Small sets of locally indistinguishable orthogonal maximally entangled states

Alessandro Cosentino[*] and Vincent Russo[†]
David R. Cheriton School of Computer Science and Institute for Quantum Computing,
University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

(Dated: July 12, 2013)

We show how to construct sets of fewer than d orthogonal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ that are not perfectly distinguishable by local operations and classical communication (LOCC). This improves upon previous results, which only showed sets of $k \geq d$ such states. Our results hold for an even wider class of operations, which is the class of positive-partial-transpose measurements (PPT). The proof uses the characterization of the PPT distinguishability problem as a semidefinite program. As an explicit example, we exhibit a set of 15 locally indistinguishable maximally entangled states in $\mathbb{C}^{16} \otimes \mathbb{C}^{16}$.

A central subject of study in quantum information theory is the interplay between entanglement and nonlocality. An important tool to study this relationship is the paradigm of local operations and classical communication (LOCC). This is a subset of all global operations, with a fairly intuitive physical description. In a two-party LOCC protocol, Alice and Bob can perform quantum operations only on their local subsystems and the communication must be classical.

A fundamental problem that has been studied to understand the limitations of LOCC protocols is the problem of distinguishing quantum states. The setup of the problem is pretty simple in the bipartite case. The two parties are given a single copy of a pure state chosen with some probability from a set and their goal is to identify which state was given, with the assumption that they have full knowledge on the set. If the states are orthogonal and global operations are permitted, then it is always possible to determine the state with certainty. In contrast, if only LOCC protocols are allowed, Alice and Bob cannot in general discover the state they have been given, even if the states are orthogonal. The problem of distinguishing a known set of quantum states by LOCC has been thoroughly investigated in quantum information theory [1–14].

It is an interesting question to understand how, for LOCC-indistinguishable sets, the number of states (denoted by k in this Letter) relates to the dimension d of each of Alice's and Bob's subsystems. Walgate et al. [2] proved that any two orthogonal pure states can always be perfectly distinguished by an LOCC measurement. Moreover, Nathanson [8] showed that perfect distinguishability is always possible for the case of any three maximally entangled states in $\mathbb{C}^3 \otimes \mathbb{C}^3$. For a general d, Fan [6] proved that any k maximally entangled states are locally distinguishable if $k(k-1) \leq 2d$, when d is prime. On the other hand, it is known that $k > d$ orthogonal maximally entangled states can never be distinguished with certainty by LOCC measurements [7]. For the weaker model of *one-way* LOCC protocols, Bandyopadhyay et al. [15] showed examples of indistinguishable sets of states with the size of the sets being equal to the dimension of the subsystems, for the particular cases of $d = 4, 5, 6$. Recently, Yu et al. [12] exhibited an explicit example of a set containing $k = 4$ maximally entangled states in $\mathbb{C}^4 \otimes \mathbb{C}^4$ that cannot be perfectly distinguished by any LOCC protocol. Their result was later generalized in [14] for higher dimensions (with the dimension d restricted to be a power of two).

It should be noted that entanglement is not a necessary feature of indistinguishable sets of states. In a famous result, Bennett et al. [1] exhibited a set of orthogonal bipartite pure product states that are perfectly distinguishable by separable operations, but not by LOCC (see [16] for a simplified proof and a generalization of this result). In fact, if we allow states that are not maximally entangled in the set, we can easily construct indistinguishable sets with a fixed size in any dimension we like. On the one hand, entanglement makes distinguishability harder, but on the other hand, it can be used as a resource by the parties involved in the protocol. This makes the distinguishability problem especially interesting in the case when the set contains only maximally entangled states.

The above-mentioned results left open the question of what is the right bound on the size of sets of locally indistinguishable orthogonal maximally entangled states. Is the dimension d of the subsystems a tight bound? Or does there exist indistinguishable sets of size $k < d$? We settle this question by exhibiting a general construction of sets that contain fewer than d orthogonal maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$, which are not perfectly distinguishable by LOCC measurements.

