Framework for distinguishability of orthogonal bipartite states by one-way local operations and classical communication

Tanmay Singal

Optics & Quantum Information Group, The Institute of Mathematical Sciences,
CIT Campus, Taramani, Chennai, 600 113, India

In the topic of perfect local distinguishability of orthogonal multipartite quantum states, most results obtained so far pertain to bipartite systems whose subsystems are of specific dimensions. In contrast very few results for bipartite systems whose subsystems are of arbitrary dimensions, are known. This is because a rich variety of (algebraic or geometric) structure is exhibited by different sets of orthogonal states owing to which it is difficult to associate some common property underlying them all, i.e., a common property that would play a crucial role in the local distinguishability of these states. In this paper, I propose a framework for the distinguishability by one-way LOCC (1-LOCC) of sets of orthogonal bipartite states in a $d_A \otimes d_B$ bipartite system, where $d_A, d_B$ are the dimensions of both subsystems, labelled as $A$ and $B$. I show that if the $i$-th party (where $i = A, B$) can initiate a 1-LOCC protocol to perfectly distinguish among a set of orthogonal bipartite states, then the information of the existence of such a 1-LOCC protocol lies in a subspace of $d_i \times d_i$ hermitian matrices, denoted by $T^{(i)}_T$, and that the method to extract this information (of the existence of this 1-LOCC protocol) from $T^{(i)}_T$ depends on the value of $\dim T^{(i)}_T$. In this way one can give sweeping results for the 1-LOCC (in)distinguishability of all sets of orthogonal bipartite states corresponding to certain values of $\dim T^{(i)}_T$. Thus I propose that the value of $\dim T^{(i)}_T$ gives the common underlying property based on which sweeping results for the 1-LOCC (in)distinguishability of orthogonal bipartite quantum states can be made.

PACS numbers: 03.67.Hk, 03.67.Mn
Keywords: local distinguishability, one-way LOCC

Introduction: The scenario in local distinguishability of bipartite orthogonal quantum states is as follows: Alice and Bob are given one of many possible orthogonal bipartite states and they have to figure out which one they’ve been given using only local operations and classical communication (LOCC). Some prominent results which apply to joint systems, whose subsystems are of arbitrary dimension, are Bennet et al’s result [1], which established that members from an unextendible product basis cannot be perfectly distinguished by LOCC, Walgate et al’s result [2], which establishes that any two multipartite orthogonal quantum states can be perfectly distinguished using only LOCC, Badziazig et al’s [3] result, which obtained a Holveo-like upper bound for the locally accessible information for an ensemble of states from a bipartite system, and Cohen’s result [4], which established that almost all sets of $d+1$ orthogonal states from $N d$-dimensional multipartite systems are not perfectly distinguishable by LOCC. Very few such generic results are known. In this paper I propose a framework for the one-way LOCC distinguishability of orthogonal bipartite states, and this proposition is made as an aforementioned generic result.

Framework: Inspired by work done in [5] and [6], I show that for a given set of orthogonal bipartite mixed states from a $d_A \otimes d_B$ bipartite system, the $i$-th party (where $i = A, B$) can be associated with a subspace of $d_i \times d_i$ hermitian matrices, $T^{(i)}$ (defined after equation (3)) which contains all information of one-way LOCC (1-LOCC) protocols which this $i$-th party can initiate to perfectly distinguish among said given set of orthogonal bipartite states. In this paper I obtain results to extract this 1-LOCC related information from $T^{(i)}_T$.

For simplifying notation, I make two assumptions, which won’t reduce the generality of results obtained: (1) Alice always initiates the protocol. This allows for simplifying the notation: $T^{(A)}_T \rightarrow T_T$. Note that to establish distinguishability by 1-LOCC (1-LOCC distinguishability), one has to extract relevant information from $T^{(A)}_T$ (for Alice starting protocol) and/or $T^{(B)}_T$ (for Bob starting protocol), separately. (2) If $d_A < d_B$, one can always extend Alice’s subsystem $A$ to a larger local system $A'$ so that $d_{A'} = d_B$. Similarly, vice versa. Thus, there’s no loss of generality in assuming that $d_A = d_B = d$.

Let Alice and Bob have $d$ dimensional quantum systems whose Hilbert spaces are denoted by $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Let them share one of $n$ orthogonal bipartite states, whose density matrices $\rho_{AB}^{(1)}, \rho_{AB}^{(2)}, \cdots, \rho_{AB}^{(n)}$ are observables on $\mathcal{H}_A \otimes \mathcal{H}_B$. They wish to establish which state they share using a 1-LOCC protocol which Alice commences. Let spectral decomposition of $\rho_{AB}^{(i)}$ be

$$\rho_{AB}^{(i)} = \sum_{j=1}^{r_i} \lambda_{ij} |\psi_{ij}\rangle \langle \psi_{ij}|,$$

where $r_i = \text{rank}(\rho_{AB}^{(i)})$, $\{\lambda_{ij}\}_{j=1}^{r_i}$ are non-zero eigen-
values of $\rho_{\alpha}^{(i)}$ and $(\psi_{ij}|\psi_{i'j'}) = \delta_{i,i'}\delta_{j,j'}$, $\forall$ $1 \leq i \leq i' \leq n$, $1 \leq j \leq i$, and $1 \leq j' \leq r_i$. Let $\{|s_i\}_{i=1}^{d}$ and $\{|s_{i'}\}_{i'=1}^{d}$ be standard orthonormal bases (ONB) for $H_A$ and $H_{\alpha}$, respectively. For any $1 \leq i \leq n$, and any $1 \leq j \leq r_i$, define $d \times d$ complex matrices $W_{ij}$ by expanding $|\psi_{ij}\rangle_{AB}$ in the basis $\{|s_i\rangle_A|s_{k}\rangle_B\}_{i,k=1}^{d}$. 

\begin{equation}
|\psi_{ij}\rangle_{AB} = \sum_{k,l=1}^{d} (W_{ij})_{kl} |s_i\rangle_A |s_k\rangle_B. \tag{2}
\end{equation}

Thus $(\psi_{ij}|\psi_{i'j'}) = Tr(W_{ij}^\dagger W_{i'j'}) = \delta_{i,i'}\delta_{j,j'}, \forall$ $1 \leq i \leq i' \leq n$, $1 \leq j \leq r_i$, and $1 \leq j' \leq r_{i'}$. Define the index set $I \equiv \{(i,i',j,j') \in \mathbb{N}^2 | 1 \leq i < i' \leq n, 1 \leq j < r_i, 1 \leq j' < r_{i'}\}$. Let $i = (i,i',j,j') \in I$. Define $W_i \equiv W_{ij}$. Then $W_i$ is $d \times d$ complex matrices with trace zero. Let $H_1 \equiv \frac{1}{d} (W_i + (W_i)^\dagger)$ and $A_1 \equiv \frac{1}{d} (W_i - (W_i)^\dagger)$. Let $S$ be the real vector space of all $d \times d$ hermitian matrices. \textit{dim} $S = d^2$. Let $T$ be a subspace of $S$, defined by

\begin{equation}
T \equiv \left\{ \sum_{i \in I} a_i H_i + b_i A_i, \forall a_i, b_i \in \mathbb{R} \right\}. \tag{3}
\end{equation}

Let $T_1$ be the orthogonal complement of $T$ in $S$. Note that $1_d \in T_1$, where $1_d$ is the $d \times d$ identity matrix.

