indistinguishable by PPT operations in the many-copy scenario.

Proof. Without loss of generality, we assume supp(ρ_1) is strongly PPT unextendible. If there exists some positive integer m such that $\{\rho_1^{\otimes m}, \ldots, \rho_n^{\otimes m}\}$ can be unambiguously distinguished by PPT operations, there exists a tuple of PPT operators $(M_k)_{k=1,\ldots,n}$ such that

$$\text{Tr}\left(M_k P_j^{\otimes m}\right) = p_k \delta_{kj}, \quad p_k > 0, \quad j = 1, \ldots, m,$$

where P_j is the projection onto supp($\rho_j^{\otimes m}$) for any $1 \leqslant j \leqslant n$ and $p_k > 0$ for any $1 \leqslant k \leqslant n$. Notice that $M_k(k \geqslant 2)$ will support on the orthogonal complement of supp($\rho_1^{\otimes m}$), which is a contradiction.

Now, it is sufficient to show that the property of being strongly PPT unextendible can be observed by a PPT-definite operator:

Lemma 3. Given a bipartite subspace S of $\mathcal{A} \otimes \mathcal{B}$, if there is a PPT-definite operator σ supporting on S, then S is strongly PPT unextendible.

Proof. Assume that there exists k such that $S^{\otimes k}$ is PPT extendible and $\rho \in \mathcal{L}(\mathcal{A}^{\otimes k} \otimes \mathcal{B}^{\otimes k})$ is the PPT operator supporting on the orthogonal complement of $S^{\otimes k}$. We will show

$$\text{Tr}(\sigma^{\otimes k} \rho) = \text{Tr}[(\sigma^{\otimes k})^{T_B} \rho^{T_B}] > 0, \tag{1}$$

which is a contradiction since supp($\sigma^{\otimes k}$) is still a subspace of supp($S^{\otimes k}$). To see this, one only need to observe that $\sigma^{\otimes k}$

is also PPT-definite. In general, let P be the projection onto supp(σ) for some state σ, then supp(σ) contains a PPT-definite state if and only if $T(\sigma) > 0$, where

$$
\begin{aligned}
T(\sigma) &= \max t, \\
\text{s.t. } 0 &\leqslant R \leqslant P, \quad R^{T_B} \geqslant t\mathbb{1}.
\end{aligned}
\tag{2}
$$

Actually, the function $T(\cdot)$ is supermultiplicative, i.e.,

$$
T(\sigma_1 \otimes \sigma_2) \geqslant T(\sigma_1)T(\sigma_2).
$$

To prove this, we can assume that the optimal solutions to SDP (2) of $T(\sigma_1)$ and $T(\sigma_2)$ are $\{R_1, t_1\}$ and $\{R_2, t_2\}$, respectively. It is clear that $0 \leqslant R_1 \otimes R_2 \leqslant P_1 \otimes P_2$ and $R_1^{T_{B_1}} \otimes R_2^{T_{B_2}} \geqslant t_1 t_2 \mathbb{1}$. Then $\{R_1 \otimes R_2, t_1 t_2\}$ is a feasible solution to SDP (2) of $T(\sigma_1 \otimes \sigma_2)$, which means that $T(\sigma_1 \otimes \sigma_2) \geqslant t_1 t_2 > 0$. It follows that supp($\sigma^{\otimes n}$) contains a PPT-definite state when $T(\sigma) > 0$, since $T(\sigma^{\otimes n}) \geqslant T(\sigma)^n > 0$. ∎

The proof of Theorem 1 is then straightforward. If there is a PPT-definite operator supporting on the support of some ρ_k, by Lemma 3, supp(ρ_k) is strongly PPT unextendible; Then by Lemma 2, $\{\rho_1, \ldots, \rho_n\}$ is PPT indistinguishable in the many-copy scenario. ∎

B. Examples of sets of quantum states which are PPT indistinguishable in the many-copy scenario

To see the power of our theorem, we apply it to extend the result of Ref. [26], which showed that the bipartite maximally entangled state and the normalized projection onto its orthogonal complement are PPT indistinguishable in the many-copy scenario. In fact, our proof illustrates that the restriction to a maximally entangled state can be removed.