We tackle the problem by studying distinguishability of states for a class of operations broader than the class of LOCC measurements, which is the class of positive-partial-transpose (PPT) measurements. As opposed to the set of LOCC measurements, the set of PPT measurements has a nice mathematical structure. Several properties of PPT operations can be characterized in the powerful framework of semidefinite programming (see [17] for an example). In particular, semidefinite duality helps to prove bounds on the power of PPT operations, and, therefore, on the power of LOCC operations. A straight-

[*] Electronic address: acosenti@cs.uwaterloo.ca

[†] Electronic address: vrusso@cs.uwaterloo.ca

forward application of this idea is a simplified proof of the previously mentioned fact that $k > d$ orthogonal maximally entangled states cannot be perfectly distinguished by LOCC [7] (see [12] and [14] for a proof that this fact holds even in the case of PPT).

The characterization of the PPT-distinguishability problem in the framework of semidefinite programming has been also exploited in [14] to find indistinguishable sets with size $k = d$. A recent work by Yu et al. [13] has investigated further properties of state distinguishability by PPT. They prove a tight bound on the entanglement necessary to distinguish between three Bell states via PPT measurements. They also show that regardless of the number of copies, a maximally entangled state cannot be distinguished by its orthogonal complement.

Before giving the definition of a PPT measurement, we review some notation. We denote by $\mathcal{A}$ and $\mathcal{B}$ the complex Euclidean spaces corresponding to Alice's and Bob's systems, respectively. We assume that $\mathcal{A}$ and $\mathcal{B}$ are isomorphic copies of $\mathbb{C}^d$. A pure state $u \in \mathcal{A}\otimes\mathcal{B}$ is called maximally entangled if $\mathrm{Tr}_{\mathcal{A}}(uu^*) = \mathrm{Tr}_{\mathcal{B}}(uu^*) = \mathbf{1}/d$. The partial transpose is a mapping on $\mathcal{A}\otimes\mathcal{B}$ defined by tensoring the transpose mapping acting on $\mathcal{A}$ and the identity mapping acting on $\mathcal{B}$ and it is denoted as $\mathrm{T}_{\mathcal{A}} = \mathrm{T}\otimes\mathbf{1}_{\mathrm{L}(\mathcal{B})}$. Let $\mathcal{A} = \mathcal{B} = \mathbb{C}^2$ and let ψ_i, for $i \in \{0, 1, 2, 3\}$, be the density operators corresponding to the standard Bell basis. Our construction is based on states that are tensor products of Bell states. We write down explicitly the action of the partial transpose on the Bell basis:

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

A positive operator $P \geq 0$ is called a *PPT operator* if it remains positive under the action of partial transposition, that is, $\mathrm{T}_{\mathcal{A}}(P) \geq 0$. A measurement $\{P_a \geq 0 : a \in \Gamma\}$ is called a *PPT measurement* if each measurement operator is PPT.

The maximum probability of distinguishing a set of states by PPT measurements can be expressed as the optimal value of the following semidefinite program (for more details, see [14]). We are interested in no-error distinguishability, so we will assume without loss of generality, that the states are drawn from the set with uniform probability, that is, $p_i = 1/k$, for each $i = 1, \dots, k$.

Primal problem

$$\begin{aligned}
\text{maximize:}\quad & \frac{1}{k}\sum_{j=1}^{k}\langle P_j, \rho_j\rangle\\
\text{subject to:}\quad & P_1 + \cdots + P_k = \mathbf{1}_{\mathcal{A}}\otimes\mathbf{1}_{\mathcal{B}},\\
& P_1, \dots, P_k \geq 0.\\
& \mathrm{T}_{\mathcal{A}}(P_1), \dots, \mathrm{T}_{\mathcal{A}}(P_k) \geq 0
\end{aligned} \tag{2}$$

The dual of the problem is easily obtained by routine calculation.