Now consider theorem 1.

\textbf{Theorem 1} (Nathanson [5]). Alice can commence a $1$-LOOC protocol to distinguish among $\rho_{\alpha}^{(1)}, \rho_{\alpha}^{(2)}, \ldots, \rho_{\alpha}^{(n)}$, if and only if an orthogonality preserving (OP) rank-one POVM exists on her side to start protocol with.

The set of POVMs acting on a quantum system $A$ (or $B$) is convex, and a rank-one POVM $\{|\tilde{l}|\tilde{l}\rangle\rangle_{i=1}^{m}$ in that set isn’t necessarily extremal (check supplemental material [5] for more information). $\sum_{i=1}^{m} |\tilde{l}|\tilde{l}\rangle\rangle = 1_A$, where $1_A$ is the identity operator on $H_A$. Let $\{|\tilde{l}|\tilde{l}\rangle\rangle\}_{i=1}^{m}$ have a convex decomposition into two distinct extreme rank-one POVMs: $|\tilde{l}|\tilde{l}\rangle\rangle = p|\tilde{l}'\rangle\rangle + (1-p)|\tilde{l}''\rangle\rangle$, $\forall$ $1 \leq i \leq m$, and where $p \in (0,1)$, $\sum_{i=1}^{m} |\tilde{l}'\rangle\rangle = \sum_{i=1}^{m} |\tilde{l}''\rangle\rangle = 1_A$. This is possible if and only if $|\tilde{l}'\rangle\rangle_{A}$ and $|\tilde{l}''\rangle\rangle_{A}$ are both scalar multiples of $1_A$. Thus if $\{|\tilde{l}|\tilde{l}\rangle\rangle\}_{i=1}^{m}$ is OP, then so are $|\tilde{l}'\rangle\rangle_{A}$ and $|\tilde{l}''\rangle\rangle_{A}$. This implies that for $\text{proj}_{\tilde{l}''\rangle\rangle}m_i$ (and $\text{proj}_{\tilde{l}''\rangle\rangle}m_i$) is OP, Alice can commence protocol with $|\tilde{l}'\rangle\rangle_{A}$ or $|\tilde{l}''\rangle\rangle_{A}$. Thus, if $\rho_{\alpha}^{(1)}, \rho_{\alpha}^{(2)}, \ldots, \rho_{\alpha}^{(n)}$ are $1$-LOOC distinguishable, Alice can always choose her starting measurement to be an extremal rank-one POVM.

\textbf{Theorem 2}. $\rho_{\alpha}^{(1)}, \rho_{\alpha}^{(2)}, \ldots, \rho_{\alpha}^{(n)}$ are $1$-LOOC distinguishable if and only if $T_1$ contains all elements of an extremal rank-one POVM.

\textbf{Proof}. \textbf{ONLY IF}: Assume that $\rho_{\alpha}^{(i)}$’s are $1$-LOOC distinguishable. Thus there exists an OP extremal rank-one POVM $\{|\tilde{l}|\tilde{l}\rangle\rangle\}_{i=1}^{m}$ on Alice’s side. Let Kraus operators of this measurement be $\{|\phi_i\rangle\langle \tilde{l}|\rangle\rangle_{i=1}^{m}$, where $\{|\phi_i\rangle\rangle_A$ are normalized. If the measurement outcome is $k$, the (unnormalized) $i$-th post-measurement state is $\langle \phi_i| k \rangle \tilde{l} |\phi_k\rangle |\tilde{l}\rangle$. Let $\rho_{\alpha}^{(i)} \mid k \rangle\rangle \langle k | \otimes 1_B \rangle_{\alpha}$, where $1_B$ is the identity operator acting on $H_B$. Since the $k$-th POVM element is OP, we get the following equations for all $1 \leq i < i' \leq n$, $1 \leq j < r_i$, and $1 \leq j' < r_{i'}$.

\begin{equation}
Tr \left( \langle \tilde{l}| k \rangle \langle k | \otimes 1_B \langle \tilde{l}'| k \rangle \langle k | \otimes 1_B \rangle \right) = 0, \tag{4}
\end{equation}

\begin{equation}
\Rightarrow \langle \rho_{\alpha}^{(i)} \rangle^2 \langle \tilde{l}| k \rangle \langle k | \otimes 1_B \rangle = 0, \tag{5}
\end{equation}

\begin{equation}
\Rightarrow \langle \psi_{ij}| \langle \tilde{l}| k \rangle \langle k | \otimes 1_B \rangle \rangle_{AB} = 0. \tag{6}
\end{equation}

Since $\{|\tilde{l}|\tilde{l}\rangle\rangle\}_{i=1}^{m}$ is a POVM, there exists an $m \times d$ isometry matrix $U$ such that $\rho_{\alpha}^{(i)} \equiv \sum_{n=1}^{m} U_{il} |\tilde{l}\rangle\rangle = 0$. Using $U$, define the following $m$ vectors in $C^d$: $|\tilde{l}^1\rangle = (U_{i1}, U_{i2}, \ldots, U_{id})^T$. Then $|\psi_{ij}\rangle = U_{ij}$. Using this in equation (5) implies that $\langle \tilde{l}^1| W_k \rangle |\tilde{l}^1\rangle = 0$ which implies that $\langle \tilde{l}^1| H_k |\tilde{l}^1\rangle = \langle \tilde{l}^1| A_k |\tilde{l}^1\rangle = 0$, $\forall i \in I$. Thus $|\tilde{l}^1\rangle = \langle \tilde{l}^1| \otimes 1_B \rangle_{\alpha}$ is an extremal rank-one POVM contained in $T_1$. IF Let $\{|\tilde{l}^i\rangle |\tilde{l}^i\rangle\}_{i=1}^{m} \subset T_1$, be an extremal rank-one POVM. It is readily seen that arguments presented in the ONLY IF part can be traced backwards to conclude that Alice has a corresponding extremal rank-one OP POVM of the form $\{|\tilde{l}|\tilde{l}\rangle\rangle\}_{i=1}^{m}$.

