Multiparticle Entanglement Certification, With or Without Tomography

Nengku Yu

Abstract—Certifying multiparticle entanglement is a fundamental task. Since \( n \)-qubit state is parameterized by \( 4^n - 1 \) real numbers, it is interesting to design a measurement setup that detects multiparticle entanglement with as little effort as possible, and at a minimum without fully revealing the whole information of the state, the so-called “tomography”. In this paper, we study the relationship between multiparticle entanglement certification and tomography, with the constraint that only single-copy measurements are allowed. We show that by using nonadaptive single-copy measurements, universal entanglement detection, among all states, can not be accomplished without full state tomography. Moreover, we show that almost all multiparticle correlations, including the genuine entanglement and the entanglement depth, require full state tomography to detect in this measurement setting. We also observe that universal entanglement detection, among pure states, can be accomplished using much fewer measurements than full state tomography even using only local measurements.

Index Terms— Quantum entanglement, state estimation.

I. INTRODUCTION

QUANTUM computing offers the potential of considerable speedup over classical computing for a number of important problems such as factoring [1] and unstructured database search [2]. To take advantage of this possibility, entanglement, a striking feature of quantum many-body systems, must be available. With shared entanglement, two or more parties can be correlated in a way that is much stronger than when correlated in any of the classical ways. Entanglement has been widely studied ever since it was proved to be an asset to information processing and computational tasks. For instance, multipartite entanglement has been used as the central resource for quantum key distribution in multipartite cryptography [3]; it is the initial resource in measurement-based quantum computing [4]; it is essential in understanding quantum phase transitions [5]; and, arguably, multipartite entanglement could even be responsible for transport efficiency in biological systems [6]. However, due to its complex structure, entanglement is still puzzling to many people.

To understand multipartite entanglement, reliable techniques to characterize entanglement properties of general quantum states are required. Therefore, qualitatively testing whether a given state is entangled or not is of fundamental importance. The pure state case has been extensively studied. For instance, it has been proved that almost all multi-qubit entangled states admit Hardy-type proofs of non-locality without inequalities or probabilities [7]. In the setting of multiple dishonest parties, it has been shown how an agent of a quantum network can perform a distributed certification of a source creating multipartite Greenberger-Horne-Zeilinger states with minimal resources, which is, nevertheless, resistant against any number of dishonest parties [8]. However, a complete answer to entanglement detection for general mixed states is still missing. There has been a considerable number of different separability criteria discovered, including the famous positive partial transpose (PPT) criterion [10]. Gurvits discovered that this problem lies in the computational complexity class NP-Hard [9]. By borrowing ideas from functional analysis, entanglement witnesses and other techniques have been introduced to detect entanglement [11], [12], [28]. A more challenging problem is the detection of genuine multipartite entanglement; as yet extensive study has not yielded satisfactory results [28].

The entanglement detection problem naturally falls into the framework of quantum property testing where the goal is to test whether a given state satisfies the given property. There are two very different scenarios, corresponding to statistical fluctuations or accurate measurements that should be considered. In the first scenario, the measurement outcome is simply a bit string distributed according to the outcome probability; see [13] for an excellent survey. In the second scenario, the measurement is accurate in the sense that the measurement outcome is exactly the probability corresponding to the measurement. In this paper, we are focusing on the second scenario where the general quantum property testing problem can be formulated as:

Quantum property testing

Let \( \mathcal{Q} \) be the set of quantum states. A subset \( \mathcal{P} \subset \mathcal{Q} \) is called a property. A quantum property tester for \( \mathcal{P} \) is an algorithm (quantum procedure) that receives a black box as input \( x \in \mathcal{Q} \). If \( x \in \mathcal{P} \) then the algorithm accepts; otherwise, it rejects.

Reconstructing the mathematical description of the given quantum state is called “quantum state tomography”. With unbounded computational power, it is possible to obtain any required information about this quantum state via quantum

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2020.300456

0018-9448 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
state tomography. However, $n$-qubit state is parameterized by $4^n - 1$ real numbers, therefore, informational complete measurements consist of exponential observables, generally making the tomography infeasible. We regard the given quantum state as a resource, and the goal of property testing is to test the property by accessing the state as infrequently as possible. Therefore, we can define the sample complexity of the property $\mathcal{P}$ to be the infimum on the number accessing the state among all quantum property testers for $\mathcal{P}$. Note that the quantity we care about most is how many times we need to access the quantum state to accomplish the property testing, not the post-processing time of the algorithm. An optimal algorithm may rely heavily on collective measurements of many identical copies of given states. This is not ideal for current experimental technology, as collective measurements are usually much more difficult to be implemented than single-copy measurements. We are focusing on single-copy measurements.

Since these problems are decision problems with the 1-bit outcome, one might hope to achieve the answers with a very small number of measurements, or at least with something much less than an informationally complete set-up. The bipartite version of this problem has been studied recently, when it was shown that testing whether a bipartite state is entangled or not requires an informationally-complete measurement [14]–[16]. In [16], various sufficient criteria are given, under which the informationally-incomplete measurements can not reveal with certainty the property for an unknown quantum state. Comparing with bipartite entanglement, the structure of multipartite entanglement turns out to be much richer and more delicate.

In this paper, we study two versions of the multipartite entanglement detection: Given a multipartite quantum state, how do we universally detect entanglement through physical observables? In the first version, $\mathcal{Q}$ is the set of multipartite mixed states, and $\mathcal{P} \subseteq \mathcal{Q}$ is a property that is invariant under stochastic local operations assisted by classical communication (SLOCC). We show that there is no such procedure to test whether a given $\rho$ is in $\mathcal{P}$ or not by nonadaptive single-copy measurements without full state tomography if $\mathcal{P}$ contains at least one positive element but not all of them. In the second version, for quantum system $\mathcal{H} = \bigotimes_{k=1}^{n} \mathcal{H}_k$ with $d_k$ being the dimension of $\mathcal{H}_k$ and $d_1 \geq d_2 \geq \cdots \geq d_n$, we use $\mathcal{Q}$ to denote the set of pure states, and $\mathcal{P} \subseteq \mathcal{Q}$ to denote the set of product pure states. To detect $\mathcal{P}$, we provide an algorithm only costs $\sum_{k=2}^{n} (2d_k - 1)$ “local” measurements, where “local” means we only need to implement individual measurements on subsystems. On the other hand, the lower bound of detecting $\mathcal{P}$ is $\sum_{k=2}^{n} (2d_k - 2)$.

**Related Results:** As we mentioned, the bipartite entanglement certification has been studied in [14], [15]. In [14], it is proved that the detection of bipartite entanglement and the property of positive partial transpose both require full quantum state tomography. In [15], we proved the same results and extended it to the property of $k-$symmetric extendibility. The proof ideas of these two papers are quite similar, studying the boundary of the set of states with the wanted property. Luckily, the boundary has a non-trivial state family whose characterization is known. Such characterization can be easily used in the analysis. For the multipartite case, the situation is much more complicated, which is the main difficulty in generalizing the results of the bipartite system. In order to overcome this obstacle, we study the more generalized class of properties: SLOCC invariant properties. We generalize the working objects from quantum states into the set of semidefinite operators. In doing so, a number of new results in the bipartite version are obtained.

**Structure of the Paper:** In Section II, we provide technical preliminaries of the basic quantum mechanics. In Section III, we recall the basic features of entanglement together with examples for illustration. In Section IV, we show that if we do not have any prior information about the given quantum state, then detecting its entanglement property requires full state tomography. Actually, almost all SLOCC equivalence property here requires full state tomography. In Section V, we show that for the pure state entanglement detection, there exists an adaptive scheme to detect entanglement which is exponentially faster than doing full state tomography. Finally, we offer conclusions and some open problems in Section VII.

**II. Preliminaries**

For the convenience of the reader, the following is a brief outline of some basic notions from linear algebra and quantum theory, which are needed in this paper. For more details, we refer to [19].

