Positive-partial-transpose-indistinguishable states via semidefinite programming

Alessandro Cosentino[*]

Institute for Quantum Computing and School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada
(Received 1 November 2012; published 18 January 2013)

We present a simple semidefinite program whose optimal value is equal to the maximum probability of perfectly distinguishing orthogonal maximally entangled states using any PPT measurement (a measurement whose operators are positive under partial transpose). When the states to be distinguished are given by the tensor product of Bell states, the semidefinite program simplifies to a linear program. In Phys. Rev. Lett. **109**, 020506 (2012), Yu, Duan, and Ying exhibit a set of four maximally entangled states in $\mathbb{C}^4 \otimes \mathbb{C}^4$, which is distinguishable by any PPT measurement only with probability strictly less than 1. Using semidefinite programming, we show a tight bound of 7/8 on this probability (3/4 for the case of unambiguous PPT measurements). We generalize this result by demonstrating a simple construction of a set of k states in $\mathbb{C}^k \otimes \mathbb{C}^k$ with the same property, for any k that is a power of 2. By running numerical experiments, we show the local indistinguishability of certain sets of generalized Bell states in $\mathbb{C}^5 \otimes \mathbb{C}^5$ and $\mathbb{C}^6 \otimes \mathbb{C}^6$ previously considered in the literature.

PACS number(s): 03.67.−a

I. INTRODUCTION

A subject of much interest in quantum information theory is understanding the powers and limitations of the set of quantum operations and measurements defined within the paradigm of local operations and classical communication (LOCC). This is aimed at a more general understanding of the role of entanglement and nonlocality in quantum information.

The challenge of distinguishing certain sets of pure states is one of the most basic problems among those used to test what can and cannot be achieved using LOCC protocols. We will consider this problem in the bipartite case, for which the setup is very simple. Suppose that Alice and Bob are given a shared quantum state, drawn with some probability from a set of orthogonal states of which they have full knowledge. Their goal is to determine which state is given. We could consider variants of this problem, according to how much error we allow, but we will only investigate the case of *perfect distinguishability*, where no error is allowed. The question in which we are interested is as follows: For what sets of states are Alice and Bob able to perfectly achieve their goal by performing only LOCC protocols? The sets we consider contain only mutually orthogonal states, so the restriction of allowing only LOCC protocols is important. If global operations were permitted, Alice and Bob could obviously distinguish the states with no error.

A fundamental result in this area is by Walgate *et al.* [1], who established that any two orthogonal pure states can be locally distinguished with no error. This result has been extended to the case of three maximally entangled states when Alice and Bob's systems are three-dimensional [2]. Both these results show a surprising power of LOCC protocols. On the other hand, there exist examples of larger sets that are not perfectly distinguishable if we limit the allowed operations to the LOCC framework. In fact, if both Alice and Bob hold d-dimensional systems, it is impossible for them to locally distinguish *any* $k > d$ maximally entangled states [3]. It is important to observe that entanglement is not an essential

feature of indistinguishable sets of states. For instance, Bennett *et al.* [4] showed a set containing only product states that cannot be perfectly distinguished by LOCC protocols.

It is natural to ask what is the upper bound on the number of states that can be perfectly distinguishable by LOCC measurements. If Alice and Bob's systems are d-dimensional, is it always possible to locally distinguish a set of $k \leqslant d$ orthogonal states? If we allow product states to be in the set, we can easily construct indistinguishable sets with a fixed size in any dimension we like by using the result in [3]. However, the question becomes interesting when we consider sets consisting only of maximally entangled states. In some sense, entanglement makes distinguishability harder, but it can also be used as a resource by the two parties. For $d \leqslant 3$, the above-mentioned results by Walgate *et al.* [1] and Nathanson [2] give a positive answer to the question. For $d \geqslant 4$, the problem is not yet as well understood. Fan [5] showed that when d is prime, any k orthogonal maximally entangled states can be perfectly distinguished if $k(k-1) \leqslant 2d$. Recently, Bandyopadhyay *et al.* [6] gave examples of sets of $k \leqslant d$ maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ for $d = 4,5,6$ that are not perfectly distinguishable by *one-way* LOCC protocols. Interestingly, for $d = 5$ and 6, they showed sets of size $d - 1$. In another recent result, Yu *et al.* [7] gave an example of a set of four maximally entangled states in $\mathbb{C}^4 \otimes \mathbb{C}^4$ that cannot be perfectly distinguished by positive partial transpose operations (PPT operations). PPT operations form a superset (in fact, a strict superset) of *separable* operations, which, in turn, form a strict superset of LOCC operations. Therefore, any upper bound on the power of PPT operations for achieving a particular task holds also against LOCC operations. The partial transpose mapping has an interesting relationship to entanglement and distillation, with the Peres-Horodecki criterion being the most renowned application of this relationship. Moreover, the structure of the set of PPT operations is mathematically simpler than the one of LOCC operations, and many problems are easier to handle when we consider PPT rather than LOCC. In fact, the set of positive-partial-transpose operators form a closed convex cone, and many problems concerning them can be studied by using semidefinite programming; e.g., see [8]. Yu *et al.* [7] also noticed that the above-mentioned result about the

indistinguishability of any set of $k > d$ states [3] holds even if we broaden the set of allowed operations to PPT.

