

# Unique decompositions, faces, and automorphisms of separable states

Erik Alfsen<sup>1, a)</sup> and Fred Shultz<sup>2, b)</sup>

<sup>1)</sup> *Mathematics Department, University of Oslo, Blindern 1053, Oslo, Norway*

<sup>2)</sup> *Mathematics Department, Wellesley College, Wellesley, Massachusetts 02481, USA*

(Dated: March 24, 2010)

Let  $S_k$  be the set of separable states on  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  admitting a representation as a convex combination of  $k$  pure product states, or fewer. If  $m > 1, n > 1$ , and  $k \leq \max(m, n)$ , we show that  $S_k$  admits a subset  $V_k$  such that  $V_k$  is dense and open in  $S_k$ , and such that each state in  $V_k$  has a unique decomposition as a convex combination of pure product states, and we describe all possible convex decompositions for a set of separable states that properly contains  $V_k$ . In both cases we describe the associated faces of the space of separable states, which in the first case are simplexes, and in the second case are direct convex sums of faces that are isomorphic to state spaces of full matrix algebras. As an application of these results, we characterize all affine automorphisms of the convex set of separable states, and all automorphisms of the state space of  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  that preserve entanglement and separability.

Keywords: entanglement, separable state, face, affine automorphism

## I. INTRODUCTION

A state on the algebra  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  of linear operators is separable if it is a convex combination of product states. States that are not separable are said to be entangled, and are of substantial interest in quantum information theory. Easily applied conditions for separability are known only for special cases, e.g., if  $m = n = 2$ , then a state is separable iff its associated density matrix has positive partial transpose (“PPT”)<sup>6,22</sup>. Other necessary and sufficient conditions are known, e.g., cf. Ref. 6, but are not easily applied in practice. An open question of great interest is to find a simple necessary and sufficient condition for a state to be separable.

A product state  $\omega \otimes \tau$  is a pure state iff  $\omega$  and  $\tau$  are pure states. Thus a separable state is precisely one that admits a representation as a convex combination of pure product states. It is natural to ask the extent to which this decomposition is unique. That is the main topic of this article. We will first summarize our results, and then discuss some related previous results about product vectors and about the tetrahedron/octahedron picture of separable states on  $\mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ .

For the full state space  $K$  of  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  each non-extreme point can be decomposed into extreme points in many different ways. But for the space  $S$  of separable states the situation is totally different. While non-extreme points with many different decompositions exist (and are easy to find) in  $S$  as well as in  $K$ , there are in  $S$  also plenty of points for which the decomposition is unique.

DiVincenzo, Terhal, and Thapliyal<sup>5</sup> defined the *optimal ensemble cardinality* of a separable state  $\rho$  to be  $k$  if  $k$  is the minimal number of pure product states required

for a convex decomposition of  $\rho$ . This cardinality cannot be less than the rank of  $\rho$ , but can exceed the rank<sup>5</sup>. Lockhart<sup>19</sup> used the term “optimal ensemble length” for the same notion. For brevity, we will simply call this number the *length* of  $\rho$ , and we denote the set of separable states of length at most  $k$  by  $S_k$ .

Assume that  $m \leq n$ . For each  $k$ , let  $V_k$  be the set of states that are convex combinations of product vector states  $\omega_{x_1 \otimes y_1}, \dots, \omega_{x_p \otimes y_p}$  where  $x_1, \dots, x_p$  are distinct (up to scalar multiples) and  $y_1, \dots, y_p$  are linearly independent, with  $p \leq k$ . In Corollary 5 we show that for each  $k$  each state in  $V_k$  has a unique decomposition into product vector states. (Actually, we show each state in  $V_k$  generates a face of  $S$  which is a simplex, from which the uniqueness follows.) Theorem 6 shows that the property of having a unique decomposition into product vector states is generic in  $S_k$  for  $k \leq n$ , by showing that  $V_k$  is dense and open in  $S_k$ .

Here openness is with respect to the relative topology of  $S_k$ ;  $V_k$  is not open or dense in  $S$  or  $K$  if  $mn > 1$ . (See the remarks after Theorem 6). Indeed it would be surprising if a subset of low rank separable states were open and dense in the set of all states of that rank, since low rank states are almost surely entangled<sup>24,30</sup>, and in general  $S$  has measure which is a decreasingly small fraction of the measure of  $K$  as  $m, n$  increase<sup>3,28</sup>.