Dual problem

$$\begin{aligned}
\text{minimize:}\quad & \frac{1}{k}\mathrm{Tr}(Y)\\
\text{subject to:}\quad & Y - \rho_j \geq \mathrm{T}_{\mathcal{A}}(Q_j), \quad j = 1, \dots, k\ ,\\
& Y \in \mathrm{Herm}\,(\mathcal{A}\otimes\mathcal{B})\,,\\
& Q_1, \dots, Q_k \geq 0.
\end{aligned} \tag{3}$$

Given a set of states, an upper bound on the probability of distinguishing them by PPT measurements can be obtained by exhibiting a feasible solution of the above dual problem.

Main Result – For any $d \geq 4$ that is a power of 2, the following theorem shows how to construct sets of d orthogonal maximally entangled states in $\mathbb{C}^d\otimes\mathbb{C}^d$, for which the above dual problem has optimal value less than or equal to C, where $C < 1$ is a constant. Given one of such sets, if we consider any of its subsets that contains only k states, then we have a set of k PPT-indistinguishable maximally entangled states in $\mathbb{C}^d\otimes\mathbb{C}^d$, where $k < d$, as long as $\frac{k}{d} > C$. Since any LOCC measurement is a PPT measurement, then such set is also indistinguishable by LOCC.

Theorem 1. *For any $d = 2^t$, where $t \geq 2$, it is possible to construct a set of k maximally entangled states in $\mathbb{C}^d\otimes\mathbb{C}^d$ for which there exists a feasible solution of the dual problem* (3) *with value equal to $\frac{7d}{8k}$.*

Proof. For the case $t = 2$ ($d = 4$), a set of states was shown by Yu et al. in [12]:

$$\begin{aligned}
\rho_1^{(2)} &= \psi_0\otimes\psi_0, \qquad \rho_3^{(2)} = \psi_2\otimes\psi_1,\\
\rho_2^{(2)} &= \psi_1\otimes\psi_1, \qquad \rho_4^{(2)} = \psi_3\otimes\psi_1.
\end{aligned} \tag{4}$$

A bound of 7/8 on the optimal probability of distinguishing these states was proved later in [14]. Here we write the feasible solution of the dual that achieves the value 7/8.

$$\begin{aligned}
Y^{(2)} &= \frac{1}{4}\mathbf{1}\otimes\mathbf{1} - \frac{1}{2}\mathrm{T}_{\mathcal{A}}(\psi_2\otimes\psi_3)\\
Q_1^{(2)} &= \frac{1}{2}[(\psi_0+\psi_1+\psi_3)\otimes\psi_2 + \psi_2\otimes(\psi_0+\psi_1)]\\
Q_2^{(2)} &= \frac{1}{2}[(\psi_0+\psi_1)\otimes\psi_3 + \psi_3\otimes(\psi_0+\psi_1+\psi_2)]\\
Q_3^{(2)} &= \frac{1}{2}[(\psi_1+\psi_3)\otimes\psi_3 + \psi_0\otimes(\psi_0+\psi_1+\psi_2)]\\
Q_4^{(2)} &= \frac{1}{2}[(\psi_0+\psi_3)\otimes\psi_3 + \psi_1\otimes(\psi_0+\psi_1+\psi_2)]
\end{aligned}$$

By using the set of equations (1), it is easy to check that the constraints of the dual problem hold for the above solution. In fact, it is a straightforward calculation to check that, for all $j \in \{1,2,3,4\}$, the following equations hold:

$$Y^{(2)} - \rho_j^{(2)} = \mathrm{T}_{\mathcal{A}}(Q_j^{(2)}). \tag{5}$$

Furthermore, we observe that $Q_1^{(2)}, Q_2^{(2)}, Q_3^{(2)}$ and $Q_4^{(2)}$ are positive semidefinite, and $\mathrm{Tr}(Y^{(4)}) = 7/2$.