In this paper, we show how the success probability of distinguishing a set of states by using PPT measurements can be expressed as the solution of a semidefinite program. A consequence of this is a simpler proof using semidefinite duality that the set given in [7] is not perfectly distinguishable by PPT measurements. In particular, we show a tight bound of 7/8 on the probability of success. We generalize this result by showing an easy construction of sets with the same properties for the case in which $k = d$ is any power of 2. Another consequence of expressing the problem as a semidefinite program is that for small dimensions we can find the optimal solution by running a semidefinite programming solver. By doing that, we find that the PPT approach cannot be used to prove that the sets mentioned by Bandyopadhyay *et al.* in [6] are not perfectly distinguishable by LOCC measurements. Recall that they only prove the impossibility of perfectly distinguishing them by one-way LOCC protocols. On the other hand, again by numerical calculation, we find examples of local indistinguishable sets of nontrivial size, whose states lie in systems of the same dimensions as the ones in [6]. In particular, these sets were considered in [3], where they were shown to be not distinguishable by teleportation protocols, a subset of LOCC protocols.

We conclude the paper with a section about unambiguous PPT discrimination. Again, we formulate the problem as a semidefinite program and we show a bound of 3/4 on the success probability of distinguishing the set given in [7], when we restrict the strategy to be unambiguous.

II. PRELIMINARIES

Throughout this paper, we will use notation and terminology that, for the most part, is standard in quantum information theory. All vector spaces discussed are assumed to be complex Euclidean spaces. We write $\mathrm{Lin}(\mathcal{X}, \mathcal{Y})$ to denote the space of linear mappings from a space $\mathcal{X}$ to a space $\mathcal{Y}$, and we write $\mathrm{Lin}(\mathcal{X})$ as shorthand for $\mathrm{Lin}(\mathcal{X}, \mathcal{X})$. For any space $\mathcal{X}$, we write $\mathrm{Herm}(\mathcal{X})$, $\mathrm{Pos}(\mathcal{X})$, $\mathrm{Den}(\mathcal{X})$, and $\mathrm{U}(\mathcal{X})$ to denote the sets of all Hermitian operators, positive-semidefinite operators, density operators, and unitary operators on $\mathcal{X}$, respectively. The identity operator acting on a given space $\mathcal{X}$ is denoted by $\mathbf{1}_{\mathcal{X}}$, or just $\mathbf{1}$ when $\mathcal{X}$ is implicit. For Hermitian operators $A, B \in \mathrm{Herm}(\mathcal{X})$, the notations $A \geqslant B$ and $B \leqslant A$ indicate that $A - B$ is positive semidefinite. When we refer to a channel, we mean a completely positive, trace-preserving linear mapping of the form

$$\Phi : \mathrm{Lin}(\mathcal{X}) \to \mathrm{Lin}(\mathcal{Y}).$$

The *transpose* mapping $\mathcal{T} : \mathrm{Lin}(\mathcal{X}) \to \mathrm{Lin}(\mathcal{X})$ is the positive (non-completely-positive) mapping defined as $\mathcal{T}(X) = X^{\mathsf{T}}$ for all $X \in \mathrm{Lin}(\mathcal{X})$. In this definition and implicitly in the rest of the paper, we use the correspondence between linear operators and matrices with respect to the standard basis. In this correspondence, X^{T} denotes the operator associated with the matrix that is obtained by transposing the matrix representation of X. The *partial transpose* on $\mathcal{X} \otimes \mathcal{Y}$ is the mapping defined by tensoring the transpose mapping acting on

$\mathcal{X}$ and the identity mapping acting on $\mathcal{Y}$, and it is denoted as

$$\mathcal{T}_{\mathcal{X}} = \mathcal{T} \otimes \mathbf{1}_{\mathrm{Lin}(\mathcal{Y})}.$$

Positive operators that remain positive under the action of partial transposition are called *PPT operators*. We write $\mathrm{PPT}(\mathcal{X} : \mathcal{Y})$ to denote the set of all PPT operators on a tensor product space $\mathcal{X} \otimes \mathcal{Y}$. Notice that for the definition of PPT operator, the subspace on which we apply the partial transposition does not matter. Let us also notice that the set $\mathrm{PPT}(\mathcal{X} : \mathcal{Y})$ is a closed convex cone. We will assume that $\mathcal{A} = \mathbb{C}^d$ and $\mathcal{B} = \mathbb{C}^d$ are two identical vector spaces referring to Alice's and Bob's systems, respectively. A pure state $u \in \mathcal{A} \otimes \mathcal{B}$ lying across these spaces is called *maximally entangled* if we are left with a maximally mixed state once we trace out one of the spaces, i.e., $\mathrm{Tr}_{\mathcal{A}}(uu^*) = \mathrm{Tr}_{\mathcal{B}}(uu^*) = \mathbf{1}/d$. Any maximally entangled state $uu^* \in \mathrm{Den}(\mathcal{A} \otimes \mathcal{B})$ may be written as

$$(U \otimes \mathbf{1}_{\mathcal{B}})M_d(U \otimes \mathbf{1}_{\mathcal{B}})^*,$$

where $U \in \mathrm{U}(\mathcal{A})$ is some unitary operator and $M_d \in \mathrm{Den}(\mathcal{A} \otimes \mathcal{B})$ is the state

$$M_d = \frac{1}{d} \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes |i\rangle\langle j|. \tag{1}$$

