

The automorphism group of separable states in quantum information theory

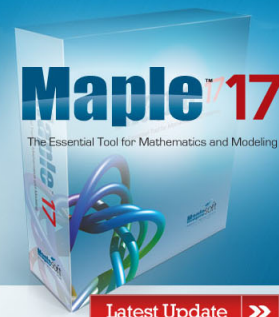
Shmuel Friedland, Chi-Kwong Li, Yiu-Tung Poon, and Nung-Sing Sze

Citation: *Journal of Mathematical Physics* **52**, 042203 (2011); doi: 10.1063/1.3578015

View online: <http://dx.doi.org/10.1063/1.3578015>

View Table of Contents: <http://scitation.aip.org/content/aip/journal/jmp/52/4?ver=pdfcov>

Published by the [AIP Publishing](#)

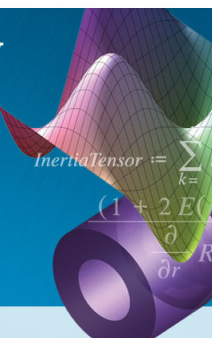


Maple 17
The Essential Tool for Mathematics and Modeling

Latest Update >>

The most comprehensive support for Physics in any mathematical software package

- State-of-the-art environment for algebraic computations in physics
- Access to Maple's full mathematical power, programming language, visualization routines, and documentation creation tools
- The only system with the ability to handle a wide range of physics computations as well as pencil-and-paper style input and textbook-quality display of results
- A programming library that gives access to almost 100 internal commands to write programs or extend the capabilities of the Physics package



InertiaTensor := $\sum_{k=1}^n$

(1 + 2 E(r) $\frac{\partial}{\partial r}$ R)

World-leading tools for performing calculations in theoretical physics

The automorphism group of separable states in quantum information theory

Shmuel Friedland,^{1,a)} Chi-Kwong Li,^{2,b)} Yiu-Tung Poon,^{3,c)} and Nung-Sing Sze^{4,d)}

¹Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, Chicago, Illinois 60607-7045, USA

²Department of Mathematics, College of William & Mary, Williamsburg, Virginia 23187-8795, USA

³Department of Mathematics, Iowa State University, Ames, Iowa 50011, USA

⁴Department of Applied Mathematics, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong

(Received 10 January 2011; accepted 23 March 2011; published online 28 April 2011)

We show that the linear group of automorphism of Hermitian matrices which preserves the set of separable states is generated by *natural* automorphisms: change of an orthonormal basis in each tensor factor, partial transpose in each tensor factor, and interchanging two tensor factors of the same dimension. We apply our results to the preservers of the product numerical range. © 2011 American Institute of Physics. [doi:10.1063/1.3578015]

I. INTRODUCTION

One of the main concepts in quantum information theory is *entanglement*. An entangled state involves at least two subsystems or more. We first discuss the two subsystems $H_m \otimes H_n$ case, also known as bipartite case. Here M_n is the space of $n \times n$ complex matrices and $H_n \subseteq M_n$ is the space of $n \times n$ complex Hermitian matrices. Denote by $D_n \subseteq H_n$ the convex set of positive semidefinite matrices of trace one, i.e., density matrices. Also let $\mathcal{S}_{m,n} \subseteq D_{mn} \subseteq H_{mn} \equiv H_m \otimes H_n$ be the set of bipartite separable states, i.e., $\mathcal{S}_{m,n} = \text{conv}\{A \otimes B : A \in D_m \text{ and } B \in D_n\}$. Clearly, $\mathcal{S}_{m,n}$ is a compact convex set. The set of entangled bipartite states is the complement of separable states in D_{mn} , i.e., $D_{mn} \setminus \mathcal{S}_{m,n}$.

Among the best known applications of entanglement are superdense coding, quantum teleportation, and more recently measurement based quantum computation (for review, see, e.g., Refs. 6 and 12). This recognition sparked an enormous stream of work in an effort to quantify entanglement in both bipartite and multipartite settings. Among the different measures of entanglement, the relative entropy of entanglement (REE) is of a particular importance. The REE is defined by (c.f. Ref. 14)

$$E_R(\rho) = \min_{\sigma' \in \mathcal{S}} S(\rho \| \sigma') = S(\rho \| \sigma),$$

where \mathcal{S} is the set of multipartite separable states. $E_R(\rho)$ is a convex function on \mathcal{S} and is strictly convex on strictly positive definite separable states.⁴ Hence, the computation of $E_R(\rho)$, which is given as the minimum of a convex function, should be in principle easy to compute, i.e., polynomial time algorithm.¹⁵ However, E_R is hard to compute in general, since the general characterization of separable states is *NP-hard*.⁵

A crucial observation of Peres¹¹ is that \mathcal{S} is invariant under the partial transpose. For example, on $H_{mn} \equiv H_m \otimes H_n$ the partial transpose linear map on the second component $\text{PT}_2 : H_{mn} \rightarrow H_{mn}$

^{a)}Electronic mail: friedlan@uic.edu.

^{b)}Electronic mail: ckli@math.wm.edu. C. K. Li is an honorary professor of the University of Hong Kong, the Taiyuan University of Technology, and the Shanghai University.

^{c)}Electronic mail: ytpoon@iastate.edu.