We also obtain results on the possible decompositions of states that are convex combinations of vector states for vectors  $\{x_i \otimes y_i \mid 1 \leq i \leq p\}$  with  $y_1, \dots, y_p$  independent without the assumption that  $x_1, \dots, x_p$  are distinct. We show such states have a unique decomposition as a convex combination of product states  $\rho_i \otimes \sigma_i$  that are not necessarily pure, but with the property that each of them generates a face of  $S$  which is also a face of  $K$  and is affinely isomorphic to the state space of  $\mathcal{B}(\mathbb{C}^{p_i})$  for a suitable  $p_i$ . From this it follows that the ambiguity in decompositions for a given state in this class is restricted to the ambiguity in decompositions for points in the state space of the matrix algebras  $\mathcal{B}(\mathbb{C}^{p_i})$ . For a

---

<sup>a)</sup> Electronic mail: [alfsen@math.uio.no](mailto:alfsen@math.uio.no)

<sup>b)</sup> Electronic mail: [fshultz@wellesley.edu](mailto:fshultz@wellesley.edu)

complete description of the possible decompositions of a state on  $\mathcal{B}(\mathbb{C}^p)$ , see Refs. 10, 16, and 26.

In the last section of the current article, we use our results on the facial structure of  $S$  to show that every affine automorphism of the space  $S$  of separable states on  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  is given by a composition of the duals of the maps that are (i) conjugation by local unitaries (i.e., unitaries of the form  $U_1 \otimes U_2$ ) (ii) the two partial transpose maps, or (iii) the swap automorphism that takes  $A \otimes B$  to  $B \otimes A$  (if  $m = n$ ). A consequence is a description of the affine automorphisms  $\Phi$  of the state space such that  $\Phi$  preserves entanglement and separability.

There is related work of Hulpke et al<sup>11</sup>. They say a linear map  $L$  on  $\mathbb{C}^m \otimes \mathbb{C}^n$  preserves *qualitative entanglement* if  $L$  sends separable (i.e., product) vectors to product vectors, and entangled vectors to entangled vectors. They show that a linear map  $L$  preserves qualitative entanglement of vectors on  $\mathbb{C}^m \otimes \mathbb{C}^n$  iff  $L$  is a local operator (i.e. one of the form  $L_1 \otimes L_2$ ), or if  $L$  is a local operator composed with the swap map that takes  $x \otimes y$  to  $y \otimes x$ . They then show that if  $L$  preserves a certain *quantitative* measure of entanglement, then  $L$  must be a local unitary.

## Related work

While dimensions are too high to be able to accurately visualize the above results, the reader may be curious about the relationship of our results to the well known tetrahedron/octahedron picture for  $m = n = 2$ , cf. Ref. 7. In that picture, there is a subset  $\mathcal{T}$  of states which is a tetrahedron, and which has the property that for every state  $\rho$  which restricts to the normalized trace on  $\mathcal{B}(\mathbb{C}^2) \otimes I$  and on  $I \otimes \mathcal{B}(\mathbb{C}^2)$ , there are unitaries  $U$  and  $V$  such that  $(U \otimes V)^* \rho (U \otimes V) \in \mathcal{T}$ . The midpoints of the six edges of this tetrahedron are the vertices of an octahedron that consists of the separable states in  $\mathcal{T}$ . Each vertex of the octahedron is a convex combination of two distinct pure product states (which of course are not in  $\mathcal{T}$ ), cf. eqn. (63) of Ref. 20. In fact, the vertices are the only states in the octahedron of length  $\leq \max(m, n) = 2$ .

It can be checked (e.g., by applying our Corollary 5) that the decomposition of each of these vertices into pure product states is unique. Each state in the interior of this octahedron has rank  $4 = mn$ , so is an interior point of the full state space  $K$ , hence has a non-unique convex decomposition into pure product states (see the remarks after Theorem 6.) The tetrahedron also arises as a parameterization for a set of unital completely positive trace preserving maps from  $M_2(\mathbb{C})$  to  $M_2(\mathbb{C})$ , with the octahedron consisting of the entanglement breaking maps in this set, cf. Appendix B of Ref. 15, Thm. 4 of Ref. 23, and Figure 2 in Ref. 24.

In proving the uniqueness results described above, an important role is played by a description of the product vectors in certain subspaces. For example, our Lemma 2 describes the product vectors in the span of a set of prod-

uct vectors  $x_1 \otimes y_1, \dots, x_p \otimes y_p$  in the case where  $y_1, \dots, y_p$  are linearly independent. Describing the set of product vectors in a given subspace of  $\mathbb{C}^m \otimes \mathbb{C}^n$  plays a role in some tests of separability, e.g., the Range Criterion<sup>8</sup>. This states that if  $\rho$  is separable, then there exist product vectors  $x_1 \otimes y_1, \dots, x_p \otimes y_p$  whose span is the range of  $\rho$ , with the span of  $x_1 \otimes \bar{y}_1, \dots, x_p \otimes \bar{y}_p$  being the range of the partially transposed state  $\rho^{T_2}$ . The Range Criterion has been used to construct states that are PPT states but are not separable<sup>4</sup>.