If Bob were to start protocol, one would have to check if $T_{\perp}$ contains all elements of some rank-one POVM, instead of $T_{\perp}$ (denoted by $T^{\perp}$ here). Note that $T_{\perp}$ is defined to be the complement of $T$ in $S$, where $T$ is defined just such as $\tilde{T}$ was in equation (3), with the difference that $W_i \equiv W_{ij} W_{i'j'}^{-1}$, not $W_{ij} W_{i'j'}^{-1}$. Any $d$ dimensional subspace of $S$ is called a maximally abelian subspace (MAS) if all matrices in it commute. Any MAS can be associated with a unique common eigenbasis such that all hermitian matrices, which are diagonal in said common eigenbasis, lie in the MAS.

\textbf{Corollary 2.1}. $\rho_{\alpha}^{(1)}, \rho_{\alpha}^{(2)}, \ldots, \rho_{\alpha}^{(n)}$ are $1$-LOOC distinguishable using only projective measurements on $H_A$ and $H_B$, if and only if $T_1$ contains a MAS.

\textbf{Proof}. \textbf{ONLY IF}: Let $\rho_{\alpha}^{(i)}$ be a $1$-LOOC distinguishable using only projective measurements on $H_A$ and $H_B$. Thus Alice can initiate protocol by an OP rank-one projective measurement $\{|\tilde{l}|\otimes 1_B \rangle\rangle_{k=1}^{d}$. Then theorem 2 (ONLY IF part) implies that $T_1$ contains all projectors of a rank-one projective measurement $\{|\tilde{l}^1\rangle \rangle_{\alpha}=1\}$ span $\{|\tilde{l}^1\rangle \rangle_{\alpha}=1\}$. Hence $\{|\tilde{l}^1\rangle \rangle_{\alpha}=1\}$ is a MAS in $T_1$. IF: Assume that $T_1$ contains a MAS of $S$. This MAS contains all
matrices which are diagonal in MAS’s common eigenbasis $\{|k\rangle k\rangle \rangle_{k=1}$. Thus this MAS contains the subset $\{|k\rangle k\rangle \rangle_{k=1}$, which is a rank-one projective measurement. Then theorem (IF part) implies that $\rho_{AB}^{(i)}$’s are 1-LOCC distinguishable by projective measurements. □

The significance of corollary 2.2 is that for certain values of $\dim T_{\alpha}$, it is easy to check if $T_{\alpha}$ contains a MAS or not, which immediately indicates the existence or nonexistence of a 1-LOCC protocol (using only rank-one projective measurements).

Non-existence of a MAS in $T_{\alpha}$ does not rule out the existence of a non-projective extremal rank-one POVM $\{|l\rangle\langle l|\rangle_{l=1}$ in $T_{\alpha}$, where $m > d$. Theorem 2 implies that if $T_{\alpha}$ contains $\{|l\rangle\langle l|\rangle_{l=1}$, then there exists a 1-LOCC distinguishability protocol which commences with an OP non-projective extremal rank-one POVM $\{|l\rangle\langle l|\rangle_{l=1}$. Then one can consider $T_{\alpha}$ to be a d-dimensional subspace of an extended m-dimensional space $\mathcal{H}_{\alpha}$, so that $|\psi_{i}\rangle_{AB} \rightarrow |\psi_{i}\rangle_{AB}$ lie in $\mathcal{H}_{\alpha} \cong \mathcal{H}_{\alpha} \otimes \mathcal{H}_{B}$. Then $T_{\alpha}$, $T_{\alpha}$ and $T_{\alpha}$ are spaces of $m \times m$ hermitian matrices corresponding to Alice’s extended space $\mathcal{H}_{\alpha}$, and $T_{\alpha}$ will contain a m-dimensional MAS, which corresponds to an m-element rank one projective measurement on $\mathcal{H}_{\alpha}$. This m-element projective measurement reduces to $\{|l\rangle\langle l|\rangle_{l=1}$ when $\mathcal{H}_{\alpha}$ is limited to $\mathcal{H}_{\alpha}$. Note that since $\dim T_{\alpha}$ elements of any extremal rank-one POVM are linearly independent (LI), $m \leq d$. It is sensible to search for an m-dimensional MAS in $T_{\alpha}$ after confirming that $T_{\alpha}$ doesn’t contain a d-dimensional MAS. Often the value of $\dim T_{\alpha}$ itself gives information about OP rank-one POVM’s which Alice can perform, e.g., Walgate et al’s result, that any two orthogonal bipartite pure states are 1-LOCC distinguishable, which corresponds to the cases $\dim T_{\alpha} \geq d^{2} - 2$. I give an alternative proof of Walgate et al’s result in the supplemental material.□

Another example: when $\dim T_{\alpha} = 1$, $\rho_{AB}^{(i)}$’s aren’t distinguishable by LOCC at all $\alpha$’s. For 1-LOCC, corollary 2.2 makes a stronger statement.

Corollary 2.2. If $\dim T_{\alpha} \leq d - 1$, there is no 1-LOCC protocol which Alice can initiate to distinguish the states.

Proof. If $\dim T_{\alpha} \leq d - 1$, $T_{\alpha}$ can’t contain all m (≥ d) LI elements of an extremal rank-one POVM. Then theorem 2 implies that there is no such protocol. □

Corollary 2.3. When $\dim T_{\alpha} = d$, states are 1-LOCC distinguishable if and only if $T_{\alpha}$ is a MAS of $\mathcal{S}$. □

Proof. IF: Already covered in corollary 2.2 ONLY IF: Given that $\dim T_{\alpha} = d$ and the states are 1-LOCC distinguishable. Theorem 2 implies that $T_{\alpha}$ contains all POVM elements of an extremal rank-one POVM $\{|k\rangle\langle k|\rangle_{k=1}$, since $\dim T_{\alpha} = d$, elements of an extremal rank-one POVM being LI implies that $m = d$. Thus the isometric matrix relating $\{|k\rangle\rangle_{k=1}$ to an ONB of $\mathbb{C}^{d}$ has to be a $d \times d$ unitary matrix, which implies that $\{|k\rangle\langle k|\rangle_{k=1} \rightarrow \{|k\rangle\langle k|\rangle_{k=1}$ is a rank-one projective measurement. Since span $\{|k\rangle\langle k|\rangle_{k=1}$ = $T_{\alpha}$, $T_{\alpha}$ is a MAS of $\mathcal{S}$. □

Consider the case when $n = d$ and the states are pure: $\rho_{AB}^{(i)} \rightarrow |\psi_{i}\rangle_{AB}$. Then the index set $I$ is $(i, k)$, $1 \leq i < k \leq d$. The cardinality of $I$ now is $\frac{d(d-1)}{2}$. One can generally expect $\{A_{i}: A_{i} \in \mathcal{S}\}$ to be a LI set, which implies that $\dim T = d(d - 1)$ and $\dim T_{\alpha} = d$ for almost all sets of $d$ orthogonal states in $\mathcal{H}_{\alpha} \otimes \mathcal{H}_{B}$. This is indeed true; proof for this was essentially given by Cohen in [4], where he showed that almost all sets of $n \geq d + 1$ orthogonal multiparticle qudit states in $d^{\otimes N}$ systems ($N \geq 2$) are locally indistinguishable, but for the sake of completeness I give a rigorous proof for this case in the supplemental material.7. Thus corollary 2.3 gives the necessary and sufficient condition for the 1-LOCC distinguishability of almost all sets of d orthogonal pure states from $\mathcal{H}_{\alpha} \otimes \mathcal{H}_{B}$. Next, consider an example of this.