For $t \geq 3$, we give a recursive construction of the states $\rho_j^{(t)}$, i.e.,

$$\rho_j^{(t)} = \begin{cases} \psi_0 \otimes \rho_j^{(t-1)} & \text{if } j \leq 2^{t-1}, \\ \psi_1 \otimes \rho_{j-2^{t-1}}^{(t-1)} & \text{if } j > 2^{t-1}, \end{cases} \tag{6}$$

for $j \in \{1, \ldots, d\}$.

Given this set of states, we can construct, again recursively, a feasible solution of the dual problem, which achieves the desired bound:

$$\begin{aligned} Y^{(t)} &= (\psi_0 + \psi_1)^{\otimes(t-2)} \otimes Y^{(2)}, \\ Q_j^{(t)} &= (\psi_0 + \psi_1)^{\otimes(t-2)} \otimes Q_r^{(2)}, \end{aligned} \tag{7}$$

where $r \equiv j \pmod 4$.

We now prove that this solution satisfies the constraints of the dual problem. First, it is easy to see that $Y^{(t)}$ is Hermitian and that $Q_j^{(t)} \geq 0$, for any $j \in \{1, \ldots, d\}$. We prove by induction on t that the rest of the constraints are also satisfied, namely all the constraints of the form

$$Y^{(t)} - \rho_j^{(t)} \geq \mathrm{T}_{\mathcal{A}}(Q_j^{(t)}), \quad j \in \{1, \ldots, d\}.$$

The base case $t = 2$ was considered above.

By the induction hypothesis, and from the fact that $\psi_0 + \psi_1 \geq 0$, it holds that

$$\begin{aligned} (\psi_0 + \psi_1) \otimes Y^{(t)} - (\psi_0 + \psi_1) \otimes \rho_j^{(t)} \\ \geq (\psi_0 + \psi_1) \otimes \mathrm{T}_{\mathcal{A}}(Q_j^{(t)}). \end{aligned} \tag{8}$$

From Eq. (6), we have $\rho_j^{(t+1)} = \psi_0 \otimes \rho_j^{(t)}$ if $j \leq 2^t$, or $\rho_j^{(t+1)} = \psi_1 \otimes \rho_j^{(t)}$ if $j > 2^t$. Since $\psi_0, \psi_1 \geq 0$, in either of the two cases we have

$$(\psi_0 + \psi_1) \otimes Y^{(t)} - \rho_j^{(t+1)} \geq (\psi_0 + \psi_1) \otimes \mathrm{T}_{\mathcal{A}}(Q_j^{(t)}). \tag{9}$$

From the set of equations (1), it is easy to see that

$$\mathrm{T}_{\mathcal{A}}(\psi_0 + \psi_1) = \psi_0 + \psi_1. \tag{10}$$

It follows that

$$(\psi_0 + \psi_1) \otimes Y^{(t)} - \rho_j^{(t+1)} \geq \mathrm{T}_{\mathcal{A}}[(\psi_0 + \psi_1) \otimes (Q_j^{(t)})]. \tag{11}$$

Finally, by the definition of the operators in Eq. (7), we have that

$$Y^{(t+1)} - \rho_j^{(t+1)} \geq \mathrm{T}_{\mathcal{A}}(Q_j^{(t+1)}). \tag{12}$$

In the case where we consider only k of the states we have constructed, the value of the program for this solution is equal to

$$\frac{\mathrm{Tr}(Y^{(t)})}{k} = \frac{2^{t-2}\,\mathrm{Tr}(Y^{(2)})}{k} = \frac{7d}{8k}. \tag{13}$$

This concludes the proof. □

It is possible to adapt the construction (6) and (7) in order to use a different couple of Bell states other than ψ_0 and ψ_1. However, these states are well-suited for a clearer proof, due to the Eq. (10).

