JOURNAL OF MATHEMATICAL PHYSICS **51**, 042202 (2010)

Approximating the set of separable states using the positive partial transpose test

Salman Beigi[1,a)] and Peter W. Shor[2]

[1]*Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125, USA*

[2]*Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Received 9 November 2009; accepted 22 February 2010; published online 27 April 2010)

The positive partial transpose test is one of the main criteria for detecting entanglement, and the set of states with positive partial transpose is considered as an approximation of the set of separable states. However, we do not know to what extent this criterion, as well as the approximation, is efficient. In this paper, we show that the positive partial transpose test gives no bound on the distance of a density matrix from separable states. More precisely, we prove that, as the dimension of the space tends to infinity, the maximum trace distance of a positive partial transpose state from separable states tends to 1. Using similar techniques, we show that the same result holds for other well-known separability criteria such as reduction criterion, majorization criterion, and symmetric extension criterion. We also bring in evidence that the sets of positive partial transpose states and separable states have totally different shapes. © *2010 American Institute of Physics.* [doi:10.1063/1.3364793]

I. INTRODUCTION

The problem of detecting entanglement has been focused in quantum information theory for many years. The problem is: given a bipartite mixed state ρ_{AB}, decide whether this state is entangled or separable. The first attack toward solving this problem is the following observation due to Peres[1] and the Horodeckis.[2] If $\rho_{AB}=\Sigma_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}$ is separable, then $(\rho_{AB})^{\mathrm{T}_B}=\Sigma_i p_i \rho_A^{(i)} \otimes (\rho_B^{(i)})^{\mathrm{T}}$, where M^{T} denotes the transpose of matrix M, is also a quantum state, and is a positive semidefinite matrix. Therefore, if ρ_{AB} is separable, its partial transpose, $(\rho_{AB})^{\mathrm{T}_B}$, should be positive semidefinite. The Horodeckis have proven that this criterion characterizes all separable states in dimensions 2×2 and 2×3.[2] However, there are entangled states in dimension 3×3 with a positive partial transpose (PPT).[3]

Although the set PPT states does not coincide with the set of separable states, it is usually considered as an approximation of this set. For example, in Ref. 4 instead of estimating the distance from separable states, the distance of an arbitrary state from PPT states has been computed as an "strongly related problem." Also in Ref. 5 the geometry of the set of PPT states has been studied to understand the properties of the set of separable states. However, we do not know how efficient these approximations are. For instance, given an upper bound on the distance of a state from PPT states, does it give an upper bound on the distance from separable states?

We can think of this problem from the point of view of complexity theory. Gurvits[6] has proven that given a bipartite density matrix ρ_{AB}, it is NP-hard to decide whether this state is separable or entangled. An approximate formulation of this problem is the following: given a bipartite density matrix ρ_{AB} and $\epsilon>0$, decide whether there exists a separable state in the ϵ-neighborhood (in trace distance) of ρ_{AB}. Gurvits has established a reduction from Knapsack to this problem and has

[a)] Electronic mail: salman@caltech.edu.

0022-2488/2010/51(4)/042202/10/$30.00

proven the NP-hardness of the separability problem, but only for exponentially small ϵ. However, as mentioned in Ref. 7 by replacing Knapsack with 2-out-of-4-SAT and repeating a similar argument, the NP-hardness can be proven for an inverse polynomial ϵ. Also, Gharibian[8] has shown the same result using a reduction from the Clique problem. Now the question is that how large ϵ can be while getting to the NP-hardness. For example, is there an efficient algorithm to decide whether the distance of a given state from separable states is less than 1/3 or it is an NP-hard problem? Equivalently, is there an efficiently implementable separability test such that if a state passes the test, then it is 1/3-close to the set of separable states?

In this paper we consider the converse of this question, i.e., given a separability criterion, if a state passes this test, can we claim a nontrivial upper bound on the distance of this state from separable states? We prove that the answer for the PPT criterion, as well as other well-known separability tests such as reduction criterion,[9] majorization criterion,[10] and symmetric extension criterion,[11,12] is no. More precisely, we prove the following theorem.

Theorem 1: *Let $\mathcal{H}$ be a bipartite Hilbert space. For every $\varepsilon > 0$, if the dimension of each subsystem of $\mathcal{H}$ is large enough, there exists a PPT state acting on $\mathcal{H}$ whose trace distance from separable states is at least* $1-\varepsilon$.

To the best knowledge of authors, this is the first result that compares separable states relative to PPT states in terms of their distance. However, the volume of these sets has been studied by several authors. For instance, by estimating the volume of separable states and PPT states in the Hilbert–Schmidt norm, it has been shown in Ref. 13 that a random PPT state is entangled. The same conclusion has been proven in Ref. 14 in terms of Bures volume. See also Refs. 15 and 16 for some other results in this setting.