In the rest of the paper, we will use the standard Pauli matrices, $\sigma_0 = \mathbf{1}, \sigma_1, \sigma_2, \sigma_3 \in \mathrm{U}(\mathbb{C}^2)$, and the standard set of *Bell states* $\{|\psi_i\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 : i \in \{0,1,2,3\}\}$, where

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and $\quad |\psi_i\rangle = (\mathbf{1} \otimes \sigma_i)|\psi_0\rangle \quad$ for $\quad i = 1,2,3.$

For any positive integer d, let $\mathbb{Z}_d$ be the ring of integers modulo d and $\omega_d = \exp(2\pi i/d)$. For any choice of $(a,b) \in \mathbb{Z}_d^2$ we define the *generalized Bell state* $|\psi_{a,b}\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ as follows:

$$|\psi_{a,b}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega_d^{aj}|j\rangle \otimes |j+b\rangle,$$

where addition is in $\mathbb{Z}_d$. Whenever we write states as lowercase Greek letters out of the kets, we will mean their density operator representation, for example, $\psi_0 = |\psi_0\rangle\langle\psi_0|$. A *measurement* on a space $\mathcal{X}$ is a set of operators $\{P_a : a \in \Gamma\} \subset \mathrm{Pos}(\mathcal{X})$, indexed by a finite, nonempty set of measurement outcomes Γ, for which the following constraint holds:

$$\sum_{a \in \Gamma} P_a = \mathbf{1}_{\mathcal{X}}.$$

In the rest of this paper, we will make use of semidefinite programming. For a formalization of semidefinite programming similar to the one used in this paper and a general overview of semidefinite duality theory, see [9].

III. PPT DISTINGUISHABILITY

Let $\mathcal{A}$ and $\mathcal{B}$ be the complex Euclidean spaces corresponding to Alice and Bob's systems and let $S = \{\rho_1, \ldots, \rho_k\} \subset \mathrm{Den}(\mathcal{A} \otimes \mathcal{B})$ be a set of states. Alice and Bob are given a state $\rho_i \in S$ for some $i \in \{1, \ldots, k\}$ drawn with some probability p_i, and their goal is to determine the value of i, assuming that they have complete knowledge of the set S. For the results in

the paper, we consider the interesting case in which the states in S are mutually orthogonal.

A measurement $\{P_a : a \in \Gamma\} \subset \text{Pos}(\mathcal{A} \otimes \mathcal{B})$ is said to be PPT if it can be implemented by a PPT channel, or equivalently, if each measurement operator is PPT, that is, $P_a \in \text{PPT}(\mathcal{A} : \mathcal{B})$ for each $a \in \Gamma$. We say that a set S is *PPT-distinguishable* if Alice and Bob can achieve the goal described above for the set S without error and by using only PPT measurements. Otherwise we say that the set S is *PPT-indistinguishable*. More formally, for the setup described above, the success probability for a measurement $\{P_i : 1 \leqslant i \leqslant k\}$ of distinguishing the set S is $\sum_{i=1}^{k} p_i \langle P_i, \rho_i \rangle$. We say that a set S is PPT-distinguishable if and only if there exists a PPT measurement for which this value is equal to 1.

A. A semidefinite program for the PPT distinguishability problem

We will now describe and analyze a semidefinite program whose optimal value is equal to the maximum success probability of PPT-distinguishing the set of states that is given as input to the program. Let $k > 0$ be an integer, $p = (p_1, \ldots, p_k) \in \mathbb{R}^k$ a probability vector, and assume that $S = \{\rho_i \in \text{Den}(\mathcal{A} \otimes \mathcal{B}) : i = 1, \ldots, k\}$ is the set of states that Alice and Bob are asked to distinguish. Each state $\rho_i \in S$ is prepared with probability p_i. We can phrase the maximum probability of successfully distinguishing S with the following semidefinite program, whose constraints characterize the fact that the measurement must be PPT.

Primal problem:

$$
\begin{aligned}
\text{maximize} : & \sum_{j=1}^{k} p_j \langle P_j, \rho_j \rangle \\
\text{subject to} : & P_1 + \cdots + P_k = \mathbf{1}_{\mathcal{A}} \otimes \mathbf{1}_{\mathcal{B}}, \\
& P_1, \ldots, P_k \in \text{PPT}(\mathcal{A} : \mathcal{B}).
\end{aligned}
\tag{2}
$$

Since we are interested in perfect distinguishability, in the rest of the paper we will assume, without loss of generality, that each state is prepared with uniform probability, i.e., $p_i = 1/k$, for each $i = 1, \ldots, k$. We obtain the following dual problem by routine calculation. The only thing to notice is that the partial transpose mapping is its own adjoint.