Example 1. Define the following states in $\mathbb{C}^{4} \otimes \mathbb{C}^{4}$:

$$|\psi_{m}\rangle_{AB} = \sum_{j,k=0}^{3} (W_{m})_{jk} |s_{j}\rangle_{A} |s_{k}\rangle_{B},$$

(7)

where $(W_{m})_{jk} = \frac{\delta_{m,0}}{\sqrt{2^{k}}} \delta_{p,m,k}, \forall j,k = 0, 1, 2, 3$. Note that any two $W_{m}$ states are pairwise orthogonal. For 1-LOCC of the states $\{|\psi_{m}\rangle_{AB}, |\psi_{m}'\rangle_{AB}\}$, $\{\psi_{m}\rangle_{AB}, |\psi_{m}'\rangle_{AB}\}$, $\mathcal{I}$ is spanned by the hermitian matrices:

$$\begin{align*}
W_{00} - W_{00}, & W_{01} - W_{01}, W_{02} - W_{02}, W_{03} - W_{03}, \\
W_{10} - W_{10}, & W_{11} - W_{11}, W_{12} - W_{12}, W_{13} - W_{13}, \\
W_{20} - W_{20}, & W_{21} - W_{21}, W_{22} - W_{22}, W_{23} - W_{23}, \\
W_{30} - W_{30}, & W_{31} - W_{31}, W_{32} - W_{32}, W_{33} - W_{33}.
\end{align*}$$

Hence $\dim \mathcal{I} = 12$. Thus $\dim T_{\alpha} = 4$, where $T_{\alpha}$ is spanned by the hermitian matrices $I_{4}$, $W_{22}$, $W_{02}$, and $W_{20}$. Note that all these matrices commute with each other. Thus $T_{\alpha}$ is a MAS. The common eigenbasis, which diagonalizes any matrix in $T_{\alpha}$ is $\{\frac{1}{\sqrt{2}}(1, 0, 1, 0)^{T}, \frac{1}{\sqrt{2}}(1, 0, -1, 1)^{T}, \frac{1}{\sqrt{2}}(1, 0, 1, 0)^{T}, \frac{1}{\sqrt{2}}(1, 0, 0, -1)^{T}\}$. It’s then seen that Alice can initiate a 1-LOCC protocol to distinguish the given set of states by performing rank-one projective measurement in the ONB $\{\frac{1}{\sqrt{2}}(1, 0, 1, 0)^{T}, \frac{1}{\sqrt{2}}(1, 0, -1, 1)^{T}, \frac{1}{\sqrt{2}}(1, 0, 1, 0)^{T}, \frac{1}{\sqrt{2}}(1, 0, 0, -1)^{T}\}$.

So when $\dim T_{\alpha} \leq d$ or $\dim T_{\alpha} \geq d^{2} - 2$, one can conclude if $T_{\alpha}$ contains a MAS or not. When $d + 1 \leq \dim T_{\alpha} \leq d^{2} - 3$, it is difficult to establish the same, but one can give partial results. Let $\dim T_{\alpha} = d + t$, where $t \geq 1$. Let $\{T_{\alpha}\}_{i=1}^{d+t}$ be an ONB for $T_{\alpha}$. Let $C$ be the real vector space, spanned by matrices in $\{i|T_{\alpha} \rangle_{\alpha} |T_{\alpha} \rangle_{\alpha}\} |1 \leq j < k \leq d + t\}$, where $|T_{\alpha} \rangle_{\alpha} \equiv |T_{\alpha} \rangle_{k} - |T_{\alpha} \rangle_{j}$. □

Theorem 3. When $1 \leq t \leq \sqrt{3d^{2} - 3d + \frac{1}{4} - (d - \frac{3}{2})^{2}}$, $T_{\alpha}$ contains no MAS if $\dim C > td + \frac{t(t+3)}{2}$.

Proof. If $T_{\alpha}$ contains a MAS, choose $\{T_{\alpha}\}_{i=1}^{d+t}$ such that $\{T_{\alpha}\}_{i=1}^{d+t}$ is an ONB for this MAS. Then number of non-zero commutators in $\{i|T_{\alpha} \rangle_{\alpha} |T_{\alpha} \rangle_{\alpha}\}$ is at most $td + \frac{t(t+3)}{2}$, implying that $\dim C$ can be at most $\text{Min}\{td + \frac{t(t+3)}{2}, d^{2} - 1\}$. When $1 \leq t \leq \sqrt{3d^{2} - 3d + \frac{1}{4} - (d - \frac{3}{2})^{2}}$ then $d \leq td + \frac{t(t+3)}{2} \leq d^{2} - 1$. Then if $\dim C > td + \frac{t(t+3)}{2}$, $T_{\alpha}$ contains no MAS.
For \( \dim T_L = d + 1 \), I give necessary and sufficient conditions for \( T_L \) to contain a MAS. Let \( \{G_j\}_{j=1}^{d+\tilde{\varphi}} \) be an ONB for \( C \). For each \( j \in \{1, 2, \cdots, \dim C\} \), define \( d+1 \times d+1 \) real antisymmetric matrix \( \Gamma_j \), whose matrix elements are given by \( (\Gamma_{jk})_{ik} = it\Gamma_j(G_j[T_k, T_j]) \). Let \( G \) be the real vector space spanned by the \( \Gamma_j \)'s. Let \( \{\Omega_j\}_{j=1}^{d+\tilde{\varphi}} \) be an ONB for \( G \). Theorem 4 follows us to assume that \( \dim G \leq d - 1 \), which implies \( \dim G \leq d - 1 \).

**Theorem 4.** When \( \dim T_L = d + 1 \), \( T_L \) contains a MAS if and only if \( \Omega_j \) is rank 2 for all \( j = 1, 2, \cdots, \dim G \) and \( \bigcap_{j=1}^{d+\tilde{\varphi}} \text{Supp}(\Omega_j) \) is one dimensional.