A. Main ideas

Let $\mathcal{H}=\mathcal{H}^A \otimes \mathcal{H}^B$ be a bipartite Hilbert space. We want to find PPT states $\rho^{(n)} \in \mathcal{H}^{\otimes n}$ such that the trace distance of $\rho^{(n)}$ from separable states is close to 1, for enough large numbers n. Suppose ρ is an entangled PPT state. Then $\rho^{\otimes n}$ is entangled and also PPT. We claim that the sequence of states $\rho^{(n)}=\rho^{\otimes n}$ works for us. The intuition is that for two different quantum states ρ and σ, the trace distance of $\rho^{\otimes n}$ and $\sigma^{\otimes n}$ tends to 1 as n tends to infinity. However, in this problem σ is not a fixed state and ranges over all separable states. Also, it is not obvious (and may not hold) that the closest separable state to $\rho^{\otimes n}$ is of the form $\sigma^{\otimes n}$. [If we replace the trace distance with $E_R(\rho)$, the relative entropy of entanglement, this property does not hold.[17]]

Another idea is to use entanglement distillation. Suppose the state ρ is distillable. It means that, having arbitrary many copies of ρ, using local quantum operations and classical communications (LOCC maps), we can obtain as many EPR pairs as we want (say m pairs). LOCC maps send separable states to separable states, and the trace distance decreases under trace preserving quantum operations. Therefore, the distance of $\rho^{\otimes n}$ from separable states is bounded from below by the distance of $\mathrm{EPR}^{\otimes m}$ from separable states, which we know is close to 1 for large numbers m. Therefore, if ρ is distillable, the trace distance of $\rho^{\otimes n}$ from separable states tends to 1 as n tends to infinity.

It is well known that PPT states are not distillable under LOCC maps. So we cannot use this idea directly. On the other hand, in this argument, the only property of LOCC maps that we use is that they send separable states to separable states. Thus we may replace LOCC maps with *nonentangling maps*, the maps that send every separable state to a separable state. Due to the seminal work of Brandao and Plenio[18,19] every entangled state is distillable under *asymptotically* nonentangling maps. As a result, by replacing LOCC maps with asymptotically nonentangling maps and repeating the previous argument, we conclude that the trace distance of $\rho^{\otimes n}$ from separable states tends to 1.

Although this idea gives a full proof of Theorem 1, we do not present it in this paper. Instead, we use more fundamental techniques, namely, *quantum state tomography* and *quantum de Finetti theorem*.[20,21] In fact, these two techniques are the basic ideas of the results of Refs. 18 and 19 that we mentioned above. Since $\rho^{\otimes(n+k)}$ is a symmetric state, we may assume that the closest separable state to $\rho^{\otimes(n+k)}$ is also symmetric. Then by tracing out k registers and using the finite quantum de

Finetti theorem we conclude that the trace distance of $\rho^{\otimes(n+k)}$ from separable states is lower bounded by the trace distance of $\rho^{\otimes n}$ from separable states of the form

$$\sum_i p_i \sigma_i^{\otimes n}. \tag{1}$$

Since such a state is separable and ρ is entangled, the sum of p_i's for which σ_i is close to ρ cannot be large. On the other, if σ_i is far from ρ, using quantum state tomography one can distinguish $\rho^{\otimes n}$ from $\sigma_i^{\otimes n}$. Putting these two points together we show that the trace distance of $\rho^{\otimes n}$ and a separable state of the form of (1) is close to 1 for large enough n.

Note that in both of these arguments the only property of PPT states that we use is that if ρ and σ are PPT, then $\rho \otimes \sigma$ is also PPT. So we can conclude the same result for any separability test which satisfies this property.

II. PRELIMINARIES

A pure state $|\psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$ is called separable if it can be written of the form $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, where $|\psi_A\rangle \in \mathcal{H}^A$ and $|\psi_B\rangle \in \mathcal{H}^B$. A density matrix acting on $\mathcal{H}^A \otimes \mathcal{H}^B$ is called separable if it can be written as a convex combination of separable pure states $|\psi\rangle\langle\psi|$. We denote the set of separable states by SEP.

For two quantum states ρ and σ we denote their trace distance by

$$\|\rho - \sigma\|_{\mathrm{tr}} = \tfrac{1}{2}\mathrm{tr}|\rho - \sigma|, \tag{2}$$

where $|X| = \sqrt{X^\dagger X}$.