^{d)}Electronic mail: raymond.sze@inet.polyu.edu.hk.

is induced by $\text{PT}_2(A \otimes B) = A \otimes B^\top$, where B^\top is the transposed matrix of $B \in H_n$. Hence, if a density matrix $C \in D_{mn}$ represents a separable state then $\text{PT}_2(C)$ is positive semidefinite. (This condition implies that $\text{PT}_1(C) = \text{PT}_2(C)^\top$ is also positive semidefinite, since the transpose map $C \mapsto C^\top$, preserves the trace and the positivity.) It was shown in Ref. 7 that for $m + n \leq 5$, $C \in \mathcal{S}_{m,n}$ if and only if C and $\text{PT}_2(C)$ are density matrices. Unfortunately, the positivity of the partial transpose does not imply separability for $m + n \geq 6$ (c.f. Ref. 7).

Denote by $\mathcal{G}(n_1, \dots, n_k)$ the group of linear automorphisms of Hermitian matrices $H_N \equiv \bigotimes_{i=1}^k H_{n_i}$ which leaves invariant the set of separable states \mathcal{S} . The structure of $\mathcal{G}(m, n)$ was determined recently in Ref. 1. In this paper we extended the above results to $\mathcal{G}(n_1, \dots, n_k)$ for $k \geq 3$. We show that this group is generated by unitary change of basis in each component, partial transposes in each component, and by permutations of the factors of the same dimension. In summary, $\mathcal{G}(n_1, \dots, n_k)$ consists only of the natural elements.

There are related works^{8,9} which study the linear maps on $\bigotimes_{i=1}^k \mathbb{C}^{n_i}$ that preserve the product states, i.e., indecomposable tensors. In these papers, the authors show some structural results similar to our results on the group $\mathcal{G}(n_1, \dots, n_k)$.

We now briefly summarize the contents of the paper. In Sec. II, we give another proof for the structure theorem of $\mathcal{G}(m, n)$ obtained in Ref. 1, and the proof is further extended to determine the structure of $\mathcal{G}(n_1, \dots, n_k)$ in Sec. III. In Sec. IV, we apply our results to preservers of the product numerical range.

II. THE BIPARTITE CASE

In what follows we use the basic notion of the dimension of a convex set C as a subset of \mathbb{R}^N , denoted by $\dim C$. It is the minimum of the dimension of an affine space, i.e., a translation of a subspace of \mathbb{R}^N , which contains C . For a set $S \subseteq \mathbb{R}^n$, denote by $\text{conv } S$ the convex set spanned by S . For k -linear spaces U_1, \dots, U_k over a given field \mathbb{F} , we denote by $\bigotimes_{i=1}^k U_i$ the tensor vector space of dimension $\prod_{i=1}^k \dim U_i$. Suppose S_i is a proper subset of U_i for $i = 1, \dots, k$. Then

$$\bigotimes_{i=1}^k S_i = \left\{ \bigotimes_{i=1}^k \mathbf{u}_i : \mathbf{u}_i \in S_i, \quad i = 1, \dots, k \right\}.$$

Denote by $I_m \in H_m$ the identity matrix. Let H_m^+ and $H_m^{(1)}$ denote the set of positive semidefinite matrices and Hermitian matrices of trace one, respectively. So $H_m^{(1)}$ is a hyperplane in H_m with $\dim H_m^{(1)} = m^2 - 1$ and $D_m = H_m^+ \cap H_m^{(1)}$. Denote by $\mathcal{P}_m \subseteq D_m$ the compact set of all Hermitian rank one matrices of trace one, i.e., the set of pure states. Then $\mathcal{P}_m \otimes \mathcal{P}_n$ is the set of separable pure states in D_{mn} . Observe that $K(\mathcal{S}_{m,n}) = \text{conv}(H_m^+ \otimes H_n^+) \subseteq H_{mn}^+$ is the cone of positive semidefinite matrices generated by separable states. The following result is well known and we present the proof for completeness.

Lemma 1: The set of separable states $\mathcal{S}_{m,n}$ is a convex set, whose extreme points is $\mathcal{P}_m \otimes \mathcal{P}_n$. Furthermore, $\dim \mathcal{S}_{m,n} = (mn)^2 - 1$ and $\frac{1}{mn} I_{mn}$ is an interior point of $\mathcal{S}_{m,n}$.

Proof: Clearly, since the set of the extreme points of D_m is \mathcal{P}_m , it follows that $\mathcal{S}_{m,n} = \text{conv}(\mathcal{P}_m \otimes \mathcal{P}_n)$. As $\mathcal{P}_m \otimes \mathcal{P}_n \subseteq \mathcal{P}_{mn}$, it follows that $\mathcal{P}_m \otimes \mathcal{P}_n$ is the set of the extreme points of $\mathcal{S}_{m,n}$. Recall next that $\frac{1}{m} I_m$ is an interior point of D_m . Hence $\frac{1}{mn} I_{mn} = \left(\frac{1}{m} I_m\right) \otimes \left(\frac{1}{n} I_n\right)$ is an interior point of $\mathcal{S}_{m,n}$. Since $\mathcal{S}_{m,n} \subseteq H_{mn}^{(1)}$, it follows that $\dim \mathcal{S}_{m,n} = (mn)^2 - 1$. \square

Lemma 2: Let $\Phi : D_{mn} \rightarrow D_{mn}$ be an affine map such that $\Phi(\mathcal{S}_{m,n}) = \mathcal{S}_{m,n}$. Then Φ can be extended uniquely to an invertible linear map $\Psi : H_{mn} \rightarrow H_{mn}$.