**A. Basic Linear Algebra**

According to von Neumann’s formalism of quantum mechanics [18], an isolated physical system is associated with a Hilbert space which is called the state space of the system. In this paper, we only consider finite-dimensional Hilbert spaces $\mathcal{H}$. Let $\mathcal{L}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$. For any $A \in \mathcal{L}(\mathcal{H})$, $A$ is Hermitian if $A^\dagger = A$ where $A^\dagger$ is the adjoint operator of $A$ such that $\langle \psi | A^\dagger | \phi \rangle = \langle \phi | A | \psi \rangle^\ast$ for any $|\psi\rangle, |\phi\rangle \in \mathcal{H}$.

The trace of $A \in \mathcal{L}(\mathcal{H})$ is defined as $\text{tr}(A) = \sum_i \langle i | A | i \rangle$ for some given orthonormal basis $\{ |i\rangle \}$ of $\mathcal{H}$. It is worth noting that the trace function is independent of the orthonormal basis selected. It is also easy to check that trace function is linear and $\text{tr}(AB) = \text{tr}(BA)$ for any operators $A, B \in \mathcal{L}(\mathcal{H})$. $A$ is called semi-definite positive if it is Hermitian and has no negative eigenvalues. $A$ is called positive if it is Hermitian and has positive eigenvalues only. We use $A \succeq 0$ and $A > 0$ to denote the semi-definite positivity and positivity of $A$, respectively. $||A||$ stands for the 2-norm of $A \in \mathcal{L}(\mathcal{H})$ by definition $||A|| = \sqrt{\text{tr}(A^\dagger A)}$.

**B. Basic Quantum Mechanics**

A pure state of a quantum system is a normalized vector in its state space, and a mixed state is represented by a density operator. The set of density operators on $\mathcal{H}$ is defined as:

$$\mathcal{D} = \{ \rho \in \mathcal{L}(\mathcal{H}) : \rho \text{ is semi-definite positive and } \text{tr}(\rho) = 1 \}.$$

Trace-preserving super-operator is used to describe a broad class of transformations that a quantum mechanical system
can undergo: if the states of the system at times \( t_1 \leq t_2 \) are \( \rho_1 \) and \( \rho_2 \), respectively, then \( \rho_2 = \sum_k E_k \rho_1 E_k^\dagger \) for some set \( \{E_k\}_k \) such that \( \sum_k E_k^\dagger E_k = I \).

A (general) quantum measurement is described by a semi-definite operator \( E \). If the system is in state \( \rho \), then the measurement outcome is \( \text{tr}(E \rho) \) in the accurate measurement setting.

A Hermitian \( O = \sum_j \lambda_j |\psi_j\rangle \langle \psi_j| \) (that is \( O = O^\dagger \)) on \( \mathcal{H} \) with orthonormal basis \( \{|\psi_j\rangle\} \) and \( \lambda_j \in \mathbb{R} \) always corresponds to the following measurement protocol. Suppose the state of a quantum system is \( \rho \), when measured in basis \( |\psi_j\rangle \langle \psi_j| \). If the outcome is \( j \), the observed result is \( \lambda_j \). Directly, the output corresponds to a random variable \( X \) such that \( p(X = \lambda_j) = \text{tr}(\rho |\psi_j\rangle \langle \psi_j|) \).

Thus, \( EX = \text{tr}(\rho O) \).

Therefore, a Hermitian operator \( O \) is called an observable, where its expectation is given by \( \text{tr}(O \rho) \) when the state is \( \rho \).

C. Tensor Product of Hilbert Space

The state-space of a composed quantum system is the tensor product of the state spaces of its component systems. Let \( \mathcal{H}_k \) be a Hilbert space with orthonormal basis \( \{|\varphi_{ik}\rangle\} \) for \( 1 \leq k \leq n \). Then the tensor product \( \bigotimes^n_{k=1} \mathcal{H}_k \) is defined to be the Hilbert space with \( \{|\varphi_i\rangle = |\varphi_{i1}\rangle \ldots |\varphi_{in}\rangle\} \) as its orthonormal basis.

In the bipartite case, the partial trace of \( A \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2) \) with respect to \( \mathcal{H}_1 \) is defined as \( \text{tr}_{\mathcal{H}_1}(A) = \sum_i \langle i | A | i \rangle \) where \( \{|i\rangle\} \) is an orthonormal basis of \( \mathcal{H}_1 \). Similarly, we can define the partial trace of \( A \) with respect to \( \mathcal{H}_2 \). Partial trace functions are also independent of the orthonormal basis selected.

For a mixed state \( \rho \) on \( \mathcal{H}_1 \otimes \mathcal{H}_2 \), partial traces of \( \rho \) have explicit physical meanings: the density operators \( \text{tr}_{\mathcal{H}_1} \rho \) and \( \text{tr}_{\mathcal{H}_2} \rho \) are exactly the reduced quantum states of \( \rho \) on the second and the first component system, respectively.

III. Entanglement

In this section, we introduce some basic facts about the most important quantum feature—entanglement. In a bipartite system, a pure state \( |\psi\rangle \) is called product (or not entangled) if it is of the form:

\[ |\psi\rangle = |\psi_1\rangle |\psi_2\rangle. \]

In general, the state of a composite system cannot be decomposed into a tensor product of the reduced states on its component systems. A well-known example is the 2-qubit state:

\[ |\Psi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle). \]

A density matrix \( \rho \) is called separable (or not entangled) if it can be written as a convex combination of the density of product pure states, that is \( p_i > 0 \) and semi-definite positive \( \rho_{i,1} \)s and \( \rho_{i,2} \)s such that:

\[ \rho = \sum_i p_i \rho_{i,1} \otimes \rho_{i,2}. \]

Otherwise, it is called entangled.

A \( n \)-particle pure state \( |\psi\rangle \) is called product if it is of form:

\[ |\psi\rangle = |\psi_1\rangle \cdots |\psi_n\rangle. \]

A multipartite density matrix \( \rho \) is called separable if it can be written as a convex combination of the density of multipartite product pure states. Otherwise, it is called entangled.

A. Positive Partial Transpose

A bipartite quantum state \( \rho \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2) \) is called positive partial transpose (or simply PPT) if \( \rho^{T_1} \geq 0 \), where \( \Gamma_1 \) means the partial transpose with respect to the party \( \mathcal{H}_1 \), i.e.,

\[ (|ij\rangle \langle kl|)^{T_1} = |kj\rangle \langle il|. \]

It had been observed by Peres that any separable state has positive partial transpose \([10]\):

\[ \rho = \sum_i p_i \rho_{i,1} \otimes \rho_{i,2} \Rightarrow \rho^{T_2} = \sum_i p_i \rho_{i,1} \otimes (\rho_{i,2})^T \geq 0. \]

The result is independent of the party that was transposed, because \( \rho^{T_1} = (\rho^{T_2})^T \).

In [20], it was proved that any \( 2 \otimes n \) density operator that remains invariant after partial transposition with respect to the first system is separable.

B. Example

In this subsection, we present one example to illustrate the significant difference between multipartite entanglement and bipartite entanglement. For instance, a multipartite pure state is a product state if and only if it is a product under any bipartition. However, this is not true for the separability of mixed state. To demonstrate this, we recall the unextendible product bases (UPB) investigated in [21], where the three-qubit state is defined as

\[ \rho = \frac{1}{4} (I - \sum_{i=1}^4 |\phi_i\rangle \langle \phi_i|), \]

where \( |\phi_i\rangle \) are defined as:

\[ |\phi_1\rangle = |0, 1, +\rangle, \]
\[ |\phi_2\rangle = |1, +, 0\rangle, \]
\[ |\phi_3\rangle = |+, 0, 1\rangle, \]
\[ |\phi_4\rangle = |-, -, -\rangle, \]

with \( |\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \).