Dual problem:

$$
\begin{aligned}
\text{minimize} : & \frac{1}{k} \text{Tr}(Y) \\
\text{subject to} : & Y - \rho_j \geqslant \mathcal{T}_{\mathcal{A}}(Q_j), \quad j = 1, \ldots, k, \\
& Y \in \text{Herm}(\mathcal{A} \otimes \mathcal{B}), \\
& Q_1, \ldots, Q_k \in \text{Pos}(\mathcal{A} \otimes \mathcal{B}).
\end{aligned}
\tag{3}
$$

If we further constrain the dual problem by imposing equality instead of inequality constraints in the above program, we obtain the following version:

$$
\begin{aligned}
\text{minimize} : & \frac{1}{k} \text{Tr}(Y) \\
\text{subject to} : & Y \geqslant \mathcal{T}_{\mathcal{A}}(\rho_j), \quad j = 1, \ldots, k, \\
& Y \in \text{Herm}(\mathcal{A} \otimes \mathcal{B}).
\end{aligned}
\tag{4}
$$

Let α, β, and β' be, respectively, the solutions of the primal (2), the dual (3), and the more constrained dual problem (4). By the weak duality theorem, we have that $\alpha \leqslant \beta \leqslant \beta'$, that is, any feasible solution to (4) upper-bounds the success probability of distinguishing the set of states $\{\rho_1, \ldots, \rho_k\}$ by performing only PPT measurements. An immediate application of this is the following simple proof of the fact shown in [7] that it is impossible for Alice and Bob to perfectly distinguish any set of $k > d$ maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ using only PPT measurements.

Theorem 1. No PPT measurement can perfectly distinguish more than d maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$.

Proof. Let $\mathcal{A} = \mathcal{B} = \mathbb{C}^d$. We are assuming that the states we want to distinguish $\{\rho_1, \ldots, \rho_k\} \subset \text{Den}(\mathcal{A} \otimes \mathcal{B})$ are all maximally entangled. Therefore, each $\rho_j \in \text{Den}(\mathcal{A} \otimes \mathcal{B})$, $j \in \{1, \ldots, k\}$, may be written as $\rho_j = (V_j \otimes \mathbf{1}_{\mathcal{B}}) M_d (V_j \otimes \mathbf{1}_{\mathcal{B}})^*$, where M_d is the state defined in Eq. (1) and $V_j \in \text{U}(\mathcal{A})$ is some unitary operator. The partial transpose of M_d is the state $\frac{1}{d} W_d$, where $W_d \in \text{U}(\mathcal{A} \otimes \mathcal{B})$ is the SWAP operator, i.e.,

$$
\mathcal{T}_{\mathcal{A}}(M_d) = \frac{1}{d} W_d = \frac{1}{d} \sum_{i,j=0}^{d-1} |j\rangle\langle i| \otimes |i\rangle\langle j|.
\tag{5}
$$

Moreover, the partial transposition map is Hermiticity-preserving. Then, for each $j = 1, \ldots, k$, we have

$$
\mathcal{T}_{\mathcal{A}}(\rho_j) = \frac{1}{d} U_j
$$

for some Hermitian unitary operator $U_j \in \text{U}(\mathcal{A} \otimes \mathcal{B}) \cap \text{Herm}(\mathcal{A} \otimes \mathcal{B})$.

It holds that $(\mathbf{1}_{\mathcal{A}} \otimes \mathbf{1}_{\mathcal{B}}) \geqslant U_j$ for each $j = 1, \ldots, k$. Therefore, $Y = (\mathbf{1}_{\mathcal{A}} \otimes \mathbf{1}_{\mathcal{B}})/d$ is a feasible solution of the semidefinite program (4) and, for any measurement $\{P_1, \ldots, P_k\} \subset \text{PPT}(\mathcal{A} : \mathcal{B})$, we have

$$
\frac{1}{k} \sum_{j=1}^{k} \langle P_j, \rho_j \rangle \leqslant \frac{1}{k} \text{Tr}(Y) = \frac{d}{k}.
$$

B. Bell diagonal states

The following two basic propositions about Bell states will be used throughout the paper and can be proved by direct inspection:

Proposition 1. Let $\mathcal{A} = \mathcal{B} = \mathbb{C}^2$ and let $\psi_i = |\psi_i\rangle\langle\psi_i| \in \text{Den}(\mathcal{A} \otimes \mathcal{B})$ for $i \in \{0, 1, 2, 3\}$, with the density operators corresponding to the standard Bell states. Then the following equations hold:

$$
\begin{aligned}
\mathcal{T}_{\mathcal{A}}(\psi_0) = \tfrac{1}{2}\mathbf{1} - \psi_2, \quad & \mathcal{T}_{\mathcal{A}}(\psi_1) = \tfrac{1}{2}\mathbf{1} - \psi_3, \\
\mathcal{T}_{\mathcal{A}}(\psi_2) = \tfrac{1}{2}\mathbf{1} - \psi_0, \quad & \mathcal{T}_{\mathcal{A}}(\psi_3) = \tfrac{1}{2}\mathbf{1} - \psi_1.
\end{aligned}
$$

Proposition 2. The Bell states are invariant under the following set of local symmetries:

$$
C = \{\mathbf{1} \otimes \mathbf{1}, \sigma_1 \otimes \sigma_1, \sigma_2 \otimes \sigma_2, \sigma_3 \otimes \sigma_3\},
$$

i.e., $\psi_i = U \psi_i U^*$ for any $U \in C$ and $i \in \{0, 1, 2, 3\}$.