Proof: First extend Φ to an affine homogeneous map (of degree one), $\Psi : K(\mathcal{S}_{m,n}) \rightarrow K(\mathcal{S}_{m,n})$ by letting $\Psi(tC) = t\Psi(C)$ for any $t \geq 0$ and $C \in \mathcal{S}_{m,n}$. Clearly Ψ is affine and homogeneous. Also $\Psi(K(\mathcal{S}_{m,n})) = K(\mathcal{S}_{m,n})$. Since $K(\mathcal{S}_{m,n}) - K(\mathcal{S}_{m,n}) = H_{mn}$, it follows that Ψ extends to a linear map of H_{mn} to itself. Since I_{mn} is an interior point of $K(\mathcal{S}_{m,n})$, it follows that $\dim K(\mathcal{S}_{m,n}) = (mn)^2$. Hence, $\dim \Psi(K(\mathcal{S}_{m,n})) = (mn)^2$. We claim that the linear map Ψ is invertible. Otherwise $\dim \Psi(H_{mn}) \leq (mn)^2 - 1$, which contradicts the fact that $\dim \Psi(K(\mathcal{S}_{m,n})) = (mn)^2$. \square

The proof of Lemma 2 implies that in order to characterize affine automorphisms of separable bipartite states it is enough to consider linear automorphisms of H_m which preserve $S_{m,n}$. The main result of this section is.

Theorem 3: Let $\Psi : H_{mn} \rightarrow H_{mn}$ be a linear map. The following are equivalent.

- (a) $\Psi(\mathcal{P}_m \otimes \mathcal{P}_n) = \mathcal{P}_m \otimes \mathcal{P}_n$.
- (b) $\Psi(S_{m,n}) = S_{m,n}$.
- (c) There are unitary $U \in M_m$ and $V \in M_n$ such that
 - (c.1) $\Psi(A \otimes B) = \psi_1(A) \otimes \psi_2(B)$ for $A \otimes B \in H_m \otimes H_n$, or
 - (c.2) $m = n$ and $\Psi(A \otimes B) = \psi_2(B) \otimes \psi_1(A)$ for $A \otimes B \in H_m \otimes H_n$, where ψ_1 has the form $A \mapsto UAU^*$ or $A \mapsto UA^T U^*$, and ψ_2 has the form $B \mapsto VBV^*$ or $B \mapsto VB^T V^*$.

To prove Theorem 3, we need the following lemma which can be viewed as the characterization of linear preservers of pure states.

Lemma 4: Suppose $\psi : H_m \rightarrow H_n$ is linear and satisfies $\psi(\mathcal{P}_m) \subseteq \mathcal{P}_n$. Then one of the following holds:

- (i) there is $R \in \mathcal{P}_n$ such that ψ has the form $A \mapsto (\text{Tr } A)R$.
- (ii) $m \leq n$ and there is a $U \in M_{m \times n}$ with $UU^* = I_m$ such that ψ has the form

$$A \mapsto U^*AU \quad \text{or} \quad A \mapsto U^*A^T U.$$

Proof: Define a map $\phi : H_{m+n} \rightarrow H_{m+n}$ given by

$$\phi(B) = \phi \left(\begin{bmatrix} B_1 & B_2 \\ B_2^* & B_3 \end{bmatrix} \right) = \begin{bmatrix} \psi(B_1) & 0 \\ 0 & 0_m \end{bmatrix} \quad \text{for all } B = \begin{bmatrix} B_1 & B_2 \\ B_2^* & B_3 \end{bmatrix} \in H_{m+n} \text{ with } B_1 \in H_m.$$

Then ϕ is linear. In particular, $\phi(A \oplus 0_n) = \psi(A) \oplus 0_m$ for all $A \in H_m$. Then $\psi(\mathcal{P}_m) \subseteq \mathcal{P}_n$ implies $\text{rank}(\phi(A)) \leq 1$ whenever $\text{rank}(A) = 1$. If $\dim \phi(H_{m+n}) = 1$, then there exist a rank one Q and a linear functional f on H_{m+n} such that $\phi(B) = f(B)Q$. Therefore, $Q = R \oplus 0_m$ for some $R \in \mathcal{P}_n$ and $\psi(A) = g(A)R$ for all $A \in H_m$, where $g(A) = f(A \oplus 0_n)$. Since $\psi(\mathcal{P}_m) \subseteq \mathcal{P}_n$, $g(P) = 1$ for all $P \in \mathcal{P}_m$. For $A \in H_m$, let $A = \sum_{i=1}^m \lambda_i P_i$ be the spectral decomposition of A . Then $g(A) = \sum_{i=1}^m \lambda_i f(P_i) = \sum_{i=1}^m \lambda_i = \text{Tr } A$.

If $\dim \psi(H_m) > 1$, by Corollary 2 in Ref. 2, there exist $\alpha \in \{1, -1\}$ and $S \in M_n$ such that ϕ has the form $B \mapsto \alpha S^*BS$ or $B \mapsto \alpha S^*B^T S$. Since $\phi(A \oplus 0_n) = \psi(A) \oplus 0_m$, ψ has the form

$$A \mapsto \alpha U^*AU \quad \text{or} \quad A \mapsto \alpha U^*A^T U,$$

where U is the leading $m \times n$ submatrix of S , i.e., $S = \begin{bmatrix} U & * \\ * & * \end{bmatrix}$. Since $\psi(\mathcal{P}_m) \subseteq \mathcal{P}_n$, if ψ has the form $\psi(A) = \alpha U^*AU$, then $x^*(\alpha U U^*)x = \text{Tr}(\alpha U^*(xx^*)U) = \text{Tr}(\psi(xx^*)) = 1$ for all unit vector $x \in \mathbb{C}^m$. This gives $\alpha U U^* = I_m$. Hence, $n \geq m$, $\alpha = 1$ and $U U^* = I_m$ and the result follows. Proof for the case when $\psi(A) = U^*A^T U$ is similar. \square

Proof of Theorem 3: The equivalence of conditions (a) and (b) follows from the fact that $\mathcal{P}_m \otimes \mathcal{P}_n$ is the set of the extreme points of $S_{m,n}$ and that Ψ is linear. The implication “(c) \Rightarrow (a)” is clear. Suppose (a) holds. We will set $\Psi(A \otimes B) = \phi_1(A, B) \otimes \phi_2(A, B)$, and show that $(\phi_1(A, B), \phi_2(A, B)) = (\psi_1(A), \psi_2(B))$ for all A and B , or $m = n$ and $(\phi_1(A, B), \phi_2(A, B)) = (\psi_2(B), \psi_1(A))$ for all A and B , where ψ_1 and ψ_2 have some standard form. Below are the technical arguments.