Theorem 4. Given any *entangled* state $|\phi\rangle \in \mathcal{A} \otimes \mathcal{B}$ with $d_\mathcal{A} = d_\mathcal{B} = d$, let $\rho = \frac{1}{d^2-1}(\mathbb{1}_{\mathcal{A} \otimes \mathcal{B}} - |\phi\rangle\langle\phi|)$ be the normalized projection onto its orthogonal complement. Then $|\phi\rangle\langle\phi|$ and ρ are PPT indistinguishable in the many-copy scenario.

Proof. It is easy to see that $\lambda_{\min}((\mathbb{1} - |\phi\rangle\langle\phi|)^{T_B}) > 0$ is equivalent to $\lambda_{\max}(|\phi\rangle\langle\phi|^{T_B}) < 1$. Suppose that the Schmidt rank of $|\phi\rangle$ is $m (> 1)$, and the Schmidt decomposition of $|\phi\rangle$ is $|\phi\rangle = \sum_{i=1}^m \lambda_i |ii\rangle$ with $\lambda_1^2 \geqslant \cdots \geqslant \lambda_m^2$ and $\sum_{i=1}^m \lambda_i^2 = 1$. The partial transposition (with respect to $\mathcal{B}$) of $|\phi\rangle\langle\phi|$ is

$$
\begin{aligned}
|\phi\rangle\langle\phi|^{T_B} &= \sum_{i=1}^m \lambda_i^2 |ii\rangle\langle ii| + \sum_{i \neq j} \lambda_i \lambda_j |ji\rangle\langle ij| \\
&= \sum_{i=1}^m \lambda_i^2 |ii\rangle\langle ii| + \sum_{i>j} \frac{\lambda_i \lambda_j}{2}[(|ij\rangle + |ji\rangle) \\
&\quad \times (\langle ij| + \langle ji|) + (|ij\rangle - |ji\rangle)(\langle ij| - \langle ji|)].
\end{aligned}
\tag{3}
$$

This shows that $\lambda_{\max}(|\phi\rangle\langle\phi|^{T_B}) = \lambda_1^2 < 1$. Therefore, $(\mathbb{1} - |\phi\rangle\langle\phi|)^{T_B}$ is positive definite and the result follows directly from Theorem 1. ∎

On the other hand, it is also interesting to construct sets of PPT-indistinguishable orthogonal quantum states in the many-copy scenario without invoking the technique of unextendible product bases (UPBs) [1]. Utilizing Theorem 1, we exhibit one simple example as follows:

Example 1. Let $d_\mathcal{A} = d_\mathcal{B} = d$. Choose a set of orthogonal bases $\{|\phi_1\rangle, \ldots, |\phi_{d^2}\rangle\}$ of $\mathcal{A} \otimes \mathcal{B}$, such that $|\phi_i\rangle$ is maximally

entangled for any $i = 1, \ldots, d^2$. For any positive integer $d^2 - d + 1 \leqslant m \leqslant d^2$ and any $k = 2, \ldots, d^2 - m + 1$, we can construct $\{\rho_i : i = 1, \ldots, k\}$ which is PPT indistinguishable in the many-copy scenario.

Proof. We first show that the projection P onto the subspace span$\{|\phi_1\rangle, \ldots, |\phi_m\rangle\}$ is PPT-definite. Notice that $P = \mathbb{1}_{d^2} - \sum_{i=m+1}^{d^2} |\phi_i\rangle\langle\phi_i|$, then

$$
\lambda_{\min}(P^{T_B}) = 1 - \lambda_{\max}\left(\sum_{i=m+1}^{d^2} |\phi_i\rangle\langle\phi_i|^{T_B}\right)
\tag{4}
$$

$$
\geqslant 1 - \sum_{i=m+1}^{d^2} \lambda_{\max}(|\phi_i\rangle\langle\phi_i|^{T_B})
\tag{5}
$$

$$
\geqslant 1 - \frac{d^2 - m}{d} \geqslant \frac{1}{d} > 0,
\tag{6}
$$

where Eq. (6) uses the fact that $\lambda_{\max}(|\phi_i\rangle\langle\phi_i|^{T_B}) = 1/d$.