Ref. 25 includes a description of the possibilities for product vectors in two dimensional subspaces of  $\mathbb{C}^2 \otimes \mathbb{C}^2$ . Ref. 17 shows that every subspace with dimension greater than  $n$  in  $\mathbb{C}^2 \otimes \mathbb{C}^n$  contains infinitely many product vectors, and that a subspace of dimension  $n$  contains at least one. On the other hand, for the purpose of finding decompositions, it is helpful to know when there are only finitely many product vector states in a subspace. In Ref. 9 it is shown if  $\rho$  is a PPT state on  $\mathbb{C}^m \otimes \mathbb{C}^n$  such that  $\text{rank}(\rho) + \text{rank}(\rho^{T_2}) \leq 2mn - m - n + 2$ , then “typically” there are only finitely many product vector states  $\omega_{x \otimes y}$  such that  $x \otimes y$  is in the range of  $\rho$  and  $x \otimes \bar{y}$  is in the range of  $\rho^{T_2}$ .

Our uniqueness results refer to the set of states that can be written as a convex combination of product vector states  $\omega_{x_i \otimes y_i}$  with  $y_1, \dots, y_n$  independent. This set of states has appeared in other contexts. In Ref. 17 (for  $m = 2$ ) and Lemma 6 and Thm. 1 of Ref. 9 (for general  $m$ ) it is shown that these states are the same as the PPT states that are supported on  $\mathbb{C}^m \otimes \mathbb{C}^n$  and have rank  $n$ . (The difficult direction is to show that such states are separable and admit a decomposition with  $y_1, \dots, y_n$  independent; the other direction is clear.) Both Refs. 17 and 9 also describe algorithms to find decompositions of such separable states into pure product states.

There are related results in the  $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^n$  context in Ref. 14. A different kind of uniqueness result appears in Ref. 18, where the existence of a decomposition of an arbitrary state into the sum of a separable (unnormalized) state plus a state of minimal trace is proven; this decomposition is shown to be unique in the  $\mathbb{C}^2 \otimes \mathbb{C}^2$  context.

## II. BACKGROUND: STATES ON $\mathcal{B}(\mathbb{C}^n)$

We review basic facts about states on  $\mathcal{B}(\mathbb{C}^n)$ , and develop some facts about the relationship of independence of vectors  $x$  in  $\mathbb{C}^n$  and of the corresponding vector states  $\omega_x$ . In the following sections we will specialize to the case of interest: separable states.

*Notation.* If  $x$  is a vector in any vector space,  $[x]$  denotes the subspace generated by  $x$ .  $\mathbb{C}^n$  denotes the set of  $n$ -tuples of complex numbers viewed as an inner product space with the usual inner product (linear in the first factor).  $\mathcal{B}(\mathbb{C}^n)$  denotes the linear transformations from  $\mathbb{C}^n$  into itself. For each unit vector  $x \in \mathbb{C}^n$ , we denote the associated vector state by  $\omega_x$ , so that  $\omega_x(A) = (Ax, x)$ . The convex set of states on  $\mathcal{B}(\mathbb{C}^n)$  will be denoted by  $K_n$ .

We recall that faces of the state space  $K_n$  of  $\mathcal{B}(\mathbb{C}^n)$  are in 1-1 correspondence with the projections in  $\mathcal{B}(\mathbb{C}^n)$ , and thus with the subspaces of  $\mathbb{C}^n$  that are the ranges of these projections. If  $Q$  is a projection in  $\mathcal{B}(\mathbb{C}^n)$ , then the associated face  $F_Q$  of  $K_n$  consists of all states taking the value 1 on  $Q$ . The restriction map is an affine isomorphism from  $F_Q$  onto the state space of  $Q\mathcal{B}(\mathbb{C}^n)Q \cong \mathcal{B}(Q(\mathbb{C}^n))$ . Thus  $F_Q$  is affinely isomorphic to the state space of  $\mathcal{B}(L)$ , where  $L = Q(\mathbb{C}^n)$ . The set of extreme points of  $K_n$  are the vector states, and it follows that the extreme points of  $F_Q$  are the vector states  $\omega_x$  with  $x$  in the range of  $Q$ , and  $F_Q$  is the convex hull of these vector states. For background, see Chapter 4 of Ref. 2

*Definition.* Recall that a convex set  $C$  is said to be the *direct convex sum* of a collection of convex subsets  $C_1, \dots, C_p$  if each point  $\omega \in C$  can be uniquely expressed as a convex combination

$$\omega = \sum_{i \in I} \lambda_i \omega_i \quad (1)$$

where  $I \subset \{1, \dots, p\}$ ,  $\lambda_i > 0$  for all  $i \in I$ ,  $\omega_i \in C_i$  for all  $i \in I$ , and  $\sum_{i \in I} \lambda_i = 1$ .