First, Lemma 2 yields that Ψ is bijective. Without loss of generality, we assume that $m \geq n > 1$. Consider the partial traces $\text{Tr}_1 : H_{mn} \rightarrow H_n$ and $\text{Tr}_2 : H_{mn} \rightarrow H_m$ on $H_{mn} \equiv H_m \otimes H_n$ defined by $\text{Tr}_1(A \otimes B) = (\text{Tr } A)B$ and $\text{Tr}_2(A \otimes B) = (\text{Tr } B)A$. Clearly Tr_1 and Tr_2 are linear maps. Define two maps $\phi_1 : (H_m, H_n) \rightarrow H_m$ and $\phi_2 : (H_m, H_n) \rightarrow H_n$ by

$$\phi_1(A, B) = \text{Tr}_2(\Psi(A \otimes B)) \quad \text{and} \quad \phi_2(A, B) = \text{Tr}_1(\Psi(A \otimes B)).$$

Notice that

$$\Psi(P \otimes Q) = \phi_1(P, Q) \otimes \phi_2(P, Q) \quad \text{for all } P \in \mathcal{P}_m \text{ and } Q \in \mathcal{P}_n. \tag{1}$$

Fixed a $Q \in \mathcal{P}_n$, then the maps $\phi_1(\cdot, Q) : H_m \rightarrow H_m$ and $\phi_2(\cdot, Q) : H_m \rightarrow H_n$ are both linear and $\phi_1(\mathcal{P}_m, Q) \subseteq \mathcal{P}_m$ while $\phi_2(\mathcal{P}_m, Q) \subseteq \mathcal{P}_n$. Therefore, by Lemma 4, both $\phi_1(\cdot, Q)$ and $\phi_2(\cdot, Q)$ have one of the following forms:

$$(i.a) \quad A \mapsto U^*AU, \quad (i.b) \quad A \mapsto U^*A^\top U, \quad \text{or} \quad (ii) \quad A \mapsto (\text{Tr } A)R, \tag{2}$$

where the unitary U and projection R depend on Q . Furthermore, the map $\phi_2(\cdot, Q)$ can only be of the form (ii) if $m > n$. For $1 \leq i, j \leq m$, let $E_{ij} \in M_m$ have 1 at the (i, j) entry and 0 elsewhere. Let $A = E_{11} - E_{22}$. Define $F : \mathcal{P}_n \rightarrow \mathbb{R}$ by $F(Q) = \|\phi_1(A, Q)\|$, where $\|\cdot\|$ is the Frobenius norm. Notice that

$$F(Q) = \|\phi_1(A, Q)\| = \begin{cases} \sqrt{2} & \text{if } \phi_1(\cdot, Q) \text{ has the form (i.a) or (i.b),} \\ 0 & \text{if } \phi_1(\cdot, Q) \text{ has the form (ii).} \end{cases}$$

Now for two distinct $Q_1, Q_2 \in \mathcal{P}_n$, write $Q_1 = \mathbf{x}\mathbf{x}^*$ and $Q_2 = \mathbf{y}\mathbf{y}^*$ with unit vectors $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$. Note that \mathbf{x} and \mathbf{y} are linearly independent. For any $t \in [0, 1]$, define

$$Q(t) = \frac{1}{\|\mathbf{x} + t(\mathbf{y} - \mathbf{x})\|^2} (\mathbf{x} + t(\mathbf{y} - \mathbf{x}))(\mathbf{x} + t(\mathbf{y} - \mathbf{x}))^* \in \mathcal{P}_n.$$

In particular, $Q(0) = Q_1$ and $Q(1) = Q_2$. For each $t \in [0, 1]$, as $\phi_1(\cdot, Q(t))$ has the form (i) [i.e., either (i.a) or (i.b)] or (ii), the continuous map $t \mapsto F(Q(t))$ is constant. Therefore, one can conclude that either $\phi_1(\cdot, Q)$ has the form (i) for all $Q \in \mathcal{P}_m$ or $\phi_1(\cdot, Q)$ has the form (ii) for all $Q \in \mathcal{P}_m$.

Now, we claim that one of the following holds.

- (I) For all $Q \in \mathcal{P}_n$, $\phi_1(\cdot, Q)$ has the form (i) and $\phi_2(\cdot, Q)$ has the form (ii).
- (II) For all $Q \in \mathcal{P}_n$, $\phi_1(\cdot, Q)$ has the form (ii) and $\phi_2(\cdot, Q)$ has the form (i).