**Proof.** Assume that \( \Omega_j \) is rank 2, \( \forall 1 \leq j \leq \dim G \), and \( \bigcap_{j=1}^{d+\tilde{\varphi}} \text{Supp}(\Omega_j) \) is one dimensional, spanned by the real \((d+1)\)-tuple \( e_{j+1} \equiv (e_1, e_2, \cdots, e_{d+1})^T \). Since \( \Omega_j \) is anti-symmetric and \( \forall 1 \leq j \leq \dim G \), it is required that \( e_j^T e_j' = 0 \). Let \( \Gamma_j = \sum_{k=1}^{d+\tilde{\varphi}} \alpha_k \Omega_k = e_{j+1} g_j^T - g_j e_{j+1}^T \), where \( g_j \equiv \sum_{k=1}^{d+\tilde{\varphi}} \alpha_k e_k \). Hence \( \Gamma_j \) are also rank 2 matrices. Complete the ONB \( \{e_1, e_2, \cdots, e_{d+1}, e_{d+2}, \cdots, e_{d+1}\} \) one can normalize \( e_j \) so that \( \langle e_j, e_j' \rangle = 1 \). Let \( O_{\Omega_j} \equiv \sum_{k=1}^{d+\tilde{\varphi}} \Omega_k T_k \). Since \( T_k \in T_L \), \( \{T_k, T_l\} \in C \). But since \( \{G_j\}_{j=1}^{d+\tilde{\varphi}} \) is an ONB for \( C \), equation [8] implies that \( \langle T_k, T_l \rangle = 0 \). Thus \( \{T_k\}_{k=1}^{d+1} \) spans a MAS in \( T_L \). \( \text{ONLY IF} \)

Assume \( T_L \) contains a MAS and let \( \{T_k\}_{k=1}^{d+1} \) be an ONB for this MAS. Then \( \text{Tr}(G_j[T_k, T_j]) = 0 \) when \( 1 \leq k, l \leq d \). Thus the \( d \times d \) upper diagonal block of \( \Gamma_j \) is zero, which makes it a rank 2 matrix. The same is true for \( \{\Omega_j\}_{j=1}^{d+\tilde{\varphi}} \). Hence, I argue that a deeper study of this structure will be a rewarding experience for studying problems of distinguishability of orthogonal states by LOCC. Hence, I argue that a deeper study of this structure will be a rewarding experience for studying problems of distinguishability of orthogonal states by LOCC.

**ACKNOWLEDGMENTS**

I thank the first and the third referees for their useful comments. I also thank my PhD. adviser Sibasish Ghosh for his help.

**Supplemental Material**

**I. EXTREMALITY OF POVMs**

Consider two POVMs with elements \( \{M_j^{(1)}\}_{j=1}^{m_1} \) and \( \{M_j^{(2)}\}_{j=1}^{m_2} \), where \( \sum_{j=1}^{m_j} M_j^{(i)} = 1_A \) (where \( 1_A \) is the identity operator acting on \( H_A \)), for \( i = 1, 2 \). Define \( E_j^{(1)} \) to be an ordered \((m_1 + m_2)\)-tuple of observables acting on \( H_A \), such that the \( k \)-th component of \( E_j^{(1)} \), i.e., \( E_k^{(1)} \)
is either a POVM element $M_j^{(i)}$ or is the null observable 0 acting on $H_A$, and also let $E^{(i)}$ be such that each POVM element from $\{M_j^{(i)} \}_{j=1}^{m_i}$ appears once as a component of $E^{(i)}$. Depending on the arrangement of $M_j^{(i)}$s as components of $E^{(i)}$, there are $\frac{(m_1+\cdots+m_m)!}{m_1!\cdots m_m!}$ such distinct ordered tuples $E^{(i)}$ corresponding to the POVM $\{M_j^{(i)} \}_{j=1}^{m_i}$. Define $E^{(i)}$ similarly for the second POVM. Choosing some two outcome probability $(p,1-p)$, (where $0 \leq p \leq q$), one can obtain a new POVM by pointwise addition of components of $E^{(i)}$ and $E^{(ii)}$, i.e., the set $\{ pE^{(i)} + (1-p)E^{(ii)} \}$, $\forall 1 \leq k \leq m_1 + m_2 : pE^{(i)} + (1-p)E^{(ii)} \neq 0$ contains all elements of a POVM which is obtained from the convex sum of the original POVMs. In this way, the set of all POVMs is a convex set. An extremal POVM in this set is one which cannot be written as a convex sum (in the aforementioned fashion) of two or more distinct POVMs.

It is also not necessary for a rank-one POVM to be an extremal rank-one POVM. For example, for $d=2$, consider the following POVM elements: $\{ \frac{1}{\sqrt{2}} |0\rangle \langle 0| + |1\rangle \langle 1| \}$ and $\{ |+\rangle \langle +| - |\rangle \langle | \}$. This POVM is non-extremal because it can be written as a convex sum of two POVMs, $\{ |0\rangle \langle 0| + |1\rangle \langle 1| \}$ and $\{ |+\rangle \langle +| - |\rangle \langle | \}$. The POVMs $\{ |0\rangle \langle 0| + |1\rangle \langle 1| \}$ and $\{ |+\rangle \langle +| - |\rangle \langle | \}$ are extremal because they cannot be written as convex sums of other POVMs. Also, an extremal rank-one POVM need not be a rank-one projective POVM. For instance, let $\{ \tilde{v}_1 \} \equiv \frac{1}{\sqrt{2}} |0\rangle \langle 0| + |1\rangle \langle 1| \}$ and $\{ \tilde{v}_3 \} \equiv \frac{1}{\sqrt{2}} |0\rangle \langle 0| - |1\rangle \langle 1| \}$; then the set $\{ |\tilde{v}_1\rangle \langle \tilde{v}_1|, |\tilde{v}_2\rangle \langle \tilde{v}_2|, |\tilde{v}_3\rangle \langle \tilde{v}_3| \}$ is an extremal but non-projective POVM. That said all rank-one projective measurements are extremal. A necessary and sufficient condition for extremality of POVMs in terms of the Kraus operators of said measurement was first given by Choi [S10]; it can be easily checked that the aforementioned POVM whose elements were $\{ |\tilde{v}_i\rangle \langle \tilde{v}_i| \}_{i=1}^{3}$, satisfy these necessary and sufficient conditions for be an extremal POVM.