If  $C$  is a convex subset of a real linear space and is located on an affine hyperplane which does not contain the origin (as is the case for our state spaces), then it is easily seen that  $C$  is the direct convex sum of convex subsets  $C_1, \dots, C_p$  iff the span of  $C$  is the direct sum of the real subspaces spanned by  $C_1, \dots, C_p$ .

A finite dimensional convex set is a *simplex* if it is the direct convex sum of a finite set of points. If the affine span of the points does not contain the origin, then their convex hull is a simplex iff the points are linearly independent (over  $\mathbb{R}$ ).

**Lemma 1.** *Let  $L$  be a subspace of  $\mathbb{C}^n$  and suppose that  $L$  is the direct sum of subspaces  $L_1, \dots, L_p$ . Let  $F_1, \dots, F_p$  be the corresponding faces of the state space of  $\mathcal{B}(\mathbb{C}^n)$ . Then the convex hull of  $F_1, \dots, F_p$  is the direct convex sum of those faces. In particular, if  $x_1, \dots, x_p$  are linearly independent unit vectors, then the corresponding vector states are linearly independent and the convex hull of the corresponding vector states is a simplex.*

*Proof.* Let  $I \subset \{0, \dots, p\}$ , and suppose  $\{\omega_i \mid i \in I\}$  are nonzero functionals on  $\mathcal{B}(\mathbb{C}^n)$  with  $\omega_i \in \text{span}_{\mathbb{R}} F_i$  for each  $i$ . To prove independence of  $\{\omega_i \mid i \in I\}$ , suppose that for scalars  $\{\gamma_i\}_{i \in I}$  we have

$$\sum_{i \in I} \gamma_i \omega_i = 0. \quad (2)$$

Let  $L_0$  be the orthogonal complement of  $L$ . Then  $\mathbb{C}^n$  as a linear space is the direct sum of  $L_0, L_1, \dots, L_p$ .

For each  $i \in I$ , let  $P_i$  be the projection associated with  $F_i$ . Then we can find  $A_i \in P_i \mathcal{B}(\mathbb{C}^n) P_i$  such that  $\omega_i(A_i) \neq 0$ . Let  $B_i \in \mathcal{B}(\mathbb{C}^n)$  be an operator such that  $B_i$  is zero on  $\sum_{j \neq i} L_j$ , and such that  $\omega_i(B_i) \neq 0$  (e.g., set  $B_i = A_i$  on  $L_i$ ). If  $x \in L_j$  and  $j \neq i$ , then  $\omega_x(B_i) = (B_i x, x) = 0$ .

Since every state in  $F_j$  is a convex combination of vector states  $\omega_x$  with  $x \in L_j$ , then  $\omega_j(B_i) = 0$  if  $j \neq i$ .

Now apply both sides of (2) to  $B_k$  to conclude that  $\gamma_k \omega_k(B_k) = 0$  for all  $k \in I$ , so  $\gamma_k = 0$  for all  $k \in I$ . Thus the set of vectors  $\omega_1, \dots, \omega_p$  is independent. We conclude that  $\text{co}(F_1, \dots, F_p)$  is the direct convex sum of  $F_1, \dots, F_p$ .

If  $x_1, \dots, x_p$  are linearly independent unit vectors, applying the result above with  $F_i = \{\omega_{x_i}\}$  shows that the convex hull of the vector states  $\omega_{x_i}$  is a simplex. Hence the set  $\{\omega_{x_1}, \dots, \omega_{x_p}\}$  is linearly independent.  $\square$

Note that the converses of the statements above are not true. For example, while no set of more than two vectors in  $\mathbb{C}^2$  is independent, it is easy to find a set of three linearly independent vector states on  $\mathcal{B}(\mathbb{C}^2)$ .

### III. UNIQUENESS OF DECOMPOSITIONS OF SEPARABLE STATES

We now turn to faces of the set of separable states on  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$ , and to the question of uniqueness of convex decompositions of such states. We identify  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  with  $\mathcal{B}(\mathbb{C}^m) \otimes \mathcal{B}(\mathbb{C}^n)$  by  $(A \otimes B)(x \otimes y) = Ax \otimes By$ . We denote the convex set of all states on  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  by  $K$ , and the convex set of all separable states by  $S$ .