Then $\{\rho_1, \ldots, \rho_k\}$ can be chosen as

$$
\begin{aligned}
\rho_1 &= \frac{1}{m} \sum_{i=1}^m |\phi_i\rangle\langle\phi_i|, \\
\rho_2 &= |\phi_{m+1}\rangle\langle\phi_{m+1}|, \\
&\cdots \\
\rho_k &= |\phi_{m+k-1}\rangle\langle\phi_{m+k-1}|,
\end{aligned}
$$

where $k \leqslant d^2 - m + 1$. ∎

Remark. For a general set of pure states $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$, we suppose λ_i is the largest Schmidt coefficient of $|\psi_i\rangle$. We can use a similar technique to show that if $\sum_{i=1}^m \lambda_i < 1$, then any set of states $\{\rho_1, \ldots, \rho_k\}$ with $\rho_1 = \frac{1}{m} \sum_{i=1}^n |\psi_i\rangle\langle\psi_i|$ is PPT indistinguishable in the many-copy scenario.

C. Minimum dimension of strongly PPT-unextendible subspace

It is of great interest to connect PPT distinguishability with other concepts in quantum information theory, and there is no doubt that Lemma 2 provides one. The notion of strongly PPT unextendible subspace is a natural generalization of strongly unextendible subspace, while the latter has been shown widely useful in quantum information theory. For instance, it has been shown in Ref. [48] that the minimum dimension of such a subspace is $d_\mathcal{A} + d_\mathcal{B} - 1$, and this result has been applied to show the superactivation of the asymptotic zero-error classical capacity of a quantum channel [37,49]. Since there is also no product state in the orthogonal complement of PPT-unextendible subspaces, the minimum dimension of the strongly PPT-unextendible subspace is at least $d_\mathcal{A} + d_\mathcal{B} - 1$. In Ref. [47], a PPT-unextendible subspace of dimension $d_\mathcal{A} + d_\mathcal{B} - 1$ has been explicitly constructed [47]. To be specific, this subspace is the orthogonal complement of

$$
\begin{aligned}
S = \text{span}\{&|j\rangle|k+1\rangle - |j+1\rangle|k\rangle : 0 \leqslant j \\
&\leqslant d_\mathcal{A} - 2, 0 \leqslant k \leqslant d_\mathcal{B} - 2\}.
\end{aligned}
$$

Using Lemma 3, we show that the subspace $S^\perp$ is actually strongly PPT unextendible, which illustrates that the minimum dimension of strongly PPT-unextendible subspaces in $\mathcal{A} \otimes \mathcal{B}$ is also $d_\mathcal{A} + d_\mathcal{B} - 1$.

Theorem 5. Let $d_A = m$, $d_B = n$ satisfying $2 \leqslant m \leqslant n$, and S is defined as above. Then $S^\perp$ is strongly PPT unextendible.

Proof. Denote $S^\perp$ by S_{mn} with respect to the dimension of $\mathcal{A}$ and $\mathcal{B}$. S_{mn} can be written in the following form:

$$S_{mn} = \text{span}\left\{ |\psi_s\rangle = \sum_{j=0}^{m-1-s} |j\rangle|m-1-s-j\rangle : s = 0,\ldots,m-1; |\phi_t\rangle = \sum_{j=t-m+1}^{\min\{n-1,t\}} |t-j\rangle|j\rangle : t = m,\ldots,m+n-2 \right\}.$$

We claim that there exist positive real numbers $x_0, x_1, \ldots, x_{m-1}, y_m, \ldots, y_{m+n-2}$ such that

$$\rho_{mn} = \sum_{s=0}^{m-1} x_{m-1-s} |\psi_s\rangle\langle\psi_s| + \sum_{t=m}^{m+n-2} y_t |\phi_t\rangle\langle\phi_t| \tag{7}$$

is PPT definite. Notice that

$$|\psi_s\rangle\langle\psi_s|^{T_B} = \sum_{j_1,j_2=0}^{n-1-s} |j_1\rangle\langle j_2| \otimes |m-1-s-j_2\rangle\langle m-1-s-j_1|,$$

$$|\phi_t\rangle\langle\phi_t|^{T_B} = \sum_{j_1,j_2=t-m+1}^{\min\{n-1,t\}} |t-j_1\rangle\langle t-j_2| \otimes |j_2\rangle\langle j_1|. \tag{8}$$