Definition 1. We will describe the mapping of Proposition 1 with the following bijection $f : \{0, 1, 2, 3\} \to \{0, 1, 2, 3\}$ between indices of the set of Bell states:

$$
f(0) = 2, \quad f(1) = 3, \quad f(2) = 0, \quad f(3) = 1.
$$

Let $v \in \mathbb{Z}_4^t$ be a t-dimensional vector and let $|\psi_v\rangle \in \mathbb{C}^{2^t} \otimes \mathbb{C}^{2^t}$ be the maximally entangled state given by the tensor product of Bell states indexed by the vector $v = (v_1, \dots, v_t)$, that is,

$$|\psi_v\rangle = |\psi_{v_1}\rangle \otimes \cdots \otimes |\psi_{v_t}\rangle.$$

In the literature, operators diagonal in the basis $\{\psi_v = |\psi_v\rangle\langle\psi_v| : v \in \mathbb{Z}_4^t\}$ are called *lattice operators*, or *lattice states* if they are also density operators [10]. It turns out that in the case in which the set to distinguish contains only lattice states, the semidefinite program (2) simplifies remarkably, as the following theorem states:

Theorem 2. If $\rho_1, \dots, \rho_k$ are lattice states, then the probability of successfully PPT-distinguishing them can be expressed as the optimal value of a linear program.

Proof. We will prove that for any feasible solution of the semidefinite program (2), there is another feasible solution of (2) consisting only of lattice operators for which the objective function takes the same value. Let $\Delta : \text{Lin}(\mathbb{C}^2 \otimes \mathbb{C}^2) \to \text{Lin}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be the channel defined as follows:

$$\Delta(X) = \frac{1}{|C|} \sum_{U \in C} U X U^*,$$

where C is the set of local unitaries defined in Proposition 2. The channel $\Delta(X)$ acts on X as a completely dephasing channel in the Bell basis. Suppose that $\mathcal{A} = \mathcal{B} = \mathbb{C}^{2^t}$ and $\rho_1, \dots, \rho_k \in \text{Den}(\mathcal{A} \otimes \mathcal{B})$ are lattice states. We let $\Phi = \Delta^{\otimes t}$ and have

$$\langle P_j, \rho_j \rangle = \langle P_j, \Phi(\rho_j) \rangle = \langle \Phi(P_j), \rho_j \rangle$$

for any $j = 1, \dots, k$. The channel Φ is unital and, in fact, it is a mixed unitary channel. Therefore, if $P_1, \dots, P_k$ are such that $P_1 + \cdots + P_k = \mathbf{1}$, then it holds that $\Phi(P_1) + \cdots + \Phi(P_k) = \mathbf{1}$. From the positivity of Δ, we have that $\Phi(P) \geqslant 0$ for any $P \geqslant 0$. Now we show that the partial transpose mapping commutes with the channel Φ. First we observe how the partial transposition modifies the action of local operators. Given $U_1 \in \text{Lin}(\mathcal{A})$, $U_2 \in \text{Lin}(\mathcal{B})$, and $X \in \text{Lin}(\mathcal{A} \otimes \mathcal{B})$, we have

$$\mathcal{T}_{\mathcal{A}}[(U_1 \otimes U_2)X(U_1 \otimes U_2)^*] = (\overline{U_1} \otimes U_2)\mathcal{T}_{\mathcal{A}}(X)(\overline{U_1} \otimes U_2)^*.$$

Notice that for the Pauli matrices, we have $\overline{\sigma_j} = \sigma_j$ for $j \in \{0, 1, 3\}$ and $\overline{\sigma_2} = -\sigma_2$. Therefore,

$$\Phi(\mathcal{T}_{\mathcal{A}}(X)) = \mathcal{T}_{\mathcal{A}}(\Phi(X)) \quad \text{for any} \quad X \in \text{Lin}(\mathcal{A} \otimes \mathcal{B}).$$

This observation, along with the positivity of Φ, leads to the following implication, which concludes the proof:

$$\mathcal{T}_{\mathcal{A}}(X) \geqslant 0 \Rightarrow \Phi(\mathcal{T}_{\mathcal{A}}(X)) \geqslant 0$$
$$\Rightarrow \mathcal{T}_{\mathcal{A}}(\Phi(X)) \geqslant 0 \quad \text{for any} \quad X \in \text{Lin}(\mathcal{A} \otimes \mathcal{B}).$$

For any feasible solution of the primal program, we found another solution consisting only of lattice operators for which the objective function takes the same value. Given that the lattice operators are diagonal in the Bell basis, we can cast the semidefinite program as a linear program.

Even though the states we will consider in the next sections are lattice states, we will always refer to the more general semidefinite programming formulation given in Sec. III A, rather than expressing the problem in a more explicit linear programming form.

C. Examples of indistinguishable sets

We are now ready to show some sets of k maximally entangled states in $\mathbb{C}^k \otimes \mathbb{C}^k$ that are not distinguishable by PPT measurements.

1. $k = d = 4$

The following set of $k = 4$ maximally entangled states was shown in [7] to be not perfectly distinguishable by PPT measurements. Here we prove via semidefinite programming that the optimal probability of success of distinguishing this set for any PPT measurement is 7/8. We do this by exhibiting a feasible solution of the more constrained dual problem (4) for which the objective function has a value 7/8.