One can verify that:

i). \( \rho \) is invariant under partial transpose of any qubit. Therefore, according to the result of [20], \( \rho \) is separable in any bipartition.

ii). There is no product state \( |\psi_1\rangle |\psi_2\rangle |\psi_3\rangle \) which is orthogonal to all \( |\phi_i\rangle \). That is, no product state lives in the orthogonal complement of the space spanned by \( |\phi_1\rangle \). Note that \( \rho \) is proportional to the projection on the orthogonal complement of the space spanned by \( |\phi_1\rangle \). Therefore, \( \rho \) is entangled as it can never be written as a convex combination of the density matrix of product states.

We have constructed a tripartite entangled state which has no bipartite entanglement. In other words, multipartite entanglement enjoys a richer structure than the intersection of bipartite entanglements.
C. Genuine Entanglement

A multipartite pure state $|\psi\rangle$ is called genuinely entangled if it is not a product state of any bipartition. The genuine entanglement for mixed states can be defined in two inequivalent ways:

- A density matrix $\rho$ is called Type A genuinely entangled if, for any fixed bipartition, it cannot be written as a convex combination of the density of pure states which is a product in this bipartition.
- A density matrix $\rho$ is called Type B genuinely entangled if it cannot be written as a convex combination of the density of pure states where each pure state is a product state in some bipartition.

The second definition is stronger than the first one as bipartitions for different pure states can be different.

D. Entanglement Depth

In [27], entanglement depth is introduced to characterize the minimal number of particles in a system that are mutually entangled.

In $n$-particle system $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \mathcal{H}_n$, $|\psi\rangle$ is called $k$-product (separable) if it can be written as

$$|\psi\rangle = |\psi^{(1)}\rangle \otimes |\psi^{(2)}\rangle \cdots \otimes |\psi^{(k)}\rangle,$$

where decomposition corresponds to a partition of the $n$ particles, $|\psi^{(i)}\rangle$ is a genuine entangled state in $\otimes_{j \in S_i} \mathcal{H}_j$ with $\bigcup S_i = \{1, 2, \cdots, n\}$ and $S_i \cap S_l = \emptyset$ for $i \neq l$. The entanglement depth of $|\psi\rangle$, $d(\psi)$, is defined as the largest cardinality of $S_i$.

The density matrix $\rho$ is called $k$-separable if it can be written as a convex combination of $k$-separable pure states.

The entanglement depth of $\rho$ is defined as follows:

$$d(\rho) = \min_{\rho = \sum \rho_i |\psi_i\rangle \langle \psi_i|} \max_i d(\psi^i).$$

IV. Mixed State Property Testing

In this section, we study the possibility of certifying multipartite correlation without full state tomography by measuring only single-copy observables non-adaptively. We assume that the state is a mixed state and the only known information about this state is the Hilbert space it lives in. Our goal is to test the properties of mixed states. In particular, we are interested in multipartite correlations that are invariant under stochastic local operations assisted by classical communication (SLOCC).

Let $\mathcal{H} = \bigotimes_{k=1}^n \mathcal{H}_k$ with $d_k$ being the dimension of $\mathcal{H}_k$. The set of density operators is defined as

$$\mathcal{D} = \{ \rho \in \mathcal{L}(\mathcal{H}) : \rho \text{ is semi-definite positive and } \text{tr}(\rho) = 1 \}.$$

The concept of SLOCC has been used to study entanglement classification [22], [23] and entanglement transformation [24]–[26]. In this paper, we call two $n$-partite quantum states $\rho$ and $\sigma$ SLOCC equivalent if:

$$\rho = (A_1 \otimes A_2 \otimes \cdots \otimes A_n) \sigma (A_1 \otimes A_2 \otimes \cdots \otimes A_n)^\dagger$$

holds for some nonsingular $A_i \in \mathcal{L}(\mathcal{H}_i)$.

A property $\mathcal{P} \subseteq \mathcal{D}$ is called SLOCC invariant if $\rho \in \mathcal{P}$ implies $\rho' \in \mathcal{P}$ for any $\rho'$ being SLOCC equivalent to $\rho$.

Our main result is given as follows.

Theorem 1: For any SLOCC invariant property $\mathcal{P} \subseteq \mathcal{D}$, such that both $\mathcal{P}$ and $\mathcal{D} \setminus \mathcal{P}$ contain some positive elements respectively, it is impossible to determine with certainty whether $\rho \in \mathcal{P}$ or not, without full state tomography of given unknown $\rho$. In other words, $t := \Pi_{i=1}^n d_i^2 - 1$ measurements are necessary to detect whether $\rho \in \mathcal{P}$ or not.

This result can be interpreted as follows, for any set of observables (Hermitian matrices) $\{O_1, O_2, \cdots, O_s\}$ of $\mathcal{H}$ with $s < t$, there always exist two states, $\rho, \sigma \in \mathcal{P}$ and $\sigma \notin \mathcal{P}$, which are not distinguishable according to the measurement results, that is, $\text{tr}(O_i \rho) = \text{tr}(O_i \sigma)$ for all $1 \leq i \leq s$.

To illustrate the structure of entanglement implied by this result, we can reuse the figure of our paper [15]. Geometrically, any open and SLOCC invariant nontrivial $\mathcal{P}$ is not ‘cylinder-like’, where a property $\mathcal{P}$ is called trivial if $\mathcal{P} = \mathcal{D}$ or $\mathcal{P} = \emptyset$. In other words, the structural relation of $\mathcal{P}$ and $\mathcal{D}$ cannot be as (b).

Proof Outline: A general SLOCC operator transforms a quantum state into a semi-definite positive operator which is not unit trace. In order to prove this theorem, in Step 1, we modify the problem of certifying the SLOCC invariant property $\mathcal{P}$ of multipartite quantum states into certifying SLOCC invariant property $\tilde{\mathcal{P}}$ of multipartite semi-definite positive operators. We show that a measurement scheme can certify $\mathcal{P}$ if and only if it can certify $\tilde{\mathcal{P}}$ by adding a measurement $I_{\mathcal{H}}$. In Step 2, we call a Hermitian $H$ “free” if $\tilde{\rho} + r H \in \tilde{\mathcal{P}}$ for any $\tilde{\rho} \in \tilde{\mathcal{P}}$ and semi-definite positive $\tilde{\rho} + r H$. Further, we show that any SLOCC transformation of “free” Hermitian is still “free”. Step 3 shows that the set of “free” Hermitian matrices is either $\{0\}$ or forms a basis of the operator space $\mathcal{L}(\mathcal{H})$. Note that, to use the “free” basis $H_0, \cdots, H_t$, we need to make sure $\tilde{\rho}$ and $\tilde{\rho} + r H_i$ are both semi-definite positive. In Step 4, we give a topological argument to show that if $\mathcal{P}$ and its complement both contain some positive elements, a “free” basis for $\tilde{\mathcal{P}}$ induces contradiction.
A detailed proof is given below.

Proof: Quantum state in $\mathcal{H}$ is always unit trace. Therefore, the informationally-complete measurements are a set of linear independent Hermitian matrices $\{N_1, N_2, \ldots, N_t\}$.

To prove the validity of this theorem, we assume that there exists observables $\{O_1, O_2, \ldots, O_s\}$ of $\mathcal{H}$ with $s < t$ which can be used to detect property $\mathcal{P}$. In other words, for any unknown $\rho$, one can determine whether $\rho \in \mathcal{P}$ or not from $\text{tr}(O_1\rho), \ldots, \text{tr}(O_s\rho)$. Then, for any pairs of $\rho$ and $\sigma$, one can conclude that $\rho, \sigma \in \mathcal{P}$ or $\rho, \sigma \notin \mathcal{P}$ if $\text{tr}(O_i\rho) = \text{tr}(O_i\sigma)$ for all $i$.

We divide the proof into the following four steps.