Corollary 2. *For any $d = 2^t$, where $t \geq 4$, there exists a set of $k < d$ maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$ that cannot be perfectly distinguished by any LOCC measurement.*

Proof. By the above Theorem, when $t \geq 4$ we can construct a set of $k < 2^t$ states that can be distinguished by any PPT measurement, and therefore any LOCC measurement, only with probability of success strictly less than 1. In fact, we have that $\frac{7}{8}\frac{2^t}{k} < 1$ whenever $t \geq 4$ and $k > \frac{7}{8}2^t$. □

Example – When $t = 4$, we can construct the following set of $k = 15$ orthogonal maximally entangled states in $\mathbb{C}^{16} \otimes \mathbb{C}^{16}$, which is not perfectly distinguishable by any PPT measurement:

$$\begin{aligned}
\rho_1^{(4)} &= \psi_0 \otimes \psi_0 \otimes \psi_0 \otimes \psi_0 \\
\rho_2^{(4)} &= \psi_0 \otimes \psi_0 \otimes \psi_1 \otimes \psi_1 \\
\rho_3^{(4)} &= \psi_0 \otimes \psi_0 \otimes \psi_2 \otimes \psi_1 \\
\rho_4^{(4)} &= \psi_0 \otimes \psi_0 \otimes \psi_3 \otimes \psi_1 \\
\rho_5^{(4)} &= \psi_0 \otimes \psi_1 \otimes \psi_0 \otimes \psi_0 \\
\rho_6^{(4)} &= \psi_0 \otimes \psi_1 \otimes \psi_1 \otimes \psi_1 \\
\rho_7^{(4)} &= \psi_0 \otimes \psi_1 \otimes \psi_2 \otimes \psi_1 \\
\rho_8^{(4)} &= \psi_0 \otimes \psi_1 \otimes \psi_3 \otimes \psi_1 \\
\rho_9^{(4)} &= \psi_1 \otimes \psi_0 \otimes \psi_0 \otimes \psi_0 \\
\rho_{10}^{(4)} &= \psi_1 \otimes \psi_0 \otimes \psi_1 \otimes \psi_1 \\
\rho_{11}^{(4)} &= \psi_1 \otimes \psi_0 \otimes \psi_2 \otimes \psi_1 \\
\rho_{12}^{(4)} &= \psi_1 \otimes \psi_0 \otimes \psi_3 \otimes \psi_1 \\
\rho_{13}^{(4)} &= \psi_1 \otimes \psi_1 \otimes \psi_0 \otimes \psi_0 \\
\rho_{14}^{(4)} &= \psi_1 \otimes \psi_1 \otimes \psi_1 \otimes \psi_1 \\
\rho_{15}^{(4)} &= \psi_1 \otimes \psi_1 \otimes \psi_2 \otimes \psi_1
\end{aligned}$$

The probability of distinguishing this set by any PPT measurement is less than or equal to 14/15. Examples in higher dimensions can be generated using the Python script available at [18].

It is worth noting that the "Entanglement Discrimination Catalysis" phenomenon, observed in [12] for the set (4), also applies to the set of states in the above example and to any set derived from our construction. If Alice and Bob are provided with a maximally entangled state as a resource, then they are able to distinguish the states in these sets and, when the protocol ends, they are still left with an untouched maximally entangled state. In the $t = 2$ case, the catalyst is used to teleport the first qubit from one party to the other, say from Alice to Bob. Bob can then measure the first two qubits in the standard Bell basis and identify which of the four states was prepared. Since the third and fourth qubits are not being acted on, they can be used in a new round of the protocol. For the case $t > 2$, let us recall the recursive construction of the states $\rho_j^{(t)}$ from (6). Distinguishing between the two cases of the recursion is equivalent to distinguishing between two Bell states. And the base case is exactly the case $t = 2$ described above, with only one maximally entangled state involved in the catalysis.

Discussion – We have shown an explicit method to generate small sets of maximally entangled states that are not distinguishable by LOCC protocols. Asymptotically, our construction allows for the cardinality of these sets to be as small as Cd, where C is a constant less than 1, and d is the dimension of each Alice's and Bob's subsystems. In particular, we have that $\frac{7}{8} \leq C < 1$. It is possible that this constant can be improved by using a different construction or by starting our recursive construction from a different base case. A further improvement would be to show a construction of indistinguishable sets with size $o(d)$. The bounds we proved in the paper hold for the class of PPT measurements. Stronger bounds might hold for separable or LOCC measurements. Finally, another open problem is to give a more general construction that works even when d is not a power of two.