Example 1. Let $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ and $\mathcal{B} = \mathcal{B}_1 \otimes \mathcal{B}_2$ be, respectively, Alice and Bob's system, with $\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{B}_1 = \mathcal{B}_2 = \mathbb{C}^2$. The set considered in [7] is $\{\rho_i = |x_i\rangle\langle x_i| : i \in [1,4]\}$, where

$$|x_1\rangle = |\psi_0\rangle \otimes |\psi_0\rangle, \quad |x_2\rangle = |\psi_1\rangle \otimes |\psi_3\rangle,$$
$$|x_3\rangle = |\psi_2\rangle \otimes |\psi_3\rangle, \quad |x_4\rangle = |\psi_3\rangle \otimes |\psi_3\rangle,$$

and the bipartition is such that $|x_i\rangle \in \mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{A}_2 \otimes \mathcal{B}_2$ for each $i \in [1,4]$.

Theorem 3. The maximal probability of success of distinguishing the set of Example 1 with a PPT measurement is equal to 7/8.

Proof. It is easy to check that the following operator satisfies the constraints in (4) and its trace is equal to 7/2:

$$Y = \tfrac{1}{4}\mathbf{1} \otimes \mathbf{1} - \tfrac{1}{2}(\psi_2 \otimes \psi_1).$$

We will check the constraint $Y \geqslant \mathcal{T}_{\mathcal{A}}(\rho_1)$ and the reader can check the remaining constraints with a similar calculation. By Proposition 1, we have

$$\mathcal{T}_{\mathcal{A}}(\rho_1) = \mathcal{T}_{\mathcal{A}}(\psi_0 \otimes \psi_0) = \left(\tfrac{1}{2}\mathbf{1} - \psi_2\right) \otimes \left(\tfrac{1}{2}\mathbf{1} - \psi_2\right)$$
$$= \tfrac{1}{4}\mathbf{1} \otimes \mathbf{1} - \tfrac{1}{2}\sum_{i \in \{0,1,3\}}(\psi_i \otimes \psi_2 + \psi_2 \otimes \psi_i)$$

and

$$Y - \mathcal{T}_{\mathcal{A}}(\rho_1) = \tfrac{1}{2}(\psi_0 \otimes \psi_2 + \psi_1 \otimes \psi_2 + \psi_3 \otimes \psi_2$$
$$+ \psi_2 \otimes \psi_0 + \psi_2 \otimes \psi_3) \geqslant 0.$$

Theorem 4. The bound of Theorem 3 is tight. In fact, there is a PPT measurement that achieves the same value.

Proof. Let $Q \in \text{Pos}(\mathbb{C}^4 \otimes \mathbb{C}^4)$ and $R, S \in \text{Pos}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be the following operators:

$$Q = \tfrac{1}{4}\mathbf{1} \otimes (\psi_1 + \psi_2), \quad R = \tfrac{7}{8}\psi_0 + \tfrac{1}{8}\psi_3,$$
$$S = \tfrac{1}{8}\psi_0 + \tfrac{7}{8}\psi_3.$$

Then the following operators define a PPT measurement that distinguishes the set of Example 1 with success probability 7/8:

$$P_1 = Q + \left(\tfrac{2}{3}\psi_0 + \tfrac{1}{3}\mathbf{1}\right) \otimes R,$$

$$P_2 = Q + \left(\tfrac{1}{3}\psi_0 + \psi_1\right) \otimes S + \tfrac{1}{3}(\psi_2 + \psi_3) \otimes R,$$

$$P_3 = Q + \left(\tfrac{1}{3}\psi_0 + \psi_2\right) \otimes S + \tfrac{1}{3}(\psi_1 + \psi_3) \otimes R,$$

$$P_4 = Q + \left(\tfrac{1}{3}\psi_0 + \psi_3\right) \otimes S + \tfrac{1}{3}(\psi_1 + \psi_2) \otimes R.$$

It is easy to check that these operators define a measurement, that is, $\sum_{i=1}^{4} P_i = \mathbf{1}$. Using the equations of Proposition 2, it is easy to check that those operators are also PPT. For instance,

$$\mathcal{T}_{\mathcal{A}}(P_1) = (\psi_1 + \psi_2 + \psi_4) \otimes \left(\tfrac{1}{3}\psi_1 + \tfrac{1}{2}\psi_2 + \tfrac{1}{3}\psi_4\right)$$
$$+ \tfrac{1}{4}\psi_3 \otimes (\psi_2 + \psi_3) \geqslant 0.$$

Finally, we have that $\langle P_i, \rho_i \rangle = \tfrac{7}{8}$ for each $i \in [1,4]$.

2. $k = d = 2^n$, $n \geqslant 2$

In [6], the authors pose the question of whether there exists a set of k maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ not perfectly distinguishable by LOCC, for some k such that $4 < k \leqslant d$. Here we give an explicit construction of such sets when $k = d$ is any power of 2 and the states are given by the tensor product of Bell states.

Lemma 1. Given a vector $\mathbf{i} = (i_1, \ldots, i_n)$, we define the set

$$K(\mathbf{i}) = \{(j_1, \ldots, j_n) : \bigoplus_{l=1,\ldots,n} \delta_{i_l j_l} = 1\},$$

where $\oplus$ denotes the sum modulo 2 and $\delta_{i_l j_l} = 1$ if and only if $i_l = j_l$. Let $\mathcal{A} = \mathcal{B} = \mathbb{C}^{2^n}$. Then the partial transpose of $\psi_{\mathbf{i}} = \psi_{i_1} \otimes \cdots \otimes \psi_{i_n} \in \mathrm{Den}\,(\mathcal{A} \otimes \mathcal{B})$ is equal to

$$\mathcal{T}_{\mathcal{A}}(\psi_{\mathbf{i}}) = \frac{1}{2^n}\left(\mathbf{1} - 2\sum_{(j_1,\ldots,j_n) \in K(\mathbf{i})} \psi_{f(j_1)} \otimes \cdots \otimes \psi_{f(j_n)}\right),$$

where f is the bijection defined in Sec. III B.