A. Separability tests

Assume that $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$ and fix an orthonormal basis $|1\rangle, \ldots, |d\rangle$ for both of Hilbert spaces. The partial transpose of matrices acting on $\mathcal{H}^A \otimes \mathcal{H}^B$ is a linear map defined by $(M_A \otimes N_B)^{\mathrm{T}_B} = M_A \otimes N_B^{\mathrm{T}}$, where the transpose is taken with respect to the fixed basis. Clearly, if ρ_{AB} is a separable state, $\rho_{AB}^{\mathrm{T}_B}$ is also a density matrix and then positive semidefinite. However, it does not hold for an arbitrary state. For example, the partial transpose of the maximally entangled state is not positive semidefinite; let $\Phi(d)$ to be the maximally entangled state on $\mathcal{H}$,

$$\Phi(d) = \frac{1}{d}\sum_{i,j=1}^{d} |i,i\rangle\langle j,j|. \tag{3}$$

$\Phi(d)$ is not positive semidefinite because

$$\Phi(d)^{\mathrm{T}_B} = \frac{1}{d}\sum_{i,j} |i\rangle\langle j| \otimes |j\rangle\langle i| = \frac{1}{d}I - \frac{1}{d}\sum_{i\neq j} |i\rangle\langle i| \otimes |j\rangle\langle j| + \frac{1}{d}\sum_{i\neq j} |i\rangle\langle j| \otimes |j\rangle\langle i| = \frac{1}{d}I - \frac{2}{d}\sum_{i<j} |\phi_{ij}\rangle\langle\phi_{ij}|,$$

where

$$|\phi_{ij}\rangle = \frac{1}{\sqrt{2}}(|i\rangle|j\rangle - |j\rangle|i\rangle). \tag{4}$$

As a result, PPT is a test to detect entanglement.[1,2] More formally, if we denote the set of density matrices with a positive semidefinite partial transpose by PPT, then SEP $\subseteq$ PPT.

Here is a list of some other separability criteria (see Refs. 22 and 23).

- Reduction criterion:[9] $I \otimes \rho_B \geq \rho_{AB}$, where $\rho_B = \mathrm{tr}_A(\rho_{AB})$. Here, by $M \geq N$ we mean $M - N$ is a positive semidefinite matrix.
- Entropic criterion:[24] $S_\alpha(\rho_{AB}) \geq S_\alpha(\rho_A)$ for $\alpha = 2$ and in the limit $\alpha \to 1$, where $S_\alpha(\rho) = [1/(1-\alpha)]\log \mathrm{tr}(\rho^\alpha)$.

- Majorization criterion:[10] $\lambda^{\downarrow}_{\rho_A} \succ \lambda^{\downarrow}_{\rho_{AB}}$, where $\lambda^{\downarrow}_{\rho}$ is the list of eigenvalues of ρ in nonincreasing order, and $y \succ x$ means that, for any k, the sum of the first k entries of list x is less than or equal to that of list y.
- Cross norm criterion:[25,26] $\mathrm{tr}|\mathcal{U}(\rho_{AB})| \leq 1$, where $\mathcal{U}$ is a linear map defined by $\mathcal{U}(M \otimes N) = v(M)v(N)^{\mathrm{T}}$ and $v(X) = (\mathrm{col}_1(X)^{\mathrm{T}}, \ldots, \mathrm{col}_d(X)^{\mathrm{T}})^{\mathrm{T}}$, where $\mathrm{col}_i(X)$ is the ith column of X.

All of these tests for separability are necessary conditions but not sufficient. Doherty *et al.*[11,12] have introduced a hierarchy of separability criteria which are both necessary and sufficient. Let $\rho_{AB} = \Sigma_i p_i \sigma_i \otimes \tau_i$ be a separable state. Then

$$\rho_{AB_1B_2\cdots B_k} = \sum_i p_i \sigma_i \otimes \tau_i^{\otimes k}$$

is an extension of ρ_{AB}, meaning that $\rho_{AB} = \mathrm{tr}_{B_2\cdots B_k}(\rho_{AB_1\cdots B_k})$. Also it is symmetric, meaning that it does not change under any permutation of subsystems B_i. More precisely, for any permutation π of k objects, if we define the linear map P_π by $P_\pi|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle = |\psi_{\pi(1)}\rangle \otimes \cdots \otimes |\psi_{\pi(k)}\rangle$, we have

$$P_\pi^{B_1\ldots B_k} \rho_{AB_1B_2\cdots B_k} (P_\pi^{B_1\ldots B_k})^\dagger = \rho_{AB_1B_2\cdots B_k}. \tag{5}$$

If such an extension exists, we say that ρ_{AB} has a symmetric extension to k copies. Doherty *et al.* have proven that a quantum state is separable if and only if it has a symmetric extension to k copies for any number k.[11,12] Also, they have shown that the problem of checking whether a given state has a symmetric extension to k copies, for a fixed k, can be expressed as a semidefinite programming and can be solved efficiently (however, the size of this semidefinite program grows exponentially in terms of k). So we get to another separability test.

Symmetric extension criterion:[11,12] if ρ_{AB} is separable, then it has a symmetric extension to k copies.