**Lemma 2.** *Let  $e_1, e_2, \dots, e_p$  and  $f_1, f_2, \dots, f_p$  be unit vectors in  $\mathbb{C}^m$  and  $\mathbb{C}^n$  respectively. We assume that  $f_1, f_2, \dots, f_p$  are linearly independent. If  $e \in \mathbb{C}^m$  and  $f \in \mathbb{C}^n$  are unit vectors such that  $e \otimes f$  is in the linear span of  $\{e_i \otimes f_i \mid 1 \leq i \leq p\}$ , then there is an index  $j$  such that  $[e] = [e_j]$  and such that  $f$  is in the span of those  $f_i$  such that  $[e_i] = [e_j]$ . In the special case where  $[e_1], \dots, [e_p]$  are distinct, then  $[e] = [e_j]$  and  $[f] = [f_j]$  for some index  $j$ , and  $\{e_i \otimes f_i \mid 1 \leq i \leq p\}$  is independent.*

*Proof.* Extend  $f_1, \dots, f_p$  to a basis  $f_1, \dots, f_n$  of  $\mathbb{C}^n$ , and let  $\hat{f}_1, \dots, \hat{f}_n$  be the dual basis. For  $1 \leq k \leq n$ , let  $T_k : \mathbb{C}^m \otimes \mathbb{C}^n \rightarrow \mathbb{C}^m$  be the linear map such that  $T_k(x \otimes y) = \hat{f}_k(y)x$  for  $x \in \mathbb{C}^m, y \in \mathbb{C}^n$ .

Suppose that the product vector  $e \otimes f$  is a linear combination

$$e \otimes f = \sum_{i=1}^p \alpha_i e_i \otimes f_i. \quad (3)$$

For  $j > p$ , applying  $T_j$  to both sides of (3) gives  $\hat{f}_j(f)e = 0$ , so  $\hat{f}_j(f) = 0$  for all such  $j$ . Now if  $1 \leq j \leq p$ , applying  $T_j$  to both sides of (3) gives

$$\hat{f}_j(f)e = \alpha_j e_j. \quad (4)$$

Since  $\hat{f}_j(f)$  can't be zero for all  $j$ , then  $e$  is a multiple of some  $e_j$ . Fix such an index  $j$ . If  $1 \leq i \leq p$  and  $[e_i] \neq [e_j]$ , then  $e_i$  can't be a multiple of  $e$ , so  $\hat{f}_i(f)e = \alpha_i e_i$  implies  $\alpha_i = 0$ , and then also  $\hat{f}_i(f) = 0$ . We have shown that

$\widehat{f}_i(f) = 0$  if  $i > p$ , or if  $i \leq p$  and  $[e_i] \neq [e_j]$ . It follows that  $f$  is in the linear span of those  $f_i$  such that  $[e_i] = [e_j]$ .

If it also happens that  $[e_1], \dots, [e_p]$  are distinct, and  $[e] = [e_j]$ , then  $[f] = [f_j]$ . Suppose now that  $\sum_i \alpha_i e_i \otimes f_i = 0$ . If  $\alpha_k \neq 0$ , then  $e_k \otimes f_k$  is a linear combination of  $\{e_i \otimes f_i \mid i \neq k\}$ . Thus by the conclusion just reached, we must have  $[e_k] = [e_i]$  for some  $i \neq k$ , contrary to the hypothesis that  $[e_1], \dots, [e_p]$  are distinct. We conclude that  $\alpha_k = 0$  for all  $k$ , and we have shown that  $\{e_i \otimes f_i \mid 1 \leq i \leq p\}$  is independent.  $\square$

**Lemma 3.** *Let  $e_1, \dots, e_p \in \mathbb{C}^m$  and  $f_1, \dots, f_p \in \mathbb{C}^n$  be unit vectors. If  $[e_1] = [e_2] = \dots = [e_p]$ , then the face  $F$  of  $S$  generated by the states  $\{\omega_{e_i \otimes f_i} \mid 1 \leq i \leq p\}$  is also a face of  $K$ , and this face of  $K$  is associated with the subspace  $L = e_1 \otimes \text{span}\{f_1, \dots, f_p\}$  of  $\mathbb{C}^m \otimes \mathbb{C}^n$ , and  $F$  is affinely isomorphic to the state space of  $\mathcal{B}(L)$ .*

*Proof.* Let  $G$  be the face of  $K$  which is associated with the subspace  $L$  of  $\mathbb{C}^m \otimes \mathbb{C}^n$ . By assumption each  $e_i$  is a multiple of  $e_1$ , so that

$$L = \text{span}\{e_1 \otimes f_i \mid 1 \leq i \leq p\} = \text{span}\{e_i \otimes f_i \mid 1 \leq i \leq p\}.$$

Hence  $G$  is the face of  $K$  generated by  $\{\omega_{e_i \otimes f_i} \mid 1 \leq i \leq p\}$ .