We consider the matrix form of $\rho_{mn}^{T_B}$ under the computational basis. Divide $\{|jk\rangle : j = 0,\ldots,m-1, k = 0,\ldots,n-1\}$ into the following families:

$$\mathcal{P}_a = \{|m-1-a+t\rangle|t\rangle : 0 \leqslant t \leqslant a\}a = 0,\ldots,m-1;$$

$$\mathcal{Q}_b = \{|r\rangle|r+b\rangle : 0 \leqslant r \leqslant \min\{n-1-b,m-1\}\}b = 1,\ldots,n-1. \tag{9}$$

The submatrices with respect to bases $\mathcal{P}_a$ and $\mathcal{Q}_b$ are denoted by P_a and Q_b. More precisely, P_a and Q_b have the following form:

$$P_a = \begin{pmatrix} x_a & x_{a-1} & \cdots & x_0 \\ x_{a-1} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & y_m \\ \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ x_0 & y_m & \cdots & y_{m+a-1} \end{pmatrix}_{(a+1)\times(a+1)} \quad 0 \leqslant a \leqslant m-1,$$

$$Q_b = \begin{pmatrix} x_{m-1-b} & \cdots & x_0 & y_m & \cdots & y_{m+b-1} \\ \vdots & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ x_0 & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ y_m & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ \vdots & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ y_{m+b-1} & \cdots & \cdots & \cdots & \cdots & y_{2m+b-2} \end{pmatrix}_{(m)\times(m)} \quad 1 \leqslant b \leqslant n-m,$$

$$Q_b = \begin{pmatrix} x_{m-1-b} & \cdots & x_0 & y_m & \cdots & y_{n-1} \\ \vdots & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ x_0 & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ y_m & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ \vdots & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ y_{n-1} & \cdots & \cdots & \cdots & \cdots & y_{2n-b-2} \end{pmatrix}_{(n-b)\times(n-b)} \quad b > n-m. \tag{10}$$

Then we have

$$\rho_{mn}^{T_B} = \left(\oplus_{a=0}^{m-1} P_a \right) \oplus \left(\oplus_{b=1}^{n-1} Q_b \right).$$

To make sure that $\rho_{mn}^{T_B}$ is positive definite, it is equivalent to make sure that P_a and Q_b are positive definite for $a = 0,\ldots,m-1$ and $b = 1\ldots,n-1$.

The case $m = n = 2$ is easy to verify. Notice that $S_{22} = \text{span}\{|00\rangle, |01\rangle + |10\rangle, |11\rangle\}$ and we can easily choose an operator $\rho = 2(|00\rangle\langle00| + |11\rangle\langle11|) + (|01\rangle + |10\rangle)(\langle01| + \langle10|)$ which is PPT definite.

We first consider $m = n$ and prove it by mathematical induction. Specifically, if $\rho_{mm}^{T_B}$ is positive definite, then we can construct $\rho_{m+1m+1}^{T_B}$ which is also positive definite. Notice

that when $m = n$, we can assume $x_a = y_{m-1+a}$, then we have $P_a = Q_{m-1-a}$ for $a = 0,\ldots,m-2$ and $\rho_{mm}^{T_B} = P_{m-1} \oplus [\oplus_{k=0}^{m-2}(P_k \oplus Q_{m-1-k})]$. Since $\rho_{mm}^{T_B}$ is positive definite, there exist positive $x_0,\ldots,x_{m-1}$ such that

$$P_k = \begin{pmatrix} x_k & x_{k-1} & \cdots & x_0 \\ x_{k-1} & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & x_1 \\ \vdots & \cdot^{\cdot^\cdot} & \cdot^{\cdot^\cdot} & \vdots \\ x_0 & x_1 & \cdots & x_k \end{pmatrix}_{(k+1)\times(k+1)}$$

is positive definite for $k = 0, \ldots, m-1$. For $\rho^{T_B}_{(m+1)(m+1)}$, we want to find $x'_0, \ldots, x'_m$ such that