B. Quantum state tomography

An informationally complete POVM on $\mathcal{H}$ is a set of positive semidefinite operators $\{M_n\}$ forming a basis for the space of hermitian matrices on $\mathcal{H}$, and such that $\Sigma_n M_n = I$. In Ref. 21 there is an explicit construction of an informationally complete POVM in any dimension. Such a POVM is useful for quantum state tomography.

Suppose $\{M_n^*\}$ is the dual of basis $\{M_n\}$, i.e., $\mathrm{tr}(M_n M_m^*) = \delta_{mn}$, where δ_{mn} is the Kronecker delta function. For any Hermitian operator X we have

$$X = \sum_n \mathrm{tr}(XM_n)M_n^*.$$

Therefore, having some copies of the state ρ, by measuring ρ using the POVM $\{M_n\}$, we can approximate $\mathrm{tr}(\rho M_n)$ and then find the matrix representation of ρ.

Assume that $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ is a bipartite Hilbert space. If $\{M_n^A\}$ and $\{M_m^B\}$ are informationally complete POVMs on $\mathcal{H}^A$ and $\mathcal{H}^B$, respectively, then $\{M_n^A \otimes M_m^B\}$ is an informationally complete POVM on $\mathcal{H}$. This means that, if the state ρ_{AB} is shared between two far apart parties, they can perform quantum state tomography using classical communication. As a result, if the state ρ_{AB} is separable, then all intermediate states during the process are separable as well.

C. Quantum de Finetti theorem

As in Eq. (5), a quantum state $\rho^{(n)}$ acting on $\mathcal{H}^{\otimes n}$ is called symmetric if $P_\pi \rho^{(n)} P_\pi^\dagger = \rho^{(n)}$ for any permutation π of n objects. A symmetric state is called *k-exchangeable* if it has a symmetric extension to $n+k$ registers, i.e., a symmetric state $\rho^{(n+k)}$, such that $\mathrm{tr}_{1,\ldots,k}\, \rho^{(n+k)} = \rho^{(n)}$. Clearly, any state of the form $\rho^{\otimes n}$ is k-exchangeable for any k. Also any convex combination of these states is k-exchangeable. *Quantum de Finetti theorem* says that the converse of this observation holds: if a state is k-exchangeable for every k, it is in the convex hall of symmetric product states.

Quantum de Finetti theorem gives a characterization of infinitely exchangeable states. The following theorem, known as the finite quantum de Finetti theorem, says that if a state is k-exchangeable [but not necessarily $(k+1)$-exchangeable], then an approximation of the above result holds.

Theorem 2: (Reference 20) *Assume that* $\rho^{(n+k)}$ *is a symmetric state acting on* $\mathcal{H}^{\otimes n+k}$. *Let* $\rho^{(n)}=\mathrm{tr}_{1\ldots k}\,\rho^{(n+k)}$ *be the state obtained by tracing out the first k registers. Then there exists a probability measure* μ *on the set of density matrices on* $\mathcal{H}$, *such that*

$$\|\rho^{(n)}-\int\mu(d\sigma)\sigma^{\otimes n}\|_{\mathrm{tr}}\leq 2\dim\mathcal{H}\frac{n}{n+k}.$$

III. PROOF OF THEOREM 1

As we mentioned our proof is based on the work of Brandao and Plenio about reversibility of entanglement transformation under asymptotically nonentangling maps. In particular, we follow similar steps as in the proof of Corollary II.2 of Ref. 27.

Let $\mathcal{H}=\mathcal{H}^A\otimes\mathcal{H}^B$ and assume that $d=\dim\mathcal{H}>6$. Then there exists a PPT state $\rho_{AB}=\rho$ acting on $\mathcal{H}$ which is not separable (see Ref. 3). Let

$$\epsilon=\min_{\sigma\in\mathrm{SEP}}\|\rho-\sigma\|_{\mathrm{tr}}. \tag{6}$$

Since ρ is entangled, $\epsilon>0$.

For every number n, $\rho^{\otimes n}$ can be considered as a bipartite state acting on $(\mathcal{H}^A)^{\otimes n}\otimes(\mathcal{H}^B)^{\otimes n}$, and it is a PPT state. Therefore, if we prove that the trace distance of $\rho^{\otimes n}$ from separable states tends to 1, as n goes to infinity, we are done.

Let $\sigma^{(n)}$ be the closest separable state to $\rho^{\otimes n}$. Since $\rho^{\otimes n}$ is a symmetric state, for any permutation π we have

$$\|\rho^{\otimes n}-P_\pi\sigma^{(n)}P_\pi^\dagger\|_{\mathrm{tr}}=\|\rho^{\otimes n}-\sigma^{(n)}\|_{\mathrm{tr}},$$

and by triangle inequality

$$\left\|\rho^{\otimes n}-\frac{1}{n!}\sum_\pi P_\pi\sigma^{(n)}P_\pi^\dagger\right\|_{\mathrm{tr}}\leq\frac{1}{n!}\sum_\pi\|\rho^{\otimes n}-P_\pi\sigma^{(n)}P_\pi^\dagger\|_{\mathrm{tr}}=\|\rho^{\otimes n}-\sigma^{(n)}\|_{\mathrm{tr}}.$$

Therefore, we may assume that $\sigma^{(n)}$ is symmetric.