We would like to show  $G = F$ . For brevity we denote the convex hull of the set  $\{\omega_{e_i \otimes f_i} \mid 1 \leq i \leq p\}$  by  $C$ , and observe that  $G$  and  $F$  are the faces of  $K$  and  $S$  respectively generated by  $C$ . It follows easily from the definition of a face that the face generated by the convex set  $C$  in either one of the two convex sets  $S$  or  $K$  consists of all points  $\rho$  in  $S$  or  $K$  respectively which satisfy an equation

$$\omega = \lambda \rho + (1 - \lambda) \sigma \quad (5)$$

where  $0 < \lambda < 1$ ,  $\omega \in C$ , and where  $\sigma$  is in  $S$  or  $K$  respectively. It follows that  $F = \text{face}_S(C) \subset \text{face}_K(C) = G$ .

Since each vector in  $L$  is a product vector, the extreme points of  $G$  are pure product states, so  $G \subset S$ . If  $\rho$  is in the face  $G$  of  $K$  generated by  $C$ , then we can find  $\sigma \in K$  and  $\omega \in C$  such that (5) holds. Then  $\sigma$  is also in  $G \subset S$ , so both  $\rho$  and  $\sigma$  are in  $S$ . Hence  $\rho$  is in the face  $F$  of  $S$  generated by  $C$ . Thus  $G \subset F$ , and so  $F = G$  follows.  $\square$

So far we have considered collections of product vectors  $\{e_i \otimes f_i\}$  with  $\{f_1, \dots, f_p\}$  linearly independent. In Lemma 3 we have described the face  $F$  of  $S$  generated these states in the special case where all of the  $e_i$  are multiples of each other. In this case  $F$  is also a face of  $K$ .

We now remove the restriction that all of the one-dimensional subspaces  $[e_i]$  coincide. We are going to partition the set of vectors  $e_i \otimes f_i$  into subsets for which these subspaces coincide, and apply Lemma 3 to each such subset. For simplicity of notation, we renumber the vectors in the fashion we now describe.

**Theorem 4.** *Let  $e_1, e_2, \dots, e_p$  and  $f_1, f_2, \dots, f_p$  be unit vectors in  $\mathbb{C}^m$  and  $\mathbb{C}^n$  respectively, and with  $f_1, \dots, f_p$  linearly independent. We assume that the vectors are ordered so that  $[e_1], \dots, [e_q]$  are distinct, and so that for  $i > q$  each  $[e_i]$  equals one of  $[e_1], \dots, [e_q]$ . For  $1 \leq i \leq q$ , let  $F_i$  be the face of  $S$  generated by the states  $\{\omega_{e_j \otimes f_j} \mid [e_j] = [e_i]\}$  and  $1 \leq j \leq p\}$ . Then each  $F_i$  is also a face of  $K$ , and the face  $F$  of  $S$  generated by  $\{\omega_{e_i \otimes f_i} \mid 1 \leq i \leq p\}$  is the direct convex sum of  $F_1, \dots, F_q$ . Moreover, each  $F_i$  is affinely isomorphic to the state space of  $\mathcal{B}(L_i)$ , where  $L_i = e_i \otimes \text{span}\{f_j \mid [e_i] = [e_j]\}$ . In the special case when  $[e_1], \dots, [e_p]$  are distinct, then  $F$  is the convex hull of  $\{\omega_{e_i \otimes f_i} \mid 1 \leq i \leq p\}$ , and  $F$  is a simplex.*

*Proof.* By Lemma 3, the face  $F_i$  of  $S$  is equal to the face of  $K$  generated by  $\{\omega_{e_j \otimes f_j} \mid [e_j] = [e_i]\}$ , and is affinely isomorphic to the state space of  $\mathcal{B}(L_i)$ .

We will show  $L_1, \dots, L_q$  are independent (i.e., that  $L_1 + L_2 + \dots + L_q$  is a vector space direct sum). For  $1 \leq i \leq q$  let  $e_i \otimes g_i$  be a nonzero vector in  $L_i$ . For  $i \neq j$ ,  $g_i$  and  $g_j$  are linear combinations of disjoint subsets of  $f_1, f_2, \dots, f_p$ , so by independence of  $f_1, f_2, \dots, f_p$ , the subset  $\{g_1, \dots, g_q\}$  is independent. Thus by Lemma 2,  $\{e_1 \otimes g_1, \dots, e_p \otimes g_p\}$  is independent, and hence the subspaces  $L_1, \dots, L_q$  are independent. Hence by Lemma 1, the convex hull of the faces  $F_i$  is a direct convex sum of those faces.