II. AN ALTERNATIVE PROOF TO WALGATE ET AL’S RESULT [S2]

Walgate et al’s result [S2] states that any two multipartite orthogonal pure states are always locally distinguishable. Their paper shows that the result for the multipartite case follows straightforwardly from the result for the bipartite case. Their proof for the bipartite case is constructive, i.e., they show that for any two orthogonal bipartite states there exists a 1-LOCC protocol which Alice and Bob can perform to distinguish the two states. That said their protocol is complicated by the fact that the starting party (assumed here to always be Alice) has to perform SWAPPING operations onto a bigger subsystem.

This result by Walgate corresponds to the case where $n=2$, i.e., all sets of two orthogonal bipartite states come within the classes corresponding to $\dim T_2 \geq d^2 - 2$. Here I show that when $\dim T_2 \geq d^2 - 2$, $T_2$ always contains a MAS, implying the Alice can initiate the 1-LOCC protocol by performing an OP rank-one projective measurement. Such a protocol is devoid of requiring any SWAPPING operations onto a bigger system.

Theorem 5. When $\dim T_2 \geq d^2 - 2$, $T_2$ always contains a MAS.

Proof. This proof is by induction. Assume that $\dim T_2 = d^2 - 2$. This implies that $\dim T = 2$. Let $A$ and $B$ be two linearly independent $d \times d$ matrices in $T$. Proposition $P(d)$: For any two $d \times d$ hermitian matrices $H$ and $A$, there exists a $d \times d$ unitary $U$, so that the diagonals of $U^\dagger U$ and $U^\dagger AU$ are multiples of $\frac{1}{\sqrt{d}}$. It’s known that $P(2)$ is true [S2]. The goal is to prove that $P(d+1)$ is true assuming that $P(d)$ is true. Let $H$ and $A$ be two $d+1 \times d+1$ traceless hermitian matrices. Let $H_{d+1}$ and $A_{d+1}$ be their $d \times d$ upper diagonal blocks. Since $P(d)$ is true, there is a $d \times d$ unitary $V_d$, so that diagonals of $V_d^\dagger H_d V_d$ and $V_d^\dagger A_d V_d$ are multiples of $\frac{1}{\sqrt{d}}$. Embed $V_d$ as the $d \times d$ upper diagonal block of a $d+1 \times d+1$ unitary $V$ whose $d+1$-th diagonal element is 1. Then it is easy to see that the diagonals of the $d \times d$ upper diagonal block of $V^\dagger Hv$ and $V^\dagger Av$ are scalar multiples of $\frac{1}{\sqrt{d}}$. Since $V^\dagger Hv$ and $V^\dagger Av$ are traceless, their diagonals are scalar multiples of $\text{matrix } D_1 \equiv \frac{1}{\sqrt{d(d+1)}} \text{Diag}(1,1,\cdots,1,-d)$, which is traceless. Let $V^\dagger Hv$ and $V^\dagger Av$ have components $\alpha$ and $\beta \in R$ along $D_1$. Then $A' \equiv \frac{\sqrt{\alpha^2 + \beta^2}}{\sqrt{d}} (-\beta V^\dagger Hv + \alpha V^\dagger Av)$ has a zero diagonal, and component of $D_1$ along $H' \equiv \frac{\alpha V^\dagger Hv + \beta V^\dagger Av}{\sqrt{\alpha^2 + \beta^2}}$ is 1. Let the $(d,d+1)$-th matrix element of $A'$ be $ae^{-i\theta}$. Define $D_a \equiv \text{Diag}(1,1,\cdots,1,e^{\frac{i\pi}{d+1}},e^{\frac{i\pi}{d+2}})$, then the $2 \times 2$ lower diagonal block of $A'' \equiv D_a A' D_a^\dagger$ is a scalar multiple of $\sigma_y$. The diagonal of $H'' \equiv D_a^\dagger H' D_a$ remains invariant. Let the real part of the $(d,d+1)$-th matrix element of $H''$ be $h$. Using an $(SO(2)$ transformation, rotate between the $d$-th and $d+1$-th matrix elements of $H''$ to obtain $H'''$, while keeping all other elements fixed. $A''$ will remain invariant. Thus the real part of the $2 \times 2$ lower diagonal block of $H'''$ will undergo the transformation

$$
\begin{array}{c|c|c|c|c}
1 & h & -d & 0 \\
-h & -d & 0 & 1 \\
0 & 0 & 0 & 0 \\
\end{array}
\leftrightarrow
\begin{array}{c|c|c|c|c}
\cos \frac{\theta}{2} & \sin \frac{\theta}{2} & \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\
-\sin \frac{\theta}{2} & \cos \frac{\theta}{2} & \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \\
\hline
\frac{1-d}{2} + \frac{1+d}{2} \cos \theta - \frac{h \sin \theta}{2} & \frac{1+d}{2} \sin \theta + \frac{h \cos \theta}{2} & \frac{1+d}{2} \sin \theta + \frac{h \cos \theta}{2} & \frac{1+d}{2} \sin \theta - \frac{h \cos \theta}{2} \\
\frac{1+d}{2} \sin \theta - \frac{h \cos \theta}{2} & \frac{1-d}{2} - \frac{1+d}{2} \cos \theta + \frac{h \sin \theta}{2} & \frac{1-d}{2} - \frac{1+d}{2} \cos \theta + \frac{h \sin \theta}{2} & \frac{1-d}{2} + \frac{1+d}{2} \cos \theta - \frac{h \sin \theta}{2} \\
\end{array}
$$

I want to solve for $\theta$ in the equation: $\frac{1-d}{2} + \frac{1+d}{2} \cos \theta - \frac{h \sin \theta}{2} = 0$. When $\theta = 0$, the LHS is $-d$ and when $\theta = \pi$, the LHS is 1. Since the LHS is a continuous function of $\theta$, there must be some $\theta \in (0,\pi)$ for which the LHS is zero. Choose $\theta$ to be this value. Then $H'''$ and $A''$ are matrices whose $d+1$-th diagonal elements are both zero. Using $P(d)$ on the $d \times d$ upper diagonal blocks of $H'''$ and $A''$, $H'''$ and $A''$ can be rotated to obtain corresponding matrices whose diagonal zero and which span the correspondingly rotated $T_2$. Then the correspondingly
rotated $T_\perp$ contains all diagonal matrices which span a MAS.

III. ALMOST ALL SETS OF d ORTHOGONAL BIPARTITE PURE STATES IN $\mathcal{H}_A \otimes \mathcal{H}_B$ CORRESPOND TO THE CASE $\dim T_\perp = d$

This proof is similar to the Cohen’s proof of theorem 1 in [4].