Let $\sigma^{(n+n^2)}$ be the closest (symmetric) separable state to $\rho^{\otimes(n+n^2)}$, and let $\mathrm{tr}_{1\ldots n^2}\,\sigma^{(n+n^2)}$ be the state obtained by tracing out n^2 registers. We have

$$\|\rho^{\otimes(n+n^2)}-\sigma^{(n+n^2)}\|_{\mathrm{tr}}\geq\|\rho^{\otimes n}-\mathrm{tr}_{1\ldots n^2}\,\sigma^{(n+n^2)}\|_{\mathrm{tr}}. \tag{7}$$

Using the finite quantum de Finetti theorem (Theorem 2), there exists a measure μ, such that

$$\mathrm{tr}_{1\ldots n^2}\,\sigma^{(n+n^2)}=\int\mu(d\tau)\tau^{\otimes n}+X_n, \tag{8}$$

where $\|X_n\|_{\mathrm{tr}}\leq 2d[n/(n+n^2)]$. Thus using (7), if we prove that

$$\|\rho^{\otimes n}-\left(\int\mu(d\tau)\tau^{\otimes n}+X_n\right)\|_{\mathrm{tr}} \tag{9}$$

tends to 1, as n goes to infinity, we are done.

Consider an informationally complete POVM on $\mathcal{H}^A$ and $\mathcal{H}^B$, and by taking their pairwise tensor product extend them to an informationally complete POVM on $\mathcal{H}$. Then apply quantum state tomography on $(n-1)$ copies of ρ in order to obtain an approximation of this state. To be more precise, let $\{M_i\}$ be the resulting informationally complete POVM on $\mathcal{H}$. So for a sequence of outcomes $(M_{l_1},\ldots,M_{l_{(n-1)}})$ we get to the approximation

$$\sum_i \frac{r_i}{n-1} M_i^*, \tag{10}$$

where r_i is the number of repetitions of M_i in $(M_{l_1},\ldots,M_{l_{(n-1)}})$.

We say that $(M_{l_1},\ldots,M_{l_{(n-1)}})$ is a *good* sequence if its corresponding estimation belongs to $B_{\epsilon/3}(\rho)$, the ball of radios $\epsilon/3$ in trace distance around ρ. Let G_{n-1} be the sum of $M_{l_1}\otimes\cdots\otimes M_{l_{(n-1)}}$ over good sequences $(M_{l_1},\ldots,M_{l_{(n-1)}})$. Therefore, by the law of large numbers,[28] $\mathrm{tr}(G_{n-1}\rho^{\otimes(n-1)})\to 1$ as n goes to infinity. Also for any τ far from ρ, $\mathrm{tr}(G_{n-1}\tau^{\otimes(n-1)})$ tends to zero.

Note that $G_{n-1}\leq I$. Thus

$$\|\rho^{\otimes n}-\left(\int\mu(d\tau)\tau^{\otimes n}+X_n\right)\|_{\mathrm{tr}}\geq \mathrm{tr}(I\otimes G_{n-1}\cdot\rho^{\otimes n})-\mathrm{tr}\left[(I\otimes G_{n-1})\cdot\left(\int\mu(d\tau)\tau^{\otimes n}+X_n\right)\right].$$

Since $\mathrm{tr}(I\otimes G_{n-1}\cdot\rho^{\otimes n})\to 1$, if we prove

$$\mathrm{tr}\left[(I\otimes G_{n-1})\cdot\left(\int\mu(d\tau)\tau^{\otimes n}+X_n\right)\right]\to 0,$$

we conclude that (9) tends to 1.

Now suppose that we perform quantum state tomography on $\int\mu(d\tau)\tau^{\otimes n}+X_n$. By (8), this state is not entangled. Moreover, since we can apply tomography locally (see Sec. II B), by starting from a separable state, the outcome of the process is always separable as well. Assuming that we get a good sequence in the process the outcome is equal to

$$\int\mu(d\tau)\mathrm{tr}[G_{n-1}\tau^{\otimes(n-1)}]\tau+\widetilde{X}_n, \tag{11}$$

where $\|\widetilde{X}_n\|_{\mathrm{tr}}\leq\|X_n\|_{\mathrm{tr}}\leq 2d[n/(n+n^2)]$. As a result, this state is separable. [Here we assume that (11) is nonzero because otherwise there is nothing to prove.]