$$P'_k = \begin{pmatrix} x'_k & x'_{k-1} & \cdots & x'_0 \\ x'_{k-1} & \ddots & \ddots & x'_1 \\ \vdots & \ddots & \ddots & \vdots \\ x'_0 & x'_1 & \cdots & x'_k \end{pmatrix}_{(k+1)\times(k+1)} > 0$$

for $k = 0, \ldots, m$. Let $x'_k = x_k$ for $k = 0, \ldots, m-1$, then $P'_k > 0$ can be guaranteed. We only need to find a positive x'_m such that

$$P'_m = \begin{pmatrix} x'_m & x_{m-1} & \cdots & x_0 \\ x_{m-1} & \ddots & \ddots & x_1 \\ \vdots & \ddots & \ddots & \vdots \\ x_0 & x_1 & \cdots & x'_m \end{pmatrix}_{(m+1)\times(m+1)}$$

is positive definite. Notice that we only need to show the leading principal minors of P'_m are all positive definite. Thus we have $m-1$ linear constraints and a quadratic constraint on variable x'_m. For all linear constraints, the coefficients of x'_m are positive, which can be easily derived since P'_k are positive definite for $k = 1, \ldots, m-1$. Moreover, the coefficient of $(x'_m)^2$ in the quadratic constraint is also positive since the following matrix

$$\begin{pmatrix} x_{m-2} & \cdots & x_1 & x_0 \\ \vdots & \ddots & x_0 & x_1 \\ x_1 & \ddots & \ddots & \vdots \\ x_0 & x_1 & \cdots & x_{m-2} \end{pmatrix}$$

is also positive definite. It is then straightforward to see that feasible solutions always exist. Thus we can choose one to make sure $\rho^{T_B}_{(m+1)(m+1)}$ is positive definite.

Finally, we extend to the case $m \neq n$ by a similar technique. Assume we have already known $x'_0, \ldots, x'_{m-1}$ such that ρ_{mm} is PPT-definite. For ρ_{mn} where $n > m$, we are going to find $x_0, \ldots, x_{m-1}$ and $y_m, \ldots, y_{m+n-2}$ such that ρ_{mn} is PPT-definite too. Let $x_i = x'_i$ for $i = 0, \ldots, m-1$ and $y_{m+j} = x_{j+1}$ for $j = 0, \ldots, m-2$. These guarantee that P_a in Eq. (10) is

positive definite for $a = 0, \ldots, m-1$. Then we consider Q_b, where $b = 1 \ldots, n-m$. When $b = 1$, we only need to determine y_{2m-1} such that $y_{2m-1} > 0$ and Q_1 is positive definite. This can be done by only guaranteeing the determinant of Q_b is always positive, which is a linear constraint for y_{2m-1}. This is true since the first $m-1$ leading principle minors of Q_1 are leading principle minors of P_{m-2}, which is automatically positive. Then we can determine $y_{2m-2}, \ldots, y_{m+n-2}$ with the same technique. Finally, we show that Q_b is positive definite for $b = n-m+1, \ldots, n-1$. In fact, this is the $(m-1)$th leading principle minor of some Q_{n-m-2}, which is positive definite. This concludes our proof. ∎

IV. CONCLUSIONS AND DISCUSSIONS

In summary, we study the indistinguishability of bipartite quantum states by PPT operations in the many-copy scenario. By introducing the concept of a strongly PPT-unextendible subspace, we show that such subspace plays a crucial role in determining PPT indistinguishability in the many-copy scenario. Connected by that, we show that the PPT-definite operators can be served as evidence of the PPT indistinguishability. And this evidence can be formalized as a semidefinite program, which can be checked efficiently [50].

We then apply our result to demonstrate that any entangled pure state and the normalized projector onto its orthogonal complement is PPT indistinguishable in the many-copy scenario. This provides a simpler and more general proof than that in Ref. [26]. On the other hand, we apply our results to show that the minimum dimension of strongly PPT-unextendible subspaces in an $m \otimes n$ quantum system is $m + n - 1$. This coincides with the minimum dimension of unextendible subspace [48] and involves an extension of the result that non-PPT subspaces can be as large as any entangled subspace in Ref. [47].