Denote $\mathcal{G}(n, d)$ as the manifold of all sets of $n$ orthogonal bipartite pure states $\{\ket{\psi}_i\}_{i=1}^n \subset \mathcal{H}_A \otimes \mathcal{H}_B$, where $\bra{\psi}_i \bra{\psi}_j = \delta_{ij}$, $\forall 1 \leq i < j \leq n$. Hence every point in $\mathcal{G}(n, d)$ is associated with a set of $d \times d$ orthonormal complex matrices $\{W_i\}_{i=1}^n$ (see equation (2) in main text), i.e., $\text{Tr}(W_i^\dagger W_j) = \delta_{ij}$, $\forall 1 \leq i < j \leq n$. Hence every point in $\mathcal{G}(n, d)$ is associated with a set of $d \times d$ orthonormal complex matrices $\{W_i\}_{i=1}^n$ (see equation (2) in main text), i.e., $\text{Tr}(W_i^\dagger W_j) = \delta_{ij}$, $\forall 1 \leq i < j \leq n$. Let’s represent the rows of $W_i$ as $w_{i1}, w_{i2}, \ldots, w_{id}$. Vectorize the $W_i$ matrices by arranging these rows $\{w_{i\ell}\}_{\ell=1}^d$ as complex $d^2$-tuples, i.e., $(w_{i1}, w_{i2}, \ldots, w_{id}) \in \mathbb{C}^{d^2}$, and arrange these vectorized $W_i$’s as the first upper $n$ rows of a $d^2 \times d^2$ unitary matrix $U$, whose remaining rows are arbitrary (also as the matrix remains unitary). Hence any point of $\mathcal{G}(n, d)$ can be associated with the first upper $n$ columns of a $d^2 \times d^2$ unitary matrix $U \in U(d^2)$. In fact, since the overall phases of these $n$ columns, the permutation of the order of their appearance in the set of first $d$ columns of $U$ and the rest of the $d^2 - n$ columns in $U$ are insignificant to describe the corresponding set of orthogonal pure states from $\mathcal{H}_A \otimes \mathcal{H}_B$, the manifold $\mathcal{G}(n, d)$ is given by $U(d^2)/(U(1)^\times n \times S_n \times U(d^2 - n))$. This is a real manifold.

Let $u(d^2)$ be the space of all $d^2 \times d^2$ hermitian matrices, then it is the space of generators for $d^2 \times d^2$ unitary matrices, i.e., if $G \in u(d^2)$, then $e^{i\alpha}G$ is a $d^2 \times d^2$ unitary matrix. Associate the ordered set of the first $n$ rows of $e^{-i\alpha}$ with the set of $n$ vectorized $W_i$’s. Then the set $\{W_i\}_{i=1}^n$ corresponds to some set of $n$ orthonormal states $\{\ket{\psi}_{AB}\}_{i=1}^n$. This maps any $G \in u(d^2)$ to a point in $\mathcal{G}(n, d)$ unambiguously. Let’s denote this map by $\mathcal{D} : u(d^2) \rightarrow \mathcal{G}(n, d)$. So $\mathcal{D}(G)$ is a point in $\mathcal{G}(n, d)$ corresponding to $\{\ket{\psi}_{AB}\}_{i=1}^n$. In the following I specify norm-induced metric for various spaces.

1. Metric for all $d^2 \times d^2$ matrices is given by the standard Hilbert Schmidt norm.

2. Let $\{A_i\}_{i=1}^n$ be an arbitrary set of $n$ complex $d \times d$ matrices, then $\|\{A_i\}_{i=1}^n\| = \left(\sum_{i=1}^n \text{Tr}(A_i^\dagger A_i)\right)^{1/2}$.

3. Let $\{\eta_i\}_{AB}\}_{i=1}^n$ be a set of $n$ arbitrary vectors in $\mathcal{H}_A \otimes \mathcal{H}_B$, then $\|\{\eta_i\}_{AB}\}_{i=1}^n\| = \left(\sum_{i=1}^n \langle \eta_i | \eta_i \rangle_{AB}\right)^{1/2}$.

Then $G \rightarrow e^{-i\alpha}$ is continuous, $e^{-i\alpha} \rightarrow \{W_i\}_{i=1}^n$ is continuous and $\{W_i\}_{i=1}^n \rightarrow \{\ket{\psi}_{AB}\}_{i=1}^n$ is continuous. This implies that $\mathcal{D}$ is continuous. It is easy to see that $\mathcal{D}$ is onto but not one-to-one.

For any set of $n$ orthonormal states $\{\ket{\psi}_{AB}\}_{i=1}^n$, one can obtain the $d(d - 1)$ matrices $\{R_iA_1\}_{i=1}^n$. Vectorize each of these matrices and arrange them as rows of a $n(n - 1) \times d^2$ matrix $M$. Define $\mathcal{D} : \mathcal{G}(n, d) \rightarrow \mathbb{R}$ by $\mathcal{D}(\{\ket{\psi}_{AB}\}_{i=1}^n) = \text{Det}(M M^\dagger)$. The goal is to establish that for no point in $\mathcal{G}(n, d)$ there is an open neighbourhood $\mathcal{N}$ containing said point such that $\mathcal{D}$ vanishes entirely in $\mathcal{N}$. Since $\mathcal{D}$ is continuous on $\mathcal{G}(n, d)$ and $\mathcal{D}$ is continuous on $u(d^2)$, $\mathcal{D} \circ \mathcal{D}$ is continuous on $u(d^2)$. Hence, if $\mathcal{D}$ vanishes entirely in some open neighbourhood $\mathcal{N}$ of $\{\ket{\psi}_{AB}\}_{i=1}^n$ in $\mathcal{G}(n, d)$, then there is some open neighbourhood of $\mathcal{O}$ in $u(d^2)$ where $\mathcal{D} \circ \mathcal{D}$ vanishes entirely too. Hence one needs to show that $\mathcal{D} \circ \mathcal{D}$ doesn’t vanish entirely in any open neighbourhood of any point in $\mathcal{G}(n, d)$.

Let $\{\lambda_i\}_{i=1}^n$ be an ONB for $u(d^2)$. Let $G = \lambda \lambda^\dagger$ be a point in $u(d^2)$ which has an open neighbourhood $\mathcal{N}$ in which $\mathcal{D} \circ \mathcal{D}$ vanishes entirely. Then there exists some $\epsilon \in \mathbb{R}$ be such that $(\lambda + \epsilon \hat{n}) \lambda^\dagger \in \mathcal{N}$ for all unit vectors $\hat{n}$ lying on $S^{d-1}$.