Step 1: We transfer the problem into the existence of informationally-incomplete measurements in testing properties of general semi-definite positive operators by letting

$$\tilde{\mathcal{D}} = \{ M \in \mathcal{L}(\mathcal{H}) : M \text{ is semi-definite positive}\}.$$ 

For any property $\mathcal{P} \subseteq \mathcal{D}$, we generalize it into property $\tilde{\mathcal{P}}$ of $\tilde{\mathcal{D}}$ as follows,

$$\tilde{\mathcal{P}} = \{ M \in \mathcal{L}(\mathcal{H}) : M/\text{tr}(M) \in \mathcal{P}, M \geq 0 \}.$$ 

We observe that $\mathcal{P}$ is SLOCC invariant if and only if $\tilde{\mathcal{P}}$ is SLOCC invariant in the sense that for all nonsingular matrices $A_i$:

$$M \in \tilde{\mathcal{P}} \iff (A_1 \otimes A_2 \otimes \cdots A_n)M(A_1 \otimes A_2 \otimes \cdots A_n)^\dagger \in \tilde{\mathcal{P}}.$$ 

$\mathcal{P}$ contains some positive element if and only if $\tilde{\mathcal{P}}$ contains some positive element. $D \setminus \tilde{\mathcal{P}}$ contains some positive element.

More importantly, one can use the following set of observables $\{O_0, O_1, O_2, \ldots, O_s\}$ with $O_0 = I_\mathcal{H}$ to test $\mathcal{P}$ of $\mathcal{D}$. For any nonzero $\tilde{\rho} \in \tilde{\mathcal{D}}$, we know that $\tilde{\rho} \in \tilde{\mathcal{P}}$ if and only if $\rho \in \mathcal{P}$ with $\rho = \tilde{\rho}/\text{tr}(O_0\tilde{\rho})$. For $i > 0$, $\text{tr}(O_i\rho) = \text{tr}(O_i\tilde{\rho})/\text{tr}(O_0\tilde{\rho})$.

Thus, for unknown $\rho$ with $O_0, O_1, \ldots, O_s$ such that $O_i = \text{tr}(O_i\tilde{\rho})$, one can conclude that $\rho \in \mathcal{P}$ if and only if the quantum states (trace 1) corresponding to $O_0 = \rho/O_0, \ldots, O_s/O_0$ are in $\mathcal{P}$. On the other hand, $\{O_0, O_1, O_2, \ldots, O_s\}$ are not informationally-complete observables as $s + 1 < \Pi_{i=1}^n d_i^2$.

Therefore, the existence of informationally-incomplete measurements to detect $\mathcal{P}$ among $\tilde{\mathcal{D}}$ indicates informationally-incomplete measurements to detect $\tilde{\mathcal{P}}$ with certainty among $\tilde{\mathcal{D}}$.

Step 2: We assume the informationally-incomplete measurements, $\{O_0, O_1, O_2, \ldots, O_s\}$ can be used to detect the nontrivial SLOCC invariant property $\tilde{\mathcal{P}}$ of semi-definite positive operators with certainty. Then, there exists an Hermitian $H \neq 0$ such that $\text{tr}(O_iH) = 0$ for all $0 \leq i \leq s$. This $H$ enjoys the following property which we called “free”: For any $\tilde{\rho} \in \tilde{\mathcal{D}}$, if $\tilde{\rho} + rH \in \tilde{\mathcal{D}}$ for some $r \in \mathbb{R}$, then $\tilde{\rho} + rH \in \tilde{\mathcal{P}}$ if and only if $\tilde{\rho} \in \tilde{\mathcal{P}}$. We can observe that $H$ is free then $rH$ is free for any $r \in \mathbb{R}$.

Since $\tilde{\mathcal{P}}$ is a SLOCC invariant property, we can conclude that for any “free” Hermitian $H$ and any non-singular $A_i$,

$$(A_1 \otimes A_2 \otimes \cdots A_n)J(A_1 \otimes A_2 \otimes \cdots A_n)^\dagger \in \tilde{\mathcal{D}}, M \in \tilde{\mathcal{P}} \text{ if and only if}$$

$$(A_1^{-1} \otimes A_2^{-1} \otimes \cdots A_n^{-1})M(A_1^{-1} \otimes A_2^{-1} \otimes \cdots A_n^{-1})^\dagger \in \tilde{\mathcal{P}}.$$ 

That is,

$$(A_1^{-1} \otimes A_2^{-1} \otimes \cdots A_n^{-1})\tilde{\rho}(A_1^{-1} \otimes A_2^{-1} \otimes \cdots A_n^{-1})^\dagger + rJ \in \tilde{\mathcal{P}}.$$ 

Invoking the fact that $J$ is “free”, this is equivalent to

$$(A_1^{-1} \otimes A_2^{-1} \otimes \cdots A_n^{-1})\tilde{\rho}(A_1^{-1} \otimes A_2^{-1} \otimes \cdots A_n^{-1})^\dagger \in \tilde{\mathcal{P}}.$$ 

Since $\tilde{\mathcal{P}}$ is SLOCC invariant, this is true if and only if

$$\tilde{\rho} \in \tilde{\mathcal{P}}.$$ 

This above argument leads us to the fact that

$$(A_1 \otimes A_2 \otimes \cdots A_n)J(A_1 \otimes A_2 \otimes \cdots A_n)^\dagger$$

is also a “free” Hermitian.

Step 3: In this part, we show that if the set of “free” Hermitian matrices is not $\{0\}$, it contains a basis of the whole space $\mathcal{L}(\mathcal{H})$. In other words, there exist linear independent “free” Hermitian matrices $H_0, H_2, \ldots, H_t$.

We assume $J \neq 0$ is a “free” Hermitian and show that $S = \mathcal{L}(\mathcal{H})$ where $S$ is the matrix space spanning by all

$$(A_1 \otimes A_2 \otimes \cdots A_n)J(A_1 \otimes A_2 \otimes \cdots A_n)^\dagger$$

with $A_i$ being non-singular.

We prove a more general statement: The set of linear maps $\mathcal{L}(\mathcal{H}), \mathcal{L}(\mathcal{H})) : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H})$ is equal to the linear span of the following linear maps

$$(A_1 \otimes A_2 \otimes \cdots A_n) \cdot (A_1 \otimes A_2 \otimes \cdots A_n)^\dagger : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H}).$$ 

We start from studying the case $n = 1$. In this case, we are going to show that the following maps

$$M \cdot I : \rho \mapsto M\rho I = M\rho \text{ and } I \cdot M : \rho \mapsto I\rho M = \rho M \text{ lie in the span of}$$

$$A \cdot A^\dagger : \rho \mapsto A\rho A^\dagger$$

with $A$ being non-singular.

Choose real $y \neq 0$ such that $M + yI, M - yI, M - iyI$ being non-singular. It is easy to verify that $M \cdot I$ and $I \cdot M$ lie in the span of

$$(M + yI) \cdot (M + yI)^\dagger,$$

$$(M - yI) \cdot (M - yI)^\dagger,$$

$$(M - iyI) \cdot (M - iyI)^\dagger$$

from

$$M \cdot I = \frac{1 - i}{2y}(M + yI) \cdot (M + yI)^\dagger - \frac{1 + i}{2y}(M - yI) \cdot (M - yI)^\dagger$$

$$- \frac{i}{2y}(M - iyI) \cdot (M - iyI)^\dagger,$$

$$I \cdot M = \frac{1 + i}{2y}(M + yI) \cdot (M + yI)^\dagger - \frac{1 - i}{2y}(M - yI) \cdot (M - yI)^\dagger$$

$$+ \frac{i}{2y}(M - iyI) \cdot (M - iyI)^\dagger.$$
One crucial observation is that $AB$ is still non-singular for non-singular $A, B$. Thus if any maps $E,F : \mathcal{L}(H) \to \mathcal{L}(H)$ lie in the span of

$$\{ A \cdot A^\dagger : A \text{ is non-singular} \}$$

their composition $E \circ F$ also lies in that span.