Let

$$Y_n=\int_{\tau\notin B_{\epsilon/2}(\rho)}\mu(d\tau)\mathrm{tr}[G_{n-1}\tau^{\otimes(n-1)}]\tau+\widetilde{X}_n$$

and

$$c_n=\int_{\tau\in B_{\epsilon/2}(\rho)}\mu(d\tau)\mathrm{tr}[G_{n-1}\tau^{\otimes(n-1)}].$$

By the law of large numbers, there exists δ_n, such that for any $\tau\notin B_{\epsilon/2}(\rho)$ we have

$$\mathrm{tr}[G_{n-1}\tau^{\otimes(n-1)}]\leq\delta_n,$$

and $\delta_n\to 0$ as n goes to infinity. Therefore, $\|Y_n\|_{\mathrm{tr}}\leq\delta_n+2d[n/(n+n^2)]$.

As we mentioned, the state

$$\widetilde{\tau}=\frac{1}{c_n+\mathrm{tr}(Y_n)}\left[\int_{\tau\in B_{\epsilon/2}(\rho)}\mu(d\tau)\mathrm{tr}[G_{n-1}\tau^{\otimes(n-1)}]\tau+Y_n\right]$$

is separable. On the other hand, by definition

$$\tilde{\rho} = \frac{1}{c_n}\int_{\tau \in B_{\epsilon/2}(\rho)} \mu(d\tau)\mathrm{tr}[G_{n-1}\tau^{\otimes(n-1)}]\tau$$

is in the $\epsilon/2$-neighborhood of ρ. Then by (6) we have

$$\begin{aligned}\epsilon &\le \|\rho - \tilde{\tau}\|_{\mathrm{tr}}\\ &\le \frac{c_n}{c_n + \mathrm{tr}(Y_n)}\|\rho - \tilde{\rho}\|_{\mathrm{tr}} + \frac{|\mathrm{tr}(Y_n)|}{c_n + \mathrm{tr}(Y_n)}\|\rho\|_{\mathrm{tr}} + \frac{1}{c_n + \mathrm{tr}(Y_n)}\|Y_n\|_{\mathrm{tr}}\\ &\le \frac{c_n}{c_n + \mathrm{tr}(Y_n)} \cdot \frac{\epsilon}{2} + \frac{2}{c_n + \mathrm{tr}(Y_n)}\|Y_n\|_{\mathrm{tr}}.\end{aligned}$$

Thus

$$\epsilon c_n + \epsilon\, \mathrm{tr}(Y_n) \le \frac{\epsilon}{2}c_n + 2\|Y_n\|_{\mathrm{tr}},$$

and then

$$c_n \le \frac{2(2+\epsilon)}{\epsilon}\|Y_n\|_{\mathrm{tr}} \le 6\epsilon^{-1}\left(\delta_n + 2d\frac{n}{n+n^2}\right).$$

Putting everything together we find that

$$\begin{aligned}\mathrm{tr}\left[(I \otimes G_{n-1}) \cdot \left(\int \mu(d\tau)\tau^{\otimes n} + X_n\right)\right] &= \mathrm{tr}\left[\int_{\tau \in B_{\epsilon/2}(\rho)} \mu(d\tau)\mathrm{tr}[G_{n-1}\tau^{\otimes(n-1)}]\tau + Y_n\right]\\ &\le c_n + \|Y_n\|_{\mathrm{tr}}\\ &\le (6\epsilon^{-1}+1) \cdot \left(\delta_n + 2d\frac{n}{n+n^2}\right),\end{aligned}$$

which gives

$$\mathrm{tr}\left[(I \otimes G_{n-1}) \cdot \left(\int \mu(d\tau)\tau^{\otimes n} + X_n\right)\right] \to 0,$$

as n goes to infinity. We are done.

IV. GEOMETRY OF THE SET OF SEPARABLE STATES

Theorem 1 tells us that estimating the distance of a bipartite state from separable state by the distance from PPT states is not a good approximation. However, one may expect that the set of PPT states is an approximation of the set of separable states from a geometrical point of view. For instance, two spheres centered at origin with radii of 1 and 2 are far from each other, while they have the same geometric properties up to a scaler factor. In the following theorem we bring in evidence that this is not the case for the set of separable states relative to PPT states.

By Theorem 1 the maximum distance of a PPT state from the boundary of the set of separable states is close to 1. We can think of this problem in another direction. What is the maximum distance of a state on the boundary of separable states from the boundary of PPT states? To get an intuition on this problem, we can think of the unit sphere centered at origin in $\mathbb{R}^n$, and the cube with vertices $(\pm 1, \ldots, \pm 1)$. It is easy to see that the distance of any point on the sphere from points of the cube is less than 2. However, the distance of $(1,\ldots,1)$ from sphere is $\sqrt{n}-1$. It is because sphere and cube have totally different shapes.