Proof. It follows straightforwardly from Proposition 1.

Theorem 5. For any $n \geqslant 2$, there is a set of $k = 2^n$ maximally entangled states in $\mathbb{C}^k \otimes \mathbb{C}^k$ that is not perfectly distinguishable by PPT operations.

Proof. The case $n = 2$ is covered in Sec. III C 1. Here we construct a set for any $n \geqslant 3$. Consider the set of states $S = \{\rho_j = \psi_0 \otimes \rho'_j : j = 1, \ldots, k\}$, where each ρ'_j is a tensor product of one of the 3^{n-1} combinations of Bell states different from ψ_0. Since $3^{n-1} > 2^n$ for any $n \geqslant 3$, we can always construct such a set. By using Lemma 1, it is easy to check that the operator

$$Y = \tfrac{1}{k}\mathbf{1} - \tfrac{2}{k}\psi_2 \otimes \cdots \otimes \psi_2$$

satisfies the constraints of the semidefinite program (4). Also, its trace is strictly less than 1.

Remark 1. An interesting feature of the set of states S considered in the above proof is that Alice and Bob are basically being provided with the maximally entangled pair $\psi_0 \in \mathrm{Den}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ as a resource, but they are still not able to

distinguish the set $\{\rho'_j : 1 \leqslant j \leqslant 2^n\} \subset \mathrm{Den}(\mathbb{C}^{2^{n-1}} \otimes \mathbb{C}^{2^{n-1}})$. In fact, for larger n, it is easy to see that we can even give them $c > 1$ maximally entangled pairs, as long as c is odd and $3^{n-c} \geqslant 2^n$, i.e., $c \leqslant (1 - \log_3 2)n$, and a construction of an indistinguishable set similar to the one above will still work.

Remark 2. The upper bound of the probability of distinguishing the sets we derive from the semidefinite program is $1 - 2/k^2$, which is the value of the trace of the operator Y in the above theorem multiplied by $1/k$. Notice that there exist sets that are in some sense even more indistinguishable. For example, in the case of $k = 8$, we could show that the following set of states cannot be PPT-distinguished with a success probability bigger than 15/16:

$$\{\psi_{(1,1,1)}, \psi_{(1,1,3)}, \psi_{(1,1,4)}, \psi_{(2,2,2)}, \psi_{(3,3,1)}, \psi_{(3,3,3)},$$
$$\times \psi_{(3,3,4)}, \psi_{(4,2,2)}\},$$

where $\psi_{(i,j,k)} = \psi_i \otimes \psi_j \otimes \psi_k$.

3. $k = d = 5,6$

We ran the semidefinite programming solver CVX [11] against the sets of the examples given in [6] for the case $k = d = 5,6$, and they turned out to be perfectly distinguishable by PPT measurements. Therefore the question they pose, namely whether LOCC protocols more powerful than one-way protocols can perfectly distinguish those sets, remains open.

On the other hand, again by running numerical computations with CVX, we show that the two sets of $k = 5$ and 6 generalized Bell states in $\mathbb{C}^k \otimes \mathbb{C}^k$ are not perfectly distinguishable by PPT measurements. These examples come from [3], where it was shown that they cannot be reliably distinguished by so-called standard teleportation protocols, which are a subset of LOCC protocols.

Example 2. Any PPT measurement errs with probability at least 0.0101 when trying to distinguish the set of generalized Bell states

$$\psi_{0,0}, \psi_{1,1}, \psi_{2,1}, \psi_{1,3}, \psi_{2,3} \in \mathbb{C}^5 \otimes \mathbb{C}^5.$$

Example 3. Any PPT measurement errs with probability at least 0.002 when trying to distinguish the set of generalized Bell states,

$$\psi_{0,0}, \psi_{1,0}, \psi_{2,0}, \psi_{3,0}, \psi_{4,0}, \psi_{0,3} \in \mathbb{C}^6 \otimes \mathbb{C}^6.$$

IV. UNAMBIGUOUS PPT DISCRIMINATION

In the preceding section, we analyzed the problem of distinguishing quantum states using PPT measurements that minimize the probability of error. Bandyopadhyay [12] raised the question of what is the probability of error if, instead, we consider an *unambiguous* PPT strategy to distinguish the sets of states of Sec. III C. In such a strategy, Alice and Bob never give an incorrect answer, although their answer can be inconclusive. If there are k states to be distinguished, an unambiguous measurement consists of $k + 1$ operators, where the outcome of the operator P_{k+1} corresponds to the inconclusive answer. In this section, we cast this problem into the framework of semidefinite programming and we make a comparison with

the result we obtained in Sec. III for the example considered in [7]. The semidefinite programming approach has already been used to study unambiguous discrimination [13], but never, as far as we know, to study unambiguous PPT discrimination. In fact, we believe that unambiguous PPT discrimination in general, or even unambiguous LOCC discrimination, has not been thoroughly investigated yet.