Therefore, for any map $M,N$, we can first implement $M \cdot I$, then apply $I \cdot N$. Observe that any linear maps from $\mathcal{L}(H)$ to $\mathcal{L}(H)$ can be written as a linear combination of the form $M \cdot N$. Thus, for the case $n = 1$, the following linear maps $A \cdot A^\dagger$ spans the set of linear maps $\mathcal{L}(\mathcal{L}(H), \mathcal{L}(H)) : \mathcal{L}(H) \to \mathcal{L}(H)$.

For general $n$, any linear maps from $\mathcal{L}(H)$ to $\mathcal{L}(H)$ can be written as a linear combination of the form $M \cdot N$. Observe that $M \cdot N$ can be written into form

$$\sum_p (A_{1p} \otimes A_{2p} \otimes \cdots A_{np}) \cdot (B_{1p} \otimes B_{2p} \otimes \cdots B_{np})$$

with $A_{ip}, B_{ip}$ being non-singular matrix of $H_i$. We can first implement $A_{ip} \cdot B_{ip}$, then tensor them together. By linearity, we obtain that the set of the linear maps

$$(A_1 \otimes A_2 \otimes \cdots A_n) \cdot (A_1 \otimes A_2 \otimes \cdots A_n)^\dagger : \mathcal{L}(H) \to \mathcal{L}(H)$$

spans the set of linear maps $\mathcal{L}(\mathcal{L}(H), \mathcal{L}(H)) : \mathcal{L}(H) \to \mathcal{L}(H)$. This span is by complex combination. To obtain a real combination, we observe the following. For any non-zero Hermitians $Q$, there exits a $G \in \mathcal{L}(\mathcal{L}(H), \mathcal{L}(H))$ such that $Q = G(J)$. Therefore, $Q$ can be written as

$$Q = \sum_{s=0}^l c_s (A_{1s} \otimes A_{2s} \otimes \cdots A_{ns}){J(A_{1s} \otimes A_{2s} \otimes \cdots A_{ns})}.$$ 

for non-singular $A_{ks}$ and complex number $c_s$.

Because $Q$ and $J$ are Hermitian, we have

$$Q^\dagger = \sum_{s=0}^l \frac{c_s}{2} (A_{1s} \otimes A_{2s} \otimes \cdots A_{ns}){J(A_{1s} \otimes A_{2s} \otimes \cdots A_{ns})}.$$ 

Then, $Q$ can be written as

$$\sum_{s=0}^l \frac{c_s^2 + c_s}{2} (A_{1s} \otimes A_{2s} \otimes \cdots A_{ns}){J(A_{1s} \otimes A_{2s} \otimes \cdots A_{ns})}.$$ 

Therefore, for non-zero Hermitian $J$,

$$(A_1 \otimes A_2 \otimes \cdots A_n)J(A_1 \otimes A_2 \otimes \cdots A_n)^\dagger$$

forms a basis of $\mathcal{L}(H)$ linear combination using real coefficients.

Step 4: According to our argument of Step 3, we can assume $H_0, H_2, \cdots, H_t$ with $t = \Pi_{i=1}^{n} d_i^2 - 1$ be a set of linear independent “free” Hermitian matrices. Let the notation $\| \cdot \|$ denote the two norm of a matrix, and $\| \cdot \|$ denote the operator norm of a matrix. We shall show that for any $\bar{\rho} > 0$, there is an open ball

$$B(\bar{\rho}, \bar{\tau}) = \{ M : \| M - \bar{\rho} \| < \bar{\tau} \}$$

with $\bar{\tau} > 0$ such that if $\tilde{\rho} \in \bar{\Omega}$, then $B(\tilde{\rho}, \bar{\tau}) \subseteq \bar{\Omega}$; otherwise $B(\tilde{\rho}, \bar{\tau}) \subseteq \hat{D} \setminus \bar{\Omega}$.

According to the “free” property of $H_i$, we only need to choose a sufficient small $\bar{\tau}$ such that for any $M = \bar{\rho} + \bar{r}' \sum_{i=0}^t \mu_i H_i$ with $0 \leq \bar{r}' < \bar{\tau}$ and $\| \sum_{i=0}^t \mu_i H_i \| = 1$, we can have $\bar{\rho} + \bar{r}' \sum_{i=0}^t \mu_i H_i \in \hat{D}$. In other words, these $t + 1$ matrices are all semi-definite positive.

For any Hermitian $Y = \sum_{i=0}^t \mu_i H_i$ such that $\| Y \| = 1$, we have $\mu_i = \text{tr}(Y H_i)$, where $H_0, H_1, \cdots, H_t$ are the dual basis of $H_0, H_1, \cdots, H_t$ satisfying $\text{tr}(H_i H_j) = \delta_{ij}$ for $0 \leq i,j \leq t$. Therefore, $| \mu_i | \leq \| Y \| \cdot \| H_i \|$. Moreover, we have

$$\sum_{i=0}^k \mu_i H_i \leq \sum_{i=0}^k | \mu_i | \text{tr} \sqrt{H_i^2} \times \text{tr} I_H \leq \sum_{i=0}^t \| H_i \| \cdot \text{tr} \sqrt{H_i^2} \times I_H.$$

Let $a > 0$ being the minimal eigenvalue of $\bar{\rho} > 0$ and $\bar{q} = \sum_{i=0}^t \| H_i \| \cdot \text{tr} \sqrt{H_i^2}$. We can verify $\bar{\rho} > a > 0$ satisfying the wanted property: If $0 < \bar{\rho} \in \bar{\Omega}$, then for any $M = \bar{\rho} + \bar{r} Y$ with $Y = \sum_{i=0}^t \mu_i H_i$ and $\| Y \| = 1, \bar{r}' < \bar{\tau}$, we have $\bar{\rho} + \bar{r}' (\sum_{i=0}^t \mu_i H_i) > 0$ for all $0 \leq k \leq t$. As $H_0$ is “free”, and $\bar{r}' \mu_0 H_0 > 0$, we have $\bar{\rho} + \bar{r}' \mu_0 H_0 \in \bar{\Omega}$, $\therefore M = \bar{\rho} + \bar{r}' Y \in \bar{\Omega}$.

If $0 < \bar{\sigma} \in \hat{D} \setminus \bar{\Omega}$, then for any $M$ with $\| \bar{\sigma} - M \| < \bar{r}$ we can have $M \in \bar{\Omega}$ by the similar argument. Write $M = \bar{\sigma} + \bar{r}' Y$ with $Y = \sum_{i=0}^t \mu_i H_i$ and $\| Y \| = 1$, then $\bar{r}' < \bar{\tau}$. Therefore, $\bar{\sigma} + \bar{r}' (\sum_{i=0}^t \mu_i H_i) > 0$ for all $0 \leq k \leq t$. As $H_1$ is “free”, and $\bar{r}' \mu_0 H_0 > 0$, we have $\bar{\sigma} + \bar{r}' \mu_0 H_0 \in \bar{\Omega}$, $\therefore M = \bar{\sigma} + \bar{r}' Y \in \bar{\Omega}$.

Now suppose $0 < \tilde{\rho} \in \bar{\Omega}$ and $0 < \bar{\sigma} \in \hat{D} \setminus \bar{\Omega}$. Then for any $0 \leq l \leq 1$, $M_l = (1-l) \tilde{\rho} + l \bar{\sigma} > 0$. Let

$$l_0 := \sup \{ l : M_\in \bar{\Omega} \forall x \leq l \}.$$ 

According to the previous argument, there is a ball of center $\bar{\rho}$ lying in $\bar{\Omega}$, then $l_0 > 0$. Also there is a ball of center $\bar{\sigma}$ lying in $\hat{D} \setminus \bar{\Omega}$, then $l_0 < 1$. Now we consider the object $M_{l_0}$.