Acknowledgments – We are grateful to John Watrous for many insightful discussions on the problem.

This research was supported by Canada's NSERC and the US ARO.

[1] C. Bennett, D. DiVncenzo, C. Fuchs, T. Mor, E. Rains, P. Shor, J. Smolin, and W. Wootters, "Quantum nonlocality without entanglement", *Phys. Rev. A* **59** (1999) 1070–1091, `arXiv:quant-ph/9804053`.

[2] J. Walgate, A. Short, L. Hardy, and V. Vedral, "Local distinguishability of multipartite orthogonal quantum states", *Phys. Rev. Letters* **85** (2000) 4972, `arXiv:quant-ph/0007098`.

[3] S. Ghosh and G. Kar, "Distinguishability of Bell states", *Phys. Rev. Letters* **87** (2001) 277902, `arXiv:quant-ph/0106148`.

[4] J. Walgate and L. Hardy, "Nonlocality, asymmetry, and distinguishing bipartite states", *Phys Rev Letters* **89** (2002) 147901, `arXiv:quant-ph/0202034`.

[5] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, "Local indistinguishability: More nonlocality with less entanglement", *Phys. Rev. Letters* **90** (2003) 047902, `arXiv:quant-ph/0301106`.

[6] H. Fan, "Distinguishability and indistinguishability by local operations and classical communication", *Phys. Rev. Letters* **92** (2004) 177905.

[7] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, "Distinguishability of maximally entangled states", *Phys. Rev. A* **70** (2004) 022304, `arXiv:quant-ph/0205105`.

[8] M. Nathanson, "Distinguishing bipartite orthogonal states using LOCC: Best and worst cases", *J. Math. Phys.* **46** (2005) 062103, `arXiv:quant-ph/0411110`.

[9] J. Watrous, "Bipartite subspaces having no bases distinguishable by local operations and classical communication", *Phys. Rev. Letters* **95** (2005) 080505.

[10] M. Owari and M. Hayashi, "Local copying and local discrimination as a study for non-locality of a set", *Phys. Rev. A* **74** (2006) 032108, `arXiv:quant-ph/0509062`.

[11] N. Yu, R. Duan, and M. Ying, "Any $2 \otimes n$ subspace is locally distinguishable", *Phys. Rev. A* **84** (2011) 012304, `arXiv:1010.2664`.

[12] N. Yu, R. Duan, and M. Ying, "Four locally indistinguishable ququad-ququad orthogonal maximally entangled states", *Phys. Rev. Letters* **109** (2012), no. 2, 020506, `arXiv:1107.3224`.

[13] N. Yu, R. Duan, and M. Ying, "Distinguishability of quantum states by positive operator-valued measures with positive partial transpose", `arXiv:1209.4222`.

[14] A. Cosentino, "PPT-indistinguishable states via semidefinite programming", *Phys. Rev. A* **87** (2013), no. 1, 012321, `arXiv:1205.1031`.

[15] S. Bandyopadhyay, S. Ghosh, and G. Kar, "LOCC distinguishability of unilaterally transformable quantum states", *New J. Phys.* **13** (2011) 123013, `arXiv:1102.0841`.

[16] A. M. Childs, D. Leung, L. Mancinska, and M. Ozols, "A framework for bounding nonlocality of state discrimination", `arXiv:1206.5822`.

[17] E. Rains, "A semidefinite program for distillable entanglement", *IEEE Transactions on Information Theory* **47** (2001) 2921–2933, `arXiv:quant-ph/0008047`.

[18] A. Cosentino and V. Russo. `https://bitbucket.org/acosenti/ppt-sdp-paper`.