The optimal value of the following semidefinite program is equal to the success probability of unambiguously distinguishing a set of states $\{\rho_1, \dots, \rho_k\}$ using PPT measurements. Again, we assume that the states are drawn with a uniform probability.

Primal problem:

$$\text{maximize}: \quad \frac{1}{k} \sum_{j=1}^{k} \langle P_j, \rho_j \rangle$$

$$\text{subject to}: \quad P_1 + \dots + P_{k+1} = \mathbf{1}_{\mathcal{A}} \otimes \mathbf{1}_{\mathcal{B}}, \quad (6)$$
$$P_1, \dots, P_{k+1} \in \text{PPT}\,(\mathcal{A} : \mathcal{B}),$$
$$\langle P_i, \rho_j \rangle = 0, \qquad 1 \leqslant i, \quad j \leqslant k, \quad i \neq j.$$

Dual problem:

$$\text{minimize}: \quad \frac{1}{k}\,\text{Tr}(Y)$$

$$\text{subject to}: \quad Y - \rho_j + \sum_{\substack{1 \leqslant i \leqslant k \\ i \neq j}} y_{i,j}\rho_i \geqslant \mathcal{T}_{\mathcal{A}}(Q_j),$$
$$j = 1, \dots, k\,,$$
$$Y \geqslant \mathcal{T}_{\mathcal{A}}(Q_{k+1}), \quad (7)$$
$$Q_1, \dots, Q_{k+1} \in \text{Pos}\,(\mathcal{A} \otimes \mathcal{B})\,,$$
$$Y \in \text{Herm}\,(\mathcal{A} \otimes \mathcal{B})\,,$$
$$y_{i,j} \in \mathbb{R}, \quad 1 \leqslant i, \quad j \leqslant k, \quad i \neq j.$$

Interestingly, the optimal probability of unambiguously distinguish the set of states of Example 1 with PPT measurements is 3/4, which should be compared with the success probability of 7/8 that can be achieved with a minimum-error strategy (see Theorem 4). In fact, using a semidefinite program solver, we were also able to verify that this bound is actually tight.

Theorem 6. The maximum success probability of unambiguously distinguishing the set of states of Example 1 with PPT measurements is equal to 3/4.

Proof. We show a feasible solution of the dual problem for which the value of the objective function is 3/4. Let

$$Y = \tfrac{1}{4}[(\mathbf{1} - \psi_1) \otimes (\mathbf{1} - 2\psi_4)$$
$$+ \psi_1 \otimes (-\psi_1 + 3\psi_2 + 3\psi_3 + \psi_4)]$$

and

$$Q_1 = (\mathbf{1} - \psi_3) \otimes \psi_3 + \psi_3 \otimes (\psi_2 + \psi_3),$$
$$Q_2 = (\psi_1 + \psi_2) \otimes \psi_2 + \psi_4 \otimes (\mathbf{1} - \psi_2),$$
$$Q_3 = (\psi_2 + \psi_4) \otimes \psi_2 + \psi_1 \otimes (\mathbf{1} - \psi_2),$$
$$Q_4 = (\psi_1 + \psi_4) \otimes \psi_2 + \psi_2 \otimes (\mathbf{1} - \psi_2),$$
$$Q_5 = \psi_3 \otimes \psi_2.$$

We can use Proposition 1 to check that the following equations hold:

$$Y - \rho_j + \sum_{\substack{1 \leqslant i \leqslant k \\ i \neq j}} \rho_i = \mathcal{T}_{\mathcal{A}}(Q_j), \quad j = 1, \dots, 4$$

$$\text{and} \quad Y \geqslant \mathcal{T}_{\mathcal{A}}(Q_5),$$

i.e., the constraints of the program (7) are satisfied. Also, we have that $\text{Tr}(Y) = 3$.

V. CONCLUSION

In summary, we have extended previously known results about the indistinguishability of some sets of d orthogonal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ using PPT measurements. We hope that our approach based on semidefinite programming can lead to a better understanding of the power of local operations at least with regard to the task of distinguishing quantum states.

The main open question is whether there exist examples of sets such as the ones we considered, but of size $k < d$. For small values of d, we obtained an unsuccessful answer to this question after running an exhaustive numerical search against sets consisting of $d - 1$ generalized Bell states, or lattice states, or states constructed from complex Hadamard matrices. It would be interesting to try some different constructions of orthogonal maximally entangled states. The following are other interesting unanswered questions related to our results:

(i) Can we achieve the same bound of Theorem 4 using a separable (or LOCC) measurement?

(ii) Are there examples of sets for which LOCC measurements do worse than PPT?

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

[2] M. Nathanson, J. Math. Phys. **46**, 062103 (2005).

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

[4] 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).

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

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

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

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

[9] J. Watrous, Theor. Comput. **5**, 11 (2009).

[10] M. Piani, Phys. Rev. A **73**, 012345 (2006).

[11] M. Grant and S. Boyd, CVX: MATLAB software for disciplined convex programming, version 1.21. http://cvxr.com/cvx, April 2011.

[12] S. Bandyopadhyay (private communication).

[13] Y. C. Eldar, IEEE Trans. Inf. Theor. **49**, 446 (2003).