If $M_{l_0} \in \bar{\Omega}$, then there is a ball of radius $r > 0$ and center $M_{l_0}$ lying in $\bar{\Omega}$, that is, $M_{x} \in \bar{\Omega}$ for any $x \leq l + r$, contradict to the definition of $l_0$. Therefore, $M_{l_0} \in \hat{D} \setminus \bar{\Omega}$. Then there is a ball $B$ of center $M_{l_0}$ lying in $\hat{D} \setminus \bar{\Omega}$. Note that

$$\{ M_x : x \leq l_0 \} \cap B \neq \emptyset.$$ 

This is not possible because $\{ M_x : x \leq l_0 \} \subset \bar{\Omega}$ and $B \subset \hat{D} \setminus \bar{\Omega}$.

Therefore, there is no “free” Hermitian basis of $\mathcal{L}(H)$. According to Step 2, there is no non-zero “free” Hermitian matrix. That is, there are no informationally-incomplete measurements which can detect the membership of $\bar{\Omega}$ of $D$ with certainty.

Thus, there is no informationally-incomplete measurements which can detect the membership of $\bar{\Omega}$ of $D$ with certainty. □

Almost all interesting properties about multipartite correlations are SLOCC invariant. Theorem 1 indicates that full state tomography is necessary for detecting almost any multipartite correlation. In other words, exponential measurement resources are necessary.

The following are four examples where our results have been applied.

Example 1: $\mathcal{P}$ is the set of all PPT states, i.e., states with positive partial transpose among any bipartition.
One can verify that $\mathcal{P}$ is SLOCC invariant. Obviously, $0 < I/t \in \mathcal{P}$, and for sufficiently small $x > 0$, $xI/t + (1-x)|\Phi\rangle\langle\Phi| \in D \setminus \mathcal{P}$ with $|\Phi\rangle$ being an entangled pure states. Applying Theorem 1, we know that full state tomography is necessary to determine with certainty whether an unknown state is PPT among any bipartition or not.

**Example 2:** $\mathcal{P}$ is the set of all entangled states.

Again, we can use the above arguments. One can verify that $\mathcal{P}$ is SLOCC invariant. Also, $0 < I/t \in D \setminus \mathcal{P}$, and for sufficiently small $x > 0$, $xI/t + (1-x)|\Phi\rangle\langle\Phi| \in D \setminus \mathcal{P}$ with $|\Phi\rangle$ being an entangled pure state.

Applying Theorem 1, we know that full state tomography is necessary to determine with certainty whether an unknown multipartite state is entangled or not.

**Example 3:** $\mathcal{P}$ is the set of all states whose entanglement depth is $k$.

Clearly, $\mathcal{P}$ is SLOCC invariant.

If $k = 1$, $0 < I/t \in \mathcal{P}$, and for sufficiently small $x > 0$, $xI/t + (1-x)|\Phi\rangle\langle\Phi| \in D \setminus \mathcal{P}$ with $|\Phi\rangle$ being an entangled pure states. Applying Theorem 1, we know that full state tomography is necessary to determine with certainty whether the entanglement depth of an unknown state is $k$ or not.

If $1 < k \leq n$, $0 < I/t \in D \setminus \mathcal{P}$, and for sufficiently small $x > 0$, $xI/t + (1-x)|\Phi\rangle\langle\Phi| \in D \setminus \mathcal{P}$ with $|\Phi\rangle$ being an entangled pure states with depth $k$. Applying Theorem 1, we know that full state tomography is necessary to determine with certainty whether the entanglement depth of an unknown state is $k$ or not.

If $k > n$, $\mathcal{P} = \emptyset$, no measurement is needed.

**Example 4:** $\mathcal{P}$ is the set of all genuine entangled states (Type A or Type B defined in Section III.C).

One can verify that $\mathcal{P}$ is SLOCC invariant.

If $0 < I/t \in D \setminus \mathcal{P}$, and for sufficiently small $x > 0$, $xI/t + (1-x)|\Phi\rangle\langle\Phi| \in D \setminus \mathcal{P}$ with $|\Phi\rangle$ being an entangled pure state.

Applying Theorem 1, we know that full state tomography is necessary to determine with certainty whether an unknown state is genuinely entangled or not.

**V. Pure State Entanglement Testing**

In this section, we assume that the state is a pure state, and the only known information about this state is the Hilbert space it lives in. We provide a lower bound together with an adaptive procedure, with an almost matching upper bound, to detect whether the state is a product or is entangled.

Let $\mathcal{H} = \bigotimes_{k=1}^{n} \mathcal{H}_k$ with $d_k$ being the dimension of $\mathcal{H}_k$, and $d_1 \geq d_2 \geq \cdots \geq d_n$. The set (state space) of pure states on $\mathcal{H}$ is defined as:

$$\{ |\psi\rangle : \langle\psi|\psi\rangle = 1 \} \subseteq \mathcal{H}.$$  

Our problem can be formalized as follows: Given a pure quantum $|\psi\rangle$, how many “local” measurements are needed to verify whether the state is a product, i.e., within form $\otimes_{k=1}^{n} |\psi_k\rangle$, or not, where a measurement is called “local” if it is applied only on one system nontrivially, say $\mathcal{H}_1$, or $\mathcal{H}_2$, or $\cdots$, or $\mathcal{H}_n$.

One can observe the following: $|\psi\rangle$ is a product if and only if $\psi_k$ is a pure state for any $1 \leq k \leq n$, where $\psi_k$ denotes the reduced density operator of $|\psi\rangle$ in $\mathcal{H}_k$. In other words, $|\psi\rangle$ is a product if for any $k$, the resulting operator is pure (rank 1) after tracing out all other systems except $k$.

**Theorem 2:** Any local “procedures” that can detect whether a $n$-partite pure state of $\mathcal{H}$ is a product or not, must accomplish the pure state tomography of at least $n-1$ parties. Furthermore, at least $\sum_{k=2}^{n} 2(d_k-1)$ observables are necessary to detect the product property adaptively. On the other hand, $\sum_{k=2}^{n} (2d_k - 1)$ observables are sufficient to detect the product property adaptively.

**Remark:** For non-adaptive procedure, the lower bound becomes $\sum_{k=2}^{n} (4d_k - 5)$ because non-adaptive pure state tomography requires least $(4d_k - 5)$ measurements [17].

**Proof:** To show the lower bound, we introduce the purity testing problem as follows: Given unknown $\sigma_k \in \mathcal{D}_k$, our goal is to detect whether $\sigma_k$ is pure or not, where $\mathcal{D}_k$ denotes the mixed state space of $\mathcal{H}_k$.

$$\mathcal{D}_k = \{ \rho_k \in \mathcal{L}(\mathcal{H}_k) : \rho_k \geq 0, tr(\rho) = 1 \}.$$  

We first observe that purity testing must accomplish the task of pure state tomography. In other words, for different pure states $|\psi_k\rangle, |\phi_k\rangle \in \mathcal{H}_k$, the purity testing should be able to distinguish them. Otherwise, by linearity, it cannot distinguish $|\psi_k\rangle \langle\psi_k| + 1/2|\psi_k\rangle \langle\phi_k| + 1/2|\phi_k\rangle \langle\phi_k|$ if $|\psi_k\rangle \langle\phi_k|$ is a product state. Without pure state tomography, the procedure cannot determine whether to output 0 (pure) or 1 (not pure).