Then $e^{-i(\alpha + \epsilon \hat{n}) \lambda} = e^{-i\epsilon \hat{n}} \lambda$

$$+ \epsilon (-i\hat{n} \lambda) + \frac{(\hat{n} \lambda)(\lambda + \alpha) + (\alpha \lambda)(\hat{n} \lambda)}{2!} + \frac{(\hat{n} \lambda)(\hat{n} \lambda)(\lambda + \alpha) + (\alpha \lambda)(\hat{n} \lambda)^2}{3!} + \cdots \quad (S1)$$

Hence it is easy to see that as $G \rightarrow G + \epsilon \hat{n} \lambda$, the $W_i$ matrices transform as $W_i \rightarrow W_i + \epsilon W_i^{(1)}(\hat{n}) + e W_i^{(2)}(\hat{n}) + O(\epsilon^3)$, where $e W_i^{(1)}(\hat{n})$ is the first order change in $\epsilon$, $e W_i^{(2)}(\hat{n})$ is the second order change in $\epsilon$ and so on. Since equation $S1$ gives the Taylor series expansion of $e^{-i(\alpha + \epsilon \hat{n}) \lambda}$ about $\epsilon = 0$, $W_i + \sum_{k=1}^\infty \epsilon^k W_i^{(k)}(\hat{n})$ is the Taylor series expansion of about $\epsilon = 0$. In fact the radius of convergence for the latter is determined by the former, and since the expression in $S1$ converges for all $\epsilon \in \mathbb{R}$ for the former, it does so too for the latter. Now $\mathcal{D}(\{\ket{\psi}_{AB}\}_{i=1}^n)$ is $\text{Det}(M M^\dagger)$ is a polynomial of the matrix elements of $W_i$. So when $W_i$ goes
to \( W_i + \sum_{k=1}^{\infty} \epsilon^k W_i^{(k)}(\hat{n}) \), \((\mathcal{D} \circ R)(G) \rightarrow (\mathcal{D} \circ R)(G) + \epsilon(\mathcal{D} \circ R)^{(1)}(\hat{n}) + \epsilon^2(\mathcal{D} \circ R)^{(2)}(\hat{n}) + \mathcal{O}(\epsilon^3)\), where 
\[ \epsilon(\mathcal{D} \circ R)^{(1)}(\hat{n}) \]
is the first order change in \( \epsilon \), \( \epsilon^2(\mathcal{D} \circ R)^{(2)}(\hat{n}) \)
is the second order change in \( \epsilon \) and so on. Note that 
\[ (\mathcal{D} \circ R)(G) + \sum_{k=1}^{\infty} \epsilon^k (\mathcal{D} \circ R)^{(k)}(\hat{n}) \]
is the Taylor series of \( \mathcal{D} \circ R \) about \( G \) in the direction \( \hat{n} \). Since the Taylor series 
\[ W_i + \sum_{k=1}^{\infty} \epsilon^k W_i^{(k)}(\hat{n}) \]
covers all for all \( \epsilon \in \mathbb{R} \), and since \( \mathcal{D} \) is a polynomial in the matrix elements of 
\( W_i \), the radius of convergence for the Taylor expansion 
\[ (\mathcal{D} \circ R)(G) + \sum_{k=1}^{\infty} \epsilon^k (\mathcal{D} \circ R)^{(k)}(\hat{n}) \]
is \( \epsilon = \infty \).

Now let \( \mathcal{D} \circ R \) vanish in \( \hat{n} \). This implies that 
\[ (\mathcal{D} \circ R)(G + c\hat{n}) = 0 \]
for all \( \hat{n} \in S^{d-1} \) and \( c \in [0, \epsilon_s] \), where \( \epsilon_s \) was chosen so that 
\((\alpha + \epsilon_s \hat{n}).A = 0 \). The Taylor series of \( \mathcal{D} \circ R \) about \( G \) is a summation of monomials in \( \epsilon \), i.e., 
\[ (\mathcal{D} \circ R)^{(k)}(\hat{n}) \]
are linearly independent in the range \( \epsilon \in [0, \epsilon_s] \). Hence the only way 
that such a summation vanishes for all \( \epsilon \in [0, \epsilon_s] \) is if 
\[ (\mathcal{D}^{(k)}(\hat{n}) = 0 \]
for all \( k \in \mathbb{N} \) and \( \hat{n} \in S^{d-1} \), and if 
\[ (\mathcal{D} \circ R)(G) = 0 \]. But note that the radius of convergence for \( \epsilon \) in this Taylor series is \( \infty \). Hence \( \mathcal{D} \circ R \) vanishes all over \( u(d^2) \). And that implies that \( \mathcal{D} \) vanishes all over \( G(n, d) \). The following counter-example will disprove this: let 
\[ |\psi_i\rangle_{AB} \equiv |s_i\rangle_A |0\rangle_B \]
where \( |0\rangle_n \in H_B \). Then 
\[ T_{AB}|\psi_i\rangle(|\psi_i\rangle) = |s_i\rangle\langle s_i| \]
when \( i \neq i' \), so \( T \) is spanned by the complex conjugate of matrices representing 
\[ \frac{1}{d}(|s_i\rangle\langle s_i|) \]
and \( \frac{1}{d}(|s_{i'}\rangle\langle s_i| - |s_i\rangle\langle s_{i'}|) \), for all \( 1 \leq i < i' \leq d \), in the standard basis. All these matrices are linearly independent, so \( \text{dim} T_{AB} = d \) and 
\[ \mathcal{D}(\{|s_i\rangle_A |0\rangle_B\}_{i=1}^N) \neq 0 \]. Hence it is not possible for \( \mathcal{D} \) to 
vanish entirely in any open neighbourhood of any point in \( G(n, d) \). This also holds true for the particular case 
when \( n = d \).

[S1] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. 82, 5385 (1999).
[S2] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. 85, 4972 (2000).
[S3] P. Badziag, M. Horodecki, A. Sen(De), and U. Sen, Phys. Rev. Lett. 91, 117901 (2003).
[S4] S. M. Cohen, Phys. Rev. A 77, 060309 (2008).
[S5] M.-Y. Ye, W. Jiang, P.-X. Chen, Y.-S. Zhang, Z.-W. Zhou, and G.-C. Guo, Phys. Rev. A 76, 032329 (2007).
[S6] M. Nathanson, Phys. Rev. A 88, 062316 (2013).
[S7] See Supplemental Material at the end of this paper for the proofs of the following: (i) a brief explanation of convexity of POVMs and extremal POVMs, (ii) an alternative proof of Walgate’s result, i.e., if \( \text{dim} T_{AB} \geq d^2 - 2 \), then \( T_{AB} \) contains a MAS, and (iii) for almost all sets of \( d \)-orthogonal bipartite pure states in \( C^d \otimes C^d \), \( \text{dim} T_{AB} = d \).
[S8] G. M. D’Ariano, P. L. Presti, and P. Perinotti, J. Phys. A: Math. Gen. 38, 5979 (2005).
[S9] A. Chefles, Phys. Rev. A 69, 050307 (2004).
[S10] M.-D. Choi, Linear Algebra and its Applications 10, 285 (1975).