Theorem 3: *Assume that $\mathcal{H}=\mathcal{H}^A\otimes\mathcal{H}^B$ and $\dim\mathcal{H}^A=\dim\mathcal{H}^B=d$. Then for any separable state ρ acting on $\mathcal{H}$ there exists a state σ on the boundary of the set of PPT states such that $\|\rho-\sigma\|_{\mathrm{tr}}\leq 1/\sqrt{d}$.*

Proof: Let σ be an arbitrary PPT state, and $\Phi(d)$ be the maximally entangled state defined in (3). Then the fidelity of σ and $\Phi(d)$ is

$$F(\sigma,\Phi(d))=[\mathrm{tr}\ \sigma\Phi(d)]^{1/2}=[\mathrm{tr}\ \sigma^{\mathrm{T}_B}\Phi(d)^{\mathrm{T}_B}]^{1/2}=\left[\mathrm{tr}\ \sigma^{\mathrm{T}_B}\left(\frac{1}{d}I-\frac{2}{d}\sum_{i<j}|\phi_{ij}\rangle\langle\phi_{ij}|\right)\right]^{1/2},$$

where $|\phi_{ij}\rangle$ is defined in (4). Thus using the fact that σ^{T_B} is a density matrix and then $\sigma^{\mathrm{T}_B}\leq I$, we obtain

$$F(\sigma,\Phi(d))\leq\frac{1}{\sqrt{d}}.$$

Therefore, by the well-known inequality between fidelity and trace distance (see Ref. 29, p. 416) we have

$$\|\sigma-\Phi(d)\|_{\mathrm{tr}}\geq 1-F(\sigma,\Phi(d))\geq 1-\frac{1}{\sqrt{d}}. \quad (12)$$

Now let ρ be an arbitrary separable state. Define $\rho_t=(1-t)\rho+t\Phi(d)$. $\rho_0=\rho$ is separable and then PPT, and $\rho_1=\Phi(d)$. So there exists $0\leq c\leq 1$, such that ρ_c is on the boundary of PPT states. Then we have

$$\|\rho-\rho_c\|_{\mathrm{tr}}=\|\rho-\Phi(d)\|_{\mathrm{tr}}-\|\rho_c-\Phi(d)\|_{\mathrm{tr}}\leq 1-\left(1-\frac{1}{\sqrt{d}}\right)=\frac{1}{\sqrt{d}},$$

where in the last inequality we use (12). ■

This theorem together with Theorem 1 say that considering the sets of separable states and PPT states in the trace-norm space, they have completely different shapes. However, due to Dvoretzky's theorem (see, for example, Ref. 30) we know that for every convex set, its intersections with *most* hyperplanes of certain dimension are close to Euclidean ball in shape. This means that the set of separable states and PPT states have the same geometry if we consider them in Euclidean space and restrict them to sections of certain dimension.

V. GENERALIZATION TO OTHER SEPARABILITY CRITERIA

According to Theorem 1, if the dimension of the space is large enough, there exists a PPT state far from separable states. Our candidate for such a state is $\rho^{\otimes n}$, where ρ is an entangled PPT state, and in the proof the only property of the set of PPT states that we use is that this set is closed under tensor product. Therefore, the same argument as in the proof of Theorem 1 gives us the following general theorem.

Theorem 4: *Assume that C is a necessary but not sufficient separability criterion, such that if ρ and σ satisfy C, then $\rho\otimes\sigma$ satisfies C as well. Then for any $\varepsilon>0$ there exists a state ρ that satisfies C, and whose trace distance from separable states is at least $1-\varepsilon$.*

Proof: Let ρ be an entangled state which satisfies C. Then $\rho^{\otimes n}$ satisfies C as well, and by the proof of Theorem 1, the trace distance of $\rho^{\otimes n}$ from separable states tends to 1 as n goes to infinity. ■

In the following theorem we prove that all separability criteria mentioned in Sec. II satisfy the assumption of Theorem 4.

Theorem 5: *For all separability criteria mentioned in Sec. II there exists an entangled state which passes the test while it is arbitrarily far, in trace distance, from separable states.*

Proof: By Theorem 4 it is sufficient to prove that those separability criteria are closed under tensor product.