Suppose first that for some $Q \in \mathcal{P}_n$, both $\phi_1(\cdot, Q)$ and $\phi_2(\cdot, Q)$ are of the form (i). Then we must have $m = n$. Then for $r = 1, 2$, there is unitary matrix U_r such that $\phi_r(\cdot, Q)$ has the form $A \mapsto U_r^*AU_r$ or $A \mapsto U_r^*A^\top U_r$. Since $m = n \geq 2$, the right-hand side of (1) is a quadratic function in $P \in \mathcal{P}_m$ while the left-hand side is linear in $P \in \mathcal{P}_m$, which is impossible. To be more precise, let

$$P_1 = E_{11}, \quad P_2 = E_{22}, \quad P_3 = \frac{1}{2}(E_{11} + E_{12} + E_{21} + E_{22}), \quad \text{and} \quad P_4 = \frac{1}{2}(E_{11} - E_{12} - E_{21} + E_{22}). \tag{3}$$

Then $\Psi(P_j \otimes Q) = U^*(P_j \otimes P_j)U$ for all $1 \leq j \leq 4$, where $U = U_1 \otimes U_2$. Notice that $P_1 + P_2 = P_3 + P_4$ and hence $P_1 \otimes Q + P_2 \otimes Q = P_3 \otimes Q + P_4 \otimes Q$. But then

$$\begin{aligned} \Psi(P_1 \otimes Q + P_2 \otimes Q) &= U^*(P_1 \otimes P_1 + P_2 \otimes P_2)U \\ &\neq U^*(P_3 \otimes P_3 + P_4 \otimes P_4)U \\ &= \Psi(P_3 \otimes Q + P_4 \otimes Q), \end{aligned}$$

which is a contradiction.

Now suppose that for some $Q \in \mathcal{P}_n$, both $\phi_1(\cdot, Q)$ and $\phi_2(\cdot, Q)$ are of the form (ii). Then $\phi_1(A, Q) = (\text{Tr } A)R_1$ and $\phi_2(A, Q) = (\text{Tr } A)R_2$ for some $R_1 \in \mathcal{P}_m$ and $R_2 \in \mathcal{P}_n$. Therefore, $\Psi(P \otimes Q) = R_1 \otimes R_2$ for all $P \in \mathcal{P}_m$. This contradicts the fact that Ψ is a bijective map. Therefore, either (I) or (II) holds. Applying a similar argument on the map $\phi_2(P, \cdot)$, one can show that

- (III) For all $P \in \mathcal{P}_m$, $\phi_1(P, \cdot)$ has the form (ii) and $\phi_2(P, \cdot)$ has the form (i).
- (IV) For all $P \in \mathcal{P}_m$, $\phi_1(P, \cdot)$ has the form (i) and $\phi_2(P, \cdot)$ has the form (ii).

Fix $P_0 \in \mathcal{P}_m$ and $Q_0 \in \mathcal{P}_n$. Suppose (I) and (IV) hold. Then for any $P \in \mathcal{P}_m$ and $Q \in \mathcal{P}_n$,

$$\phi_2(P, Q) = \phi_2(P_0, Q) = \phi_2(P_0, Q_0).$$

Notice that the former equality is by (I) while the latter equality is by (IV). Contradiction arrived. Similarly, it is impossible that both (II) and (III) hold. Hence, we can conclude that either (I) and (III) hold or (II) and (IV) hold.

Now suppose (I) and (III) hold. Then $\psi_1(\cdot) = \phi_1(\cdot, Q_0)$ and $\psi_2(\cdot) = \phi_2(P_0, \cdot)$ are both of the form (i.a) or (i.b). For all $P \in \mathcal{P}_m$ and $Q \in \mathcal{P}_n$, $\phi_1(P, \cdot)$ and $\phi_2(\cdot, Q)$ are both of the form (ii). Hence, $\phi_1(P, Q_0) = \phi_1(P, Q)$ and $\phi_2(P, Q) = \phi_2(P_0, Q)$. Therefore,

$$\Psi(P \otimes Q) = \phi_1(P, Q) \otimes \phi_2(P, Q) = \phi_1(P, Q_0) \otimes \phi_2(P_0, Q) = \psi_1(P) \otimes \psi_2(Q).$$

Then by the linearity of Ψ and the fact that $\mathcal{P}_m \otimes \mathcal{P}_n$ spans H_{mn} , the result follows. Finally, if (II) and (IV) hold, we may replace Ψ by the linear map $A \otimes B \rightarrow \Psi(B \otimes A)$ and apply the above argument. \square

III. EXTENSION TO MULTIPARTITE SYSTEMS

One can extend Theorem 3 to tensor product of more than two factors as follows:

Theorem 5: Suppose $n_1 \geq \dots \geq n_k \geq 2$ are positive integers with $k > 1$ and $N = \prod_{i=1}^k n_i$. Assume that $\Psi : H_N \rightarrow H_N (\equiv \otimes_{i=1}^k H_{n_i})$ is a linear map. The following are equivalent.

- (a) $\Psi(\otimes_{i=1}^k \mathcal{P}_{n_i}) = \otimes_{i=1}^k \mathcal{P}_{n_i}$.
- (b) $\Psi(\text{conv}(\otimes_{i=1}^k \mathcal{P}_{n_i})) = \text{conv}(\otimes_{i=1}^k \mathcal{P}_{n_i})$.
- (c) There is a permutation π on $\{1, \dots, k\}$ and linear maps ψ_i on H_{n_i} for $i = 1, \dots, k$ such that

$$\Psi(\otimes_{i=1}^k A_i) = \otimes_{i=1}^k \psi_i(A_{\pi(i)}) \quad \text{for} \quad \otimes_{i=1}^k A_i \in \otimes_{i=1}^k H_{n_i},$$

where ψ_i has the form $X \mapsto U_i X U_i^*$ or $X \mapsto U_i X^T U_i^*$, for some unitary $U_i \in M_{n_i}$ and $n_{\pi(i)} = n_i$ for $i = 1, \dots, k$.