Suppose for parties $\mathcal{H}_1$ and $\mathcal{H}_2$, the procedure does not accomplish the pure state tomography. In other words, there exist $|\psi_1\rangle, |\phi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle, |\phi_2\rangle \in \mathcal{H}_2$ such that the procedure cannot distinguish them. Then there exists an entangled pure bipartite state $|\Omega_{12}\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ such that its reduced density matrices are $\Omega_1 = \lambda |\psi_1\rangle \langle\psi_1| + (1-\lambda)|\phi_1\rangle \langle\phi_1|$, and $\Omega_2 = \mu |\psi_2\rangle \langle\psi_2| + (1-\mu)|\phi_2\rangle \langle\phi_2|$ for some $0 < \lambda, \mu < 1$. The existence of $|\Omega_{12}\rangle$ is equivalent to finding $0 < \lambda, \mu < 1$ such that $|\lambda|\psi_1\rangle \langle\psi_1| + (1-\lambda)|\phi_1\rangle \langle\phi_1|$ and $|\mu|\psi_2\rangle \langle\psi_2| + (1-\mu)|\phi_2\rangle \langle\phi_2|$ share the same eigenvalues. We only need to choose $\lambda$ to be a very small positive number, then the corresponding $\mu$ does exist. Now, the procedure cannot distinguish the following entangled state

$$|\Omega_{12}\rangle \otimes |\psi_3\rangle \otimes \cdots \otimes |\psi_n\rangle$$

and the product state

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes \cdots \otimes |\psi_n\rangle,$$

contradicting to the assumption that the procedure can detect product property.

Therefore, the procedure must accomplish the pure state tomography for at least $n-1$ parties. On the other hand, $n-1$ parties are enough since we have the constraint that the whole state is pure.

Pure state tomography of $d$-dimensional system requires at least $2d-2$ observables because $d$-dimensional pure state has $2d-2$ free real parameters. Thus, at least $\sum_{k=2}^{n} (2d_k - 1)$ observables are necessary to detect product property. To show the upper bound, we suppose $\mathcal{H}_k$ with orthornormal basis $|0\rangle, \cdots, |d_k - 1\rangle$ and use the following algorithm.
Algorithm 1 Pure Entanglement Testing

1. Let the unknown pure state $|\psi\rangle \in \mathcal{H}$ with $\psi_k$ being its reduced density matrix in subsystem $\mathcal{H}_k$;
2. Outputs 0 for product $|\psi\rangle$; 1 for entangled $|\psi\rangle$;
3. $k \leftarrow 2$;
4. $b \leftarrow 0$;
5. while $b = 0$ and $k < n$ do
   6. \[ l \leftarrow l + 1; \]
   7. while $\text{tr}(|l\rangle\langle l|\psi_k) = 0$ do
      8. $\alpha_{l,k} \leftarrow \sqrt{\text{tr}(|l\rangle\langle l|\psi_k)}$;
      9. $s \leftarrow s + 1$
   10. for $j = l + 1 \rightarrow d_k - 1$ do
      11. Measure $\psi_k$ using $F_j = |j\rangle\langle j| + |l\rangle\langle l|$;
      12. $x \leftarrow \text{tr}[F_j|\psi_k|$;
      13. Measure $\psi_k$ using $G_j = i(|j\rangle\langle l| - |l\rangle\langle j|)$;
      14. $y \leftarrow \text{tr}[G_j|\psi_k|$;
      15. $\alpha_{j,k} \leftarrow (x + iy)/(2\alpha_{l,k})$;
      16. $s \leftarrow s + |\alpha_{j,k}|^2$
   17. if $s \neq 1$ then
      18. $b \leftarrow 1$
   19. else
      20. $k \leftarrow k + 1$
  22. Output $b$;

To show that Algorithm 1 outputs 0 for produce $|\psi\rangle$, we let

\[ |\psi_k\rangle = \sum_{m=0}^{d_k-1} \beta_{m,k}|m\rangle. \]

To find the smallest $l$ such that $\beta_{l} \neq 0$, we measure $|\psi_k\rangle$ sequentially until $\text{tr}(|\psi\rangle\langle \psi| |l\rangle\langle l|)$ is non-zero at Line 7. We conclude that the state is

\[ |\psi_k\rangle = \sum_{m=0}^{d_k-1} \beta_{m,k}|m\rangle. \]

We know that $\alpha_k,m = \beta_k,m = \sqrt{\text{tr}(|\psi\rangle\langle \psi| |l\rangle\langle l|)}$ is positive since the global phase of a quantum state is ignorable.

The goal of Line 12 to Line 16 is to obtain $\beta_{m,j}$ for all $m \geq l$ by employing the coherence between $|m\rangle$ and $|l\rangle$. We obtain the $(j+1)$-th row of $|\psi\rangle$ for $x = \langle \psi_k | F_j | \psi_k \rangle = \beta_{l,k} \beta_{j,k} + \beta_{l,k} \beta_{j,k}^*$,

\[ y = \langle \psi_k | G_j | \psi_k \rangle = \beta_{l,k} \beta_{j,k}^* - \beta_{l,k} \beta_{j,k}. \]

As we have assumed that $\beta_{l,k}$ is real, it is obvious that $\beta_{j,k}^* = \beta_{j,k}$ for all $j > l$. Therefore, we have

\[ \beta_{j,k} = \frac{x - iy}{2\alpha_{j,k}} = \alpha_{j,k}. \]

Since $|\psi_k\rangle$ is a normalized pure state, we have

\[ \sum_{j=l}^{d_k-1} |\alpha_{j,k}|^2 = \sum_{j=l}^{d_k-1} |\beta_{j,k}|^2 = \langle \psi_k | \psi_k \rangle = 1. \]

Therefore, if all $\psi_k$s are pure, then Line 18-19 of Algorithm 1 will never be called. That means, the output $b$ is 0.

Next, we show that Algorithm 1 outputs 1 for entangled $|\psi\rangle$. To derive a contradiction, we assume that Algorithm 1 outputs 0 for some entangled $|\psi\rangle$. Suppose $p > 1$ is the smallest number such that $\psi_p$ is not a pure state. According to the previous argument, the execution of Lines 5-21 in the Algorithm such that $1 < k < p$, would not change the value of $b$ because $\psi_k$ is a pure state here.

We show that if the value of $b$ is not changed after the execution of Lines 5-21 for $k = p$, then $\psi_k = (r_{ka,bb})_{d_k \times d_k}$ is pure. Since the value of $b$ is not changed, we know that $\sum_{j=l}^{d_k-1} |\alpha_{j,k}|^2 = 1$. We can define a pure state

\[ |\phi_k\rangle = \sum_{m=0}^{d_k-1} \alpha_{m,k}|m\rangle. \]

We show that $\psi_k = |\phi_k\rangle \langle \phi_k|$.

For $m < l$, we have

\[ r_{km,km} = \text{tr}(|\psi_k|\langle m|\langle m|) = \text{tr}(|\phi_k\rangle\langle \phi_k|\langle m|\langle m|) = 0. \]

Thus, $r_{kl,kl} = \text{tr}(|\psi_k|\langle l|\langle l|) = \text{tr}(|\phi_k\rangle\langle \phi_k|\langle l|\langle l|) = \alpha_{k,l}^2\alpha_{k,m}$. For $l \leq m \leq d_k - 1$, we have

\[ r_{km,kl} = \text{tr}(|\psi_k|\langle l|\langle m|) = \text{tr}(|\phi_k\rangle\langle \phi_k|\langle l|\langle m|) = \alpha_{k,l} \alpha_{k,m}. \]

As $\psi_k$ is semi-definite positive, we know that the first $l$ rows and columns of $\psi_k$ are all zero.

For any $l \leq m \leq d_k - 1$, we choose the sub-matrix of $\psi_k$ of $\{|l\rangle, |m\rangle\} \times \{|l\rangle, |m\rangle\}$,

\[ \begin{bmatrix} \alpha_{k,l}^2 & \alpha_{k,l} \alpha_{k,m} \\ \alpha_{k,l} \alpha_{k,m} & \alpha_{k,m} \end{bmatrix}. \]

This sub-matrix is also semi-definite positive. Thus,

\[ r_{km,km} \geq |\alpha_{k,m}|^2. \]

According to $\text{tr}(|\psi_k\rangle\langle \psi_k|) = 1$, we have

\[ 1 = \sum_{m} r_{km,km} \geq \sum_{m} |\alpha_{k,m}|^2 = 1. \]

Thus, $r_{km,km} = |\alpha_{k,m}|^2$.