- Reduction criterion: Let X, Y, Z, and W be positive semidefinite matrices, such that $X \geq Y$ and $Z \geq W$. Then $(X-Y)\otimes(Z+W)$ and $(X+Y)\otimes(Z-W)$ are positive semidefinite. Therefore, $X \otimes Z - Y \otimes W = \frac{1}{2}[(X-Y)\otimes(Z+W)+(X+Y)\otimes(Z-W)]$ is positive semidefinite. It means that if $X \geq Y$ and $Z \geq W$, then $X \otimes Z \geq Y \otimes U$. Now assume that ρ_{AB} and $\sigma_{A'B'}$ pass the reduction criterion. Therefore, $\rho_A \otimes I \geq \rho_{AB}$ and $\sigma_{A'} \otimes I \geq \sigma_{A'B'}$, and then $\rho_A \otimes \sigma_{A'} \otimes I \geq \rho_{AB} \otimes \sigma_{A'B'}$, which means that $\rho_{AB} \otimes \sigma_{A'B'}$ satisfies the reduction criterion.
- Entropic criterion: It follows easily from $S_\alpha(\rho\otimes\sigma)=S_\alpha(\rho)+S_\alpha(\sigma)$.
- Majorization criterion: $x \prec y$ if and only if there exists a doubly stochastic matrix D (a matrix all of whose entries is positive, and the sum of entries on any row and column is equal to 1), such that $x=Dy$ (see Ref. 29, p. 575). Therefore, if $x \prec y$ and $x' \prec y'$, there exist D and D' such that $x=Dy$ and $x'=D'y'$. Hence $x \otimes x' = (D \otimes D')(y \otimes y')$ and then $x \otimes x' \prec y \otimes y'$. The proof follows easily using this property.
- Cross norm criterion: Using $v(X \otimes X') = v(X) \otimes v(X')$ we have $\mathcal{U}((X\otimes X')\otimes(Y\otimes Y'))=\mathcal{U}(X\otimes Y)\otimes\mathcal{U}(X'\otimes Y')$. The proof follows from this equation.
- Symmetric extension criterion: If $\rho^{(k)}$ and $\sigma^{(k)}$ are symmetric extensions of ρ and σ to k copies, respectively, then $\rho^{(k)} \otimes \sigma^{(k)}$ is a symmetric extension of $\rho\otimes\sigma$ to k copies. ■

VI. CONCLUSION

We have proven that for any separability criterion that is closed under tensor product, the set of states that pass the test is not a good approximation of the set of separable states. For the special case of PPT test, we have shown that the sets of PPT states and separable states have totally different shapes. A problem that arises naturally is to find a separability criterion which is not weaker than the known ones, and also is not closed under tensor product. Finding such a separability test may clarify the complexity of the separability problem: is it NP-hard to decide whether there exists a separable state whose trace distance from a given state is less than a given constant c?

ACKNOWLEDGMENTS

Authors are grateful to Karol Życzkowski and Stanisław J. Szarek for providing some background about the comparison of the volume of the sets of separable states and PPT states. S.B. is also thankful to Barbara Terhal for useful discussions.

[1] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[2] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[3] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[4] F. Verstraete, J. Dehaene, and B. De Moor, J. Mod. Opt. **49**, 1277 (2002).
[5] S. J. Szarek, I. Bengtsson, and K. Życzkowski, J. Phys. A **39**, L119 (2006).
[6] L. Gurvits, J. Comput. Syst. Sci. **69**, 448 (2004).
[7] S. Beigi, Quantum Inf. Comput. **10**, 0141 (2010).
[8] S. Gharibian, Quantum Inf. Comput. **10**, 0343 (2010).
[9] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
[10] M. Nielsen and J. Kempe, Phys. Rev. Lett. **86**, 5184 (2001).
[11] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).
[12] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[13] G. Aubrun and S. J. Szarek, Phys. Rev. A **73**, 022109 (2006).
[14] D. Ye, J. Math. Phys. **50**, 083502 (2009).
[15] S. J. Szarek, Phys. Rev. A **72**, 032304 (2005).
[16] S. J. Szarek, E. Werner, and K. Życzkowski, J. Math. Phys. **49**, 032113 (2008).
[17] K. G. H. Vollbrecht and R. F. Werner, Phys. Rev. A **64**, 062307 (2001).
[18] F. G. S. L. Brandao, Ph.D. thesis, Imperial College London, 2008; e-print arXiv:0810.0026.
[19] F. G. S. L. Brandäo and M. B. Plenio, Nat. Phys. **4**, 873 (2008).
[20] M. Christandl, R. König, G. Mitchison, and R. Renner, Commun. Math. Phys. **273**, 473 (2007).
[21] R. König and R. Renner, J. Math. Phys. **46**, 122108 (2005).
[22] L. M. Ioannou, Quantum Inf. Comput. **7**, 335 (2007).
[23] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States* (Cambridge University Press, Cambridge, 2007).
[24] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **210**, 377 (1996).
[25] O. Rudolph, Quantum Inf. Process. **4**, 219 (2005).

[26] K. Chen and L.-A. Wu, Quantum Inf. Comput. **3**, 193 (2003).

[27] F. G. S. L. Brandao and M. B. Plenio, Commun. Math. Phys. **295**, 791 (2010); e-print arXiv:0904.0281.

[28] R. M. Dudley, *Real Analysis and Probability* (Cambridge University Press, Cambridge, 2002).

[29] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[30] G. Aubrun, S. Szarek, and E. Werner, J. Math. Phys. **51**, 022102 (2010).