Proof: The implications (c) \Rightarrow (a) \Leftrightarrow (b) are clear. Assume that (a) holds. A straightforward generalization of Lemma 2 yields that Ψ is bijective. For $1 \leq r_1 < \dots < r_p \leq k$, define the following linear map

$$\text{Tr}^{r_1, \dots, r_p} : \otimes_{i=1}^k H_{n_i} \rightarrow \otimes_{j=1}^p H_{n_{r_j}} \quad \otimes_{i=1}^k A_i \mapsto \left(\prod_{i \neq r_1, \dots, r_p} \text{Tr} A_i \right) \otimes_{j=1}^p A_{r_j}.$$

In particular, the linear map $\text{Tr}^r : H_N \rightarrow H_{n_r}$ is given by $\text{Tr}^r(\otimes_{i=1}^k A_i) = (\prod_{i \neq r} \text{Tr} A_i) A_r$. For $r = 1, \dots, k$, define maps $\phi_r : (H_{n_1}, \dots, H_{n_k}) \rightarrow H_{n_r}$ by

$$\phi_r(A_1, \dots, A_k) = \text{Tr}^r(\Psi(\otimes_{i=1}^k A_i)) \quad \text{for all} \quad (A_1, \dots, A_k) \in (H_{n_1}, \dots, H_{n_k}).$$

Notice that

$$\Psi(\otimes_{i=1}^k P_i) = \otimes_{r=1}^k \phi_r(P_1, \dots, P_k) \quad \text{for all} \quad (P_1, \dots, P_k) \in (\mathcal{P}_{n_1}, \dots, \mathcal{P}_{n_k}).$$

Given arbitrary $Q_i \in \mathcal{P}_{n_i}$ for $i = 2, \dots, k$, the map $\phi_r(\cdot, Q_2, \dots, Q_k)$ maps \mathcal{P}_{n_1} into \mathcal{P}_{n_r} . By Lemma 4, the map must have the form (i) or (ii) in (2). We claim the following.

Claim: All but one of the maps $\phi_r(\cdot, Q_2, \dots, Q_k)$, $r = 1, \dots, k$, have the form (ii) for all $Q_i \in \mathcal{P}_{n_i}$ and the exceptional map has and the form (i) for all $Q_i \in \mathcal{P}_{n_i}$.

Let $A_1 = E_{11} - E_{22} \in H_{n_1}$. Define $F_r : (\mathcal{P}_{n_2}, \dots, \mathcal{P}_{n_k}) \rightarrow \mathbb{R}$ by

$$F_r(Q_2, \dots, Q_k) = \|\phi_r(A_1, Q_2, \dots, Q_k)\|.$$

Similar to the argument in the proof of Theorem 3, F_r is a constant function. Thus, either

$\phi_r(\cdot, Q_2, \dots, Q_k)$ always have the form (i) for all $Q_i \in \mathcal{P}_{n_i}$, or

$\phi_r(\cdot, Q_2, \dots, Q_k)$ always have the form (ii) for all $Q_i \in \mathcal{P}_{n_i}$.

Next, since Ψ is a bijection, it is impossible to have all $\phi_r(\cdot, Q_2, \dots, Q_k)$ being constant maps. Assume that the maps $\phi_s(\cdot, Q_2, \dots, Q_k)$ and $\phi_t(\cdot, Q_2, \dots, Q_k)$, with $s \neq t$, have the form (i) and

the rest have the form (ii). In this case, $n_s = n_t = n_1$. Consider the linear map $L : H_{n_1} \rightarrow H_{n_s} \otimes H_{n_t}$ defined by $L(A) = \text{Tr}^{s,t} (\Psi (A \otimes (\otimes_{i=2}^k Q_i)))$. Then

$$L(P) = \phi_s(P, Q_2, \dots, Q_k) \otimes \phi_t(P, Q_2, \dots, Q_k) \quad \text{for all } P \in \mathcal{P}_{n_1}.$$

Recall that $\phi_s(P, Q_2, \dots, Q_k)$ and $\phi_t(P, Q_2, \dots, Q_k)$ are of the form (i). Following the same argument as in the proof of Theorem 3, one sees that $P_1 + P_2 = P_3 + P_4$ while $L(P_1) + L(P_2) \neq L(P_3) + L(P_4)$, where P_1, P_2, P_3 , and P_4 are defined in (3). This contradicts that L is a linear map. Thus, the claim holds.

For $p = 2, \dots, k$, applying the same argument on the map $\phi_r(Q_1, \dots, Q_{p-1}, \cdot, Q_{p+1}, \dots, Q_k)$, one can show that all but one of the map $\phi_r(Q_1, \dots, Q_{p-1}, \cdot, Q_{p+1}, \dots, Q_k)$ has the form (ii) for all $Q_i \in \mathcal{P}_{n_i}$ and the exceptional map has and the form (i) for all $Q_i \in \mathcal{P}_{n_i}$. Furthermore, there is a permutation $(\pi(1), \dots, \pi(k))$ of $(1, \dots, k)$ such that $\phi_{\pi(p)}(Q_1, \dots, Q_{p-1}, \cdot, Q_{p+1}, \dots, Q_k)$ has the form (i) for all $Q_i \in \mathcal{P}_{n_i}$. Otherwise, there is r such that $\phi_r(Q_1, \dots, Q_{p-1}, \cdot, Q_{p+1}, \dots, Q_k)$ has the form (ii) for all p and for all $Q_i \in \mathcal{P}_{n_i}$, which contradicts that Ψ is a bijection.