Now for any $m, s > l$, we choose the sub-matrix of $\psi_k$ of $\{|s\rangle, |m\rangle\} \times \{|s\rangle, |m\rangle\}$,

\[ \begin{bmatrix} \alpha_{k,l}^2 & \alpha_{k,l} \alpha_{k,s} \\ \alpha_{k,l} \alpha_{k,s} & \alpha_{k,s} \end{bmatrix}. \]

According to its positivity of determinant, we have $r_{ks,ks} = \alpha_{k,s} \alpha_{k,m}$. That is $\psi_k = |\phi_k\rangle \langle \phi_k|$. This contradicts our assumption that $\psi_k$ is not pure. Therefore, if $|\psi\rangle$ is entangled, Algorithm 1 would output 1.

For each $k > 1$, the execution of testing $\psi_k$ uses at most $2d_k - 1$ observables: Lines 6-7 uses $l$ observables, Lines 11-17 uses $2d_k - l$ observables. In total, Algorithm 1 uses at most $\sum_{k=2}^{n} (2d_k - 1)$ observables. □
VI. CONCLUSION & ACKNOWLEDGMENT

In this paper, we study the relation between entanglement certification and tomography. We show that tomography is necessary to reveal the one-bit information of membership for almost all multipartite correlation, including genuine entanglement detection and entanglement depth certification if only nonadaptive single-copy measurements are allowed. However, universal entanglement detection among pure states can be much more efficient, even if we allow only local measurements. An almost optimal adaptive local measurement scheme for detecting pure state entanglement is provided.

There are many interesting open problems related to this topic. One particular challenge is to certify entanglement in the setting that the measurement output is a classical bit string distributed according to the output probability. A recent result [29] solved a very special case of entanglement testing—the tensor product testing. To make further progress in resolving the general problem of certifying entanglement, especially the lower bound part, we believe quantum Shannon theory is needed.

REFERENCES

[1] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in Proc. 35th Annu. Symp. Found. Comput. Sci., Nov. 1994, pp. 124–134.
[2] L. K. Grover, “Quantum mechanics helps in searching for a needle in a haystack,” Phys. Rev. Lett., vol. 79, no. 2, pp. 325–328, Jul. 1997.
[3] D. Markham and B. C. Sanders, “Graph states for quantum secret sharing,” Phys. Rev. A, Gen. Phys., vol. 78, no. 4, Oct. 2008, Art. no. 042309.
[4] R. Raussendorf and H. J. Briegel, “A one-way quantum computer,” Phys. Rev. Lett., vol. 86, no. 22, pp. 5188–5191, May 2001.
[5] S. Sachdev, Quantum Phase Transitions. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[6] M. Sarovar, A. Ishizaki, G. R. Fleming, and K. B. Whaley, “Quantum entanglement in photosynthetic light-harvesting complexes,” Nature Phys., vol. 6, no. 6, pp. 462–467, Apr. 2010.
[7] S. Abramsky, C. M. Constantin, and S. Ying, “Hardy is (almost) everywhere: Nonlocality without inequalities for almost all entangled multipartite states,” Inf. Comput., vol. 250, pp. 3–14, Oct. 2016.
[8] A. Pappa, A. Chaliloux, S. Wehner, E. Diamanti, and J. Kerenidis, “Multipartite entanglement verification resistant against dishonest parties,” Phys. Rev. Lett., vol. 108, no. 26, Jun. 2012, Art. no. 260502.
[9] L. Gurvits, “Classical complexity and quantum entanglement,” J. Comput. Syst. Sci., vol. 69, no. 3, pp. 448–484, Nov. 2004.
[10] A. Peres, “Separability criterion for density matrices,” Phys. Rev. Lett., vol. 77, no. 8, pp. 1413–1415, Aug. 1996.
[11] M. Horodecki, P. Horodecki, and R. Horodecki, “Separability of mixed states: Necessary and sufficient conditions,” Phys. Lett. A, vol. 223, nos. 1–2, pp. 1–8, Nov. 1996.
[12] B. M. Terhal, “Bell inequalities and the separability criterion,” Phys. Lett. A, vol. 271, nos. 5–6, pp. 319–326, Jul. 2000.
[13] A. Montanaro and R. de Wolf, “A survey of quantum property testing,” Theory Comput. Graduate Surv., vol. 7, pp. 1–81, Jul. 2016.
[14] C. Carmeli, T. Heinosaari, A. Karlsson, J. Schultz, and A. Toigo, “Verifying the quantumness of bipartite correlations,” Phys. Rev. Lett., vol. 116, no. 23, Jun. 2016, Art. no. 230403.
[15] D. Lu et al., “Tomography is necessary for universal entanglement detection with single-copy observables,” Phys. Rev. Lett., vol. 116, no. 23, Jun. 2016, Art. no. 230501.
[16] C. Carmeli, T. Heinosaari, J. Schultz, and A. Toigo, “Probing quantum state space: Does one have to learn everything to learn something?” Proc. Roy. Soc. A, Math. Phys. Eng. Sci., vol. 473, no. 2201, May 2017, Art. no. 20160866.
[17] T. Heinosaari, L. Mazzarella, and M. M. Wolf, “Quantum tomography under prior information,” Commun. Math. Phys., vol. 318, no. 2, pp. 355–374, Feb. 2013.
[18] J. von Neumann, Mathematical Foundations of Quantum Mechanics. Princeton, NJ, USA: Princeton Univ. Press, 1955.
[19] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[20] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, “Separability in 2 × N composite quantum systems,” Phys. Rev. A, Gen. Phys., vol. 61, no. 6, May 2000, Art. no. 062302.
[21] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, “Unextendible product bases and bound entanglement,” Phys. Rev. Lett., vol. 82, no. 26, pp. 5385–5388, Jun. 1999.
[22] W. Dürr, G. Vidal, and J. I. Cirac, “Three qubits can be entangled in two inequivalent ways,” Phys. Rev. A, Gen. Phys., vol. 62, no. 6, Nov. 2000, Art. no. 062314.
[23] G. Gour and N. R. Wallach, “Classification of multipartite entanglement of all finite dimensionality,” Phys. Rev. Lett., vol. 111, no. 6, Aug. 2013, Art. no. 060502.
[24] N. Yu, E. Chitambar, C. Guo, and R. Duan, “Tensor rank of the tripartite state (W ⊗n),” Phys. Rev. A, Gen. Phys., vol. 81, no. 1, Jan. 2010, Art. no. 014301.
[25] N. Yu, C. Guo, and R. Duan, “Obtaining a W state from a Greenberger-Horne-Zeilinger state via stochastic local operations and classical communication with a rate approaching unity,” Phys. Rev. Lett., vol. 112, no. 16, Apr. 2014, Art. no. 160401.
[26] Y. Qiao, X. Sun, and N. Yu, “Characterization of multipartite entanglement in terms of local transformations,” 2014, arXiv:1401.2627. [Online]. Available: http://arxiv.org/abs/1401.2627
[27] A. S. Sørensen and K. Mølmer, “Entanglement and extreme spin squeezing,” Phys. Rev. Lett., vol. 86, no. 20, pp. 4431–4434, May 2001.
[28] A. Dimić and B. Dakić, “Single-copy entanglement detection,” npj Quantum Inf., vol. 4, no. 1, pp. 1–8, Dec. 2018.
[29] N. Yu, “Quantum closeness testing: A streaming algorithm and applications,” 2019, arXiv:1904.03218. [Online]. Available: http://arxiv.org/abs/1904.03218