Finally, we need to show that this convex hull coincides with the face  $F$  of  $S$ . Extreme points of  $F$  are extreme points of  $S$ , so are pure product states. Suppose that  $\omega_{x \otimes y}$  is a pure product state in  $F$ . Then  $\omega_{x \otimes y}$  is in the face of  $K$  generated by  $\{\omega_{e_i \otimes f_i} \mid 1 \leq i \leq p\}$ , so  $x \otimes y$  is in  $\text{span}\{e_i \otimes f_i \mid 1 \leq i \leq p\}$ . By Lemma 2,  $[x] = [e_j]$  for some  $j$ , and  $y \in \text{span}\{f_i \mid [e_i] = [e_j]\}$ . Hence  $\omega_{x \otimes y} \in F_j$ . Thus each extreme point of  $F$  is in some  $F_j$ , so  $F$  is contained in the convex hull of  $\{F_i \mid 1 \leq i \leq q\}$ . Evidently  $F$  contains every  $F_j$ , so this convex hull equals  $F$ .  $\square$

In Theorem 4 we showed that the face  $F$  is the direct convex sum of faces that are affinely isomorphic to state spaces of full matrix algebras. Convex sets of this type were studied by Vershik (in both finite and infinite dimensions), who called them *block simplexes*<sup>29</sup>. Other examples are provided by state spaces of any finite dimensional  $C^*$ -algebra. Our Theorem 4 provides new examples of such block simplexes.

**Corollary 5.** *Let  $e_1, e_2, \dots, e_p$  and  $f_1, f_2, \dots, f_p$  be unit vectors in  $\mathbb{C}^m$  and  $\mathbb{C}^n$  respectively. We assume that  $[e_i] \neq [e_j]$  for  $i \neq j$ , and that  $f_1, f_2, \dots, f_p$  are linearly independent. If  $\lambda_1, \dots, \lambda_k$  are nonnegative numbers with sum 1, then the separable state  $\omega = \sum_i \lambda_i \omega_{e_i \otimes f_i}$  has a unique representation as a convex combination of pure product states.*

*Proof.* Suppose  $\omega$  equals the convex combination  $\sum_j \gamma_j \tau_j$  where each  $\tau_j$  is a pure product state. Then each  $\tau_j$  is in the face  $F$  of  $S$  generated by  $\omega$ . By Theorem 4,  $F$  is a simplex, and the extreme points of  $F$  are all of the form  $\omega_{e_i \otimes f_i}$ . Since each  $\tau_j$  is a vector state, it is a pure

state as well, so each state  $\tau_j$  must be an extreme point of  $F$ , and thus must equal some  $\omega_{e_i \otimes f_i}$ . Uniqueness of the representation of  $\omega$  follows from the uniqueness of convex decompositions into extreme points of a (finite dimensional) simplex.  $\square$

*Definition.* A separable state  $\omega$  has *length*  $k$  if  $\omega$  can be expressed as a convex combination of  $k$  pure product states and admits no decomposition into fewer than  $k$  pure product states. We denote by  $S_k$  the set of separable states of length at most  $k$ .

*Definition.* A separable state  $\omega$  has a *unique decomposition* if it can be written as a convex combination of pure product states in just one way

By the above result, roughly speaking decompositions of separable states on  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  of length  $\leq \max(m, n)$  generically are unique. Here's a more precise statement.

Let  $k \leq \max(m, n)$ , and let  $V_k$  be the set of states  $\omega$  admitting a convex decomposition  $\omega = \sum_{i=1}^k \lambda_i \omega_{e_i \otimes f_i}$ , where  $e_1, \dots, e_k$  and  $f_1, \dots, f_k$  are unit vectors in  $\mathbb{C}^m$  and  $\mathbb{C}^n$  respectively,  $0 < \lambda_i$  for  $1 \leq i \leq k$ ,  $[e_1], \dots, [e_k]$  are distinct, and  $\{f_1, \dots, f_k\}$  is linearly independent.

**Theorem 6.** *Let  $m, n > 1$ . For a given  $k \leq \max(m, n)$ , the states in  $V_k$  have length  $k$ , and have unique decompositions. The set  $V_k$  is open and dense in the set  $S_k$  of separable states of length at most  $k$ .*

*Proof.* Without loss of generality, we may assume  $m \leq n$ . By Corollary 5, each  $\omega \in V_k$  admits a unique representation as a convex combination of pure product states, and each state in  $V_k$  has length  $k$ . We will show that  $V_k$  is open and dense in  $S_k$ .