Notice also that $n_p \leq n_{\pi(p)}$ for all $p = 1, \dots, k$. This is possible only when $n_p = n_{\pi(p)}$ for all p . Now replacing Ψ by the map of the form $\otimes_{i=1}^k Q_i \mapsto \Psi (\otimes_{i=1}^k Q_{\pi^{-1}(i)})$, we may assume that $\pi(p) = p$. Then $\phi_p(Q_1, \dots, Q_{p-1}, \cdot, Q_{p+1}, \dots, Q_k)$ has the form (i) for all $Q_i \in \mathcal{P}_{n_i}$, and for any $r \neq p$, $\phi_r(Q_1, \dots, Q_{p-1}, \cdot, Q_{p+1}, \dots, Q_k)$ has the form (ii) for all $Q_i \in \mathcal{P}_{n_i}$. Now fix some $Q_i \in \mathcal{P}_{n_i}$. Then for any $P_i \in \mathcal{P}_{n_i}$,

$$\Psi (\otimes_{i=1}^k P_i) = \otimes_{i=1}^k \phi_i(P_1, \dots, P_k) = \otimes_{i=1}^k \phi_i(Q_1, \dots, Q_{i-1}, P_i, Q_{i+1}, \dots, Q_k) = \otimes_{i=1}^k \phi_i(P_i),$$

where $\phi_i(\cdot) = \phi_i(Q_1, \dots, Q_{i-1}, \cdot, Q_{i+1}, \dots, Q_k)$ has the form (i). By the linearity of Ψ , the result follows. □

Next, we show that one cannot replace condition (b) in Theorem 5 by the weaker condition that Ψ preserves the separable states $\mathcal{S} = \text{conv} (\otimes_{i=1}^k \mathcal{P}_{n_i})$, i.e., $\Psi(\mathcal{S}) \subseteq \mathcal{S}$. In fact, we will see that the convex set \mathcal{L} of separable states preserving linear maps has dimension $N^4 - N^2$, which is the dimension of the convex set of density matrices preserving linear maps on H_N .

Lemma 6: Let $H_N \equiv \otimes_{i=1}^k H_{n_i}$. Define the linear map $L_0 : H_N \rightarrow H_N$ by

$$L_0(A) = \frac{1}{N} \text{Tr}(A)I_N$$

and let $L_1 : H_N \rightarrow H_N$ be any linear operator satisfying

$$\text{Tr}(L_1(A)) = 0 \quad \text{for all } A \in H_N.$$

Then there exists $\tau = \tau(L_1) > 0$ such that $(L_0 + tL_1)(\mathcal{S}) \subseteq \mathcal{S}$ for each $t \in (-\tau(L_1), \tau(L_1))$. Furthermore $\det(L_0 + tL_1) = t^{N^2-1}f(L_1)$, where $f(L_1)$ is a minor of order $N^2 - 1$ of the representation matrix of L_1 in a basis of H_N which contains I_N . In particular, if $f(L_1) \neq 0$ then for each $t \in (-\tau(L_1), \tau(L_1)) \setminus \{0\}$ the linear operator $L_0 + tL_1$ is invertible.

Proof: Clearly, for each $t \in \mathbb{R}$ the operator $L(t) = L_0 + tL_1$ is trace preserving. Hence it maps the hyperplane $\text{Tr}(A) = 1$ to itself. Note that $L(0)(\mathcal{S}) = \frac{1}{N}I_N$. The generalized version of Lemma 1 yields that $\dim \mathcal{S} = N^2 - 1$ and $\frac{1}{N}I_N$ is an interior point of \mathcal{S} . The continuity argument yields that there exists $\tau = \tau(L_1)$ such that $(L_0 + tL_1)(\mathcal{S})$ lies in the interior of \mathcal{S} for $|t| < \tau(L_1)$.

Let L_1^\top be the adjoint operator of L_1 with respect to the standard inner product $\langle A, B \rangle = \text{Tr} AB$ on H_N . The assumption that $\text{Tr}(L_1(A)) = 0$ for all A is equivalent to the assumption that $L_1^\top(I_N) = 0$. Note that $L_0^\top = L_0$, $\text{rank } L_0 = 1$ and $L_0(I_N) = I_N$. Choose a basis in H_N where I_N is one of the elements of this basis. Then $L_0 = E_{ii}$, for some $i \in \{1, \dots, N^2\}$ and L_1 has a zero row i . Clearly $\det L(t) = tf(L_1)$, where $f(L_1)$ is corresponding minor of L_1 . The last claim of the lemma is obvious. □

Corollary 7: Let \mathcal{L} be the set of all linear transformations $L : H_N \rightarrow H_N$ satisfying $L(\mathcal{S}) \subseteq \mathcal{S}$. Then \mathcal{L} is a convex compact set of dimension $N^4 - N^2$. Furthermore the subset $\mathcal{L}_0 \subseteq \mathcal{L}$ of invertible transformations is an open dense set in \mathcal{L} . Hence $\dim \mathcal{L}_0 = N^4 - N^2$.

Proof: Since any $L \in \mathcal{L}$ is trace preserving it follows that $L^\top(I_N) = I_N$. Let \mathcal{L}_1 be the affine set of all linear transformations of H_N to itself satisfying $L^\top(I_N) = I_N$. Then \mathcal{L}_1 is a translation of a linear subspace of dimension $N^4 - N^2$. Hence $\dim \mathcal{L} \leq N^4 - N^2$. Lemma 6 yields that $\dim \mathcal{L} = \dim \mathcal{L}_0 = N^4 - N^2$. \square

IV. THE PRODUCT NUMERICAL RANGE

In Ref. 3 the authors introduced the concept of (tensor) product numerical range of $T \in M_{mn}$ defined by

$$W^\otimes(T) = \{\text{Tr}(TX) : X \in \mathcal{P}_m \otimes \mathcal{P}_n\}.$$

This is also known as the decomposable numerical range associated with the tensor product of an operator; see Ref. 10 and its references. It was shown in Refs. 3 and 13 that the product numerical range is a useful concept in studying various problems in quantum information theory. To avoid the nontrivial case we let $m, n \geq 2$.