[1] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).

[2] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).

[3] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).

[4] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).

[5] H. Fan, Phys. Rev. Lett. **92**, 177905 (2004).

[6] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Phys. Rev. A **70**, 022304 (2004).

[7] S. De Rinaldis, Phys. Rev. A **70**, 022309 (2004).

[8] M. Nathanson, J. Math. Phys. **46**, 62103 (2005).

[9] J. Watrous, Phys. Rev. Lett. **95**, 080505 (2005).

[10] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, Phys. Rev. Lett. **96**, 040501 (2006).

[11] M. Owari and M. Hayashi, Phys. Rev. A **74**, 032108 (2006).

[12] R. Duan, Y. Feng, Z. Ji, and M. Ying, Phys. Rev. Lett. **98**, 230502 (2007).

[13] Y. Feng and Y. Shi, IEEE Trans. Inf. Theory **55**, 2799 (2009).

[14] N. Yu, R. Duan, and M. Ying, Phys. Rev. A **84**, 012304 (2011).

[15] S. Bandyopadhyay, S. Ghosh, and G. Kar, New J. Phys. **13**, 123013 (2011).

[16] S. Bandyopadhyay, Phys. Rev. Lett. **106**, 210402 (2011).

[17] N. Yu, R. Duan, and M. Ying, Phys. Rev. Lett. **109**, 020506 (2012).

[18] C. Lancien and A. Winter, Commun. Math. Phys. **323**, 555 (2013).

[19] E. Chitambar, R. Duan, and M.-H. Hsieh, IEEE Trans. Inf. Theory **60**, 1549 (2014).

[20] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, IEEE Trans. Inf. Theory **61**, 3593 (2014).

[21] A. Cosentino, Phys. Rev. A **87**, 012321 (2013).

[22] S. Bandyopadhyay and J. Walgate, J. Phys. A **42**, 072002 (2009).

[23] A. Chefles, Phys. Rev. A **69**, 050307 (2004).

[24] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).

[25] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Commun. Math. Phys. **238**, 379 (2003).

[26] N. Yu, R. Duan, and M. Ying, IEEE Trans. Inf. Theory **60**, 2069 (2014).

[27] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[28] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[29] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[30] E. M. Rains, IEEE Trans. Inf. Theory **47**, 2921 (2001).

[31] X. Wang and R. Duan, arXiv:1605.00348.

[32] X. Wang and R. Duan, Phys. Rev. A **94**, 050301 (2016).

[33] S. Ishizaka, Phys. Rev. Lett. **93**, 190501 (2004).

[34] W. Matthews and A. Winter, Phys. Rev. A **78**, 012317 (2008).

[35] D. Leung and W. Matthews, IEEE Trans. Inf. Theory **61**, 4486 (2015).

[36] X. Wang, W. Xie, and R. Duan, arXiv:1610.06381.

[37] T. S. Cubitt, J. Chen, and A. W. Harrow, IEEE Trans. Inf. Theory **57**, 8114 (2011).

[38] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).

[39] M. Piani and J. Watrous, Phys. Rev. Lett. **114**, 060404 (2015).

[40] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous, J. ACM **58**, 30 (2011).

[41] X. Wang and R. Duan, in *IEEE International Symposium on Information Theory (ISIT), 2016* (IEEE, 2016), pp. 1690–1694.

[42] R. Duan and A. Winter, IEEE Trans. Inf. Theory **62**, 891 (2016).

[43] P. Skrzypczyk, M. Navascues, and D. Cavalcanti, Phys. Rev. Lett. **112**, 180404 (2014).

[44] X. Wang and R. Duan, arXiv:1606.09421.

[45] M. Berta, O. Fawzi, and V. B. Scholz, SIAM J. Optim. **26**, 1529 (2016).

[46] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).

[47] N. Johnston, Phys. Rev. A **87**, 064302 (2013).

[48] T. Cubitt, A. Montanaro, and A. Winter, J. Math. Phys. **49**, 022107 (2008).

[49] R. Duan, arXiv:0906.2527.

[50] L. G. Khachiyan, USSR Comput. Math. Math. Phys. **20**, 53 (1980).