Observe that H_m is real subspace of M_m and $M_m = H_m \oplus \sqrt{-1}H_m$. Hence, any real linear automorphism of H_m lifts to a complex linear automorphism of M_m . Recall that M_m is endowed with the standard inner product $\langle X, Y \rangle = \text{Tr} XY^*$. Assume that $\Phi : M_m \rightarrow M_m$ is a linear map. Then $\Psi^* : M_m \rightarrow M_m$ is the dual linear map given by the equality $\langle \Psi(X), Y \rangle = \langle X, \Psi(Y) \rangle$ for all $X, Y \in M_m$. Theorem 3 yields.

Theorem 8: Let $m, n \geq 2$ and $\Psi : M_{mn} \rightarrow M_{mn}$ be a linear map. The following are equivalent.

- (a) $W^\otimes(\Psi(T)) = W^\otimes(T)$ for all $T \in M_{mn}$.
- (b) $\text{conv} \{W^\otimes(\Psi(T))\} = \text{conv} \{W^\otimes(T)\}$ for all $T \in M_{mn}$.
- (c) Ψ has the form described in Theorem 3 (c).

Proof: The implications (c) \Rightarrow (a) \Rightarrow (b) are clear. Suppose (b) holds. Note that

$$\text{conv} \{W^\otimes(T)\} = \{\text{Tr}(TZ) : Z \in \mathcal{S}_{m,n}\}.$$

Thus the dual map Ψ^* satisfies $\Psi^*(\mathcal{S}_{m,n}) = \mathcal{S}_{m,n}$ and has the form described in Theorem 3 (c). One readily checks that the dual map of such a map has the same form. The result follows. \square

In the multipartite case, we can define the product numerical range of a matrix by

$$W^\otimes(T) = \{\text{Tr}(TZ) : Z \in \otimes_{i=1}^k \mathcal{P}_{n_i}\},$$

and deduce the following from Theorem 5.

Theorem 9: Suppose $n_1 \geq \dots \geq n_k \geq 2$ are positive integers with $k > 1$ and $N = \prod_{i=1}^k n_i > 1$. Suppose $\Psi : M_N \rightarrow M_N$ is a linear map. The following are equivalent.

- (a) $W^\otimes(\Psi(T)) = W^\otimes(T)$ for all $T \in M_N$.
- (b) $\text{conv} \{W^\otimes(\Psi(T))\} = \text{conv} \{W^\otimes(T)\}$ for all $T \in M_N$.
- (c) Ψ has the form described in Theorem 5 (c).

ACKNOWLEDGMENTS

This research was done while the second author was visiting the George Washington University during his SSRL leave from the College of William & Mary in the fall of 2010. Research of Li and Poon was partially supported by USA NSF. Research of Li and Sze was partially supported by HK RGC. Li was also supported by the Key Disciplines of Shanghai Municipality Grant S30104.

¹ Alfsen, E. and Shultz, F., "Unique decompositions, faces, and automorphisms of separable states," *J. Math. Phys.* **51**, 052201 (2010).

² Baruch, E. M. and Loewy, R., "Linear preservers on spaces of Hermitian or real symmetric matrices," *Numer. Linear Algebra Appl.* **183**, 89 (1993).

³ Bengtsson, I. and Życzkowski, K., *Geometry of Quantum States* (Cambridge University Press, Cambridge, UK, 2006).

- ⁴Friedland, S. and Gour, G., "Closed formula for the relative entropy of entanglement in all dimensions," (submitted); e-print arXiv:1007.4544 [quant-ph].
- ⁵Gurvits, L., "Classical deterministic complexity of Edmonds problem and quantum entanglement, in *Proceedings of the 35th ACM Symposium on Theory of Computing*, June 9–11, 2003, San Diego, CA, USA (ACM Press, New York, 2003).
- ⁶Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K., "Quantum entanglement," *Rev. Mod. Phys.* **81**, 865 (2009).
- ⁷Horodecki, M., Horodecki, P., and Horodecki, R., "Separability of mixed states: Necessary and sufficient conditions," *Phys. Lett. A* **223**, 1 (1996).
- ⁸Hulpke, F., Poulsen, U. V., Sanpera, A., Sen(De), A., Sen, U., and Lewenstein, M., "Unitary as preservation of entropy and entanglement in quantum systems," *Found. Phys.* **36** 477 (2006).
- ⁹Johnston, N., "Characterizing operations preserving separability measures via linear preserver problems," e-print arXiv:1010.1432.
- ¹⁰Li, C. K. and Zaharia, Z., "Induced operators on symmetry classes of tensors," *Trans. Amer. Math. Soc.* **354**(2), 807 (2002).
- ¹¹Peres, A., "Separability criterion for density matrices," *Phys. Rev. Lett.* **77**, 1413 (1996).
- ¹²Plenio, M. B. and Virmani, S., "An introduction to entanglement measures," *Quantum Inf. Comput.* **7**, 1 (2007).
- ¹³Puchala, Z., Gawron, P., Miszczak, J. A., Skowronek, Ł., Choi, M. D., and Życzkowski, K., "Product numerical range in a space with tensor product structure," *Linear Algebra Appl.* **434**, 327 (2011).
- ¹⁴Vedral, V. and Plenio, M. B., "Entanglement measures and purification procedures," *Phys. Rev. A* **57**, 1619 (1998).
- ¹⁵Zinchenko, Y., Friedland, S., and Gour, G., "Numerical estimation of the relative entropy of entanglement," *Phys. Rev. A* **82**, 052336 (2010).