To prove density, let  $\omega \in S_k$  have a convex decomposition  $\omega = \sum_{i=1}^k \lambda_i \omega_{x_i \otimes y_i}$ . By slightly perturbing the coefficients  $\lambda_i$  if necessary, we may assume that  $\lambda_i > 0$  for all  $i$ .

Given  $\epsilon > 0$ , by perturbing each  $x_i$  and  $y_i$  if necessary, we can find a second convex combination of pure product states  $\omega' = \sum_{i=1}^k \lambda_i \omega_{e_i \otimes f_i}$  with  $\|\omega - \omega'\| < \epsilon$ , with  $[e_1], \dots, [e_k]$  distinct, and with  $\{f_1, \dots, f_k\}$  independent. (Indeed, to achieve independence we may append unit vectors  $y_{k+1}, \dots, y_n$  to the vectors  $y_1, \dots, y_k$  to give the subset  $\{y_1, y_2, \dots, y_n\}$  of  $\mathbb{C}^n$ , and by small perturbations arrange that the determinant of the matrix with columns  $y_1, \dots, y_n$  is nonzero.) Thus  $V_k$  is dense in  $S_k$ . The norm intended above is the usual norm for linear functionals on  $M_n$ , called the base norm, cf. Ref. 2, but in finite dimensions all norms are equivalent, so density holds with respect to any norm.

Let  $I_0 = \{(\lambda_1, \lambda_2, \dots, \lambda_k) \in [0, 1]^k \mid \sum_i \lambda_i = 1\}$ . Let  $U_m$  be the unit sphere of  $\mathbb{C}^m$  and  $U_n$  the unit sphere of  $\mathbb{C}^n$ . Let  $X = I_0 \times (U_m)^k \times (U_n)^k$ . Define  $\psi : X \rightarrow S$  by

$$\psi((\lambda_1, \dots, \lambda_k), (x_1, \dots, x_k), (y_1, \dots, y_k)) = \sum_i \lambda_i \omega_{x_i \otimes y_i}.$$

Note that  $\psi$  is continuous, that  $X$  is compact with respect to the product topology, and that  $\psi(X) = S_k$ .

Now let  $X_0$  be the set  $\{((\lambda_1, \dots, \lambda_k), (x_1, \dots, x_k), (y_1, \dots, y_k))\}$  of members of  $X$  such that  $[x_1], \dots, [x_k]$  are distinct, such that  $\{y_1, \dots, y_k\}$  is linearly independent, and such that  $\lambda_i > 0$  for  $1 \leq i \leq k$ . By lower semicontinuity of the rank of a matrix whose columns are  $y_1, \dots, y_k$ , the set of elements  $((\lambda_1, \dots, \lambda_k), (x_1, \dots, x_m), (y_1, \dots, y_k))$  of  $X$  with  $\{y_1, \dots, y_k\}$  linearly independent is open in  $X$ , so it is clear that  $X_0$  is an open subset of  $X$ . By construction,  $\psi(X_0) = V_k$ . Since  $X_0$  is open in  $X$ , then  $X \setminus X_0$  is closed and hence compact. Since  $\psi$  maps  $X \setminus X_0$  onto  $S_k \setminus \psi(X_0)$ , then the latter is closed, so  $V_k = \psi(X_0)$  is open in  $S_k$ .  $\square$

As remarked in the introduction, the sets  $V_k$  are open and dense in the relative topology on  $S_k$ , but are not open or dense in  $S$  or  $K$  if  $mn > 1$ . To see this recall that a point  $\sigma$  in a convex set  $C$  is an algebraic interior point if for every point  $\rho$  in  $C$  there is a point  $\tau$  in  $C$  such that  $\sigma$  lies on the open line segment from  $\rho$  to  $\tau$ . Clearly for every algebraic interior point  $\sigma$  of  $S$  and every pure product state  $\rho$ , there is a convex decomposition of  $\sigma$  that includes  $\rho$  with positive weight. Since there are infinitely many pure product states, there are infinitely many convex decompositions for every algebraic interior point of  $S$ .

Every nonempty subset which is open in  $S$  contains an algebraic interior point of  $S$ , cf. pp. 88–91 of Ref. 27, so contains points with nonunique decompositions. Thus  $V_k$  is not open in  $S$  or  $K$ . It is not dense in  $S$  or  $K$ , since for any  $m, n$  there exists  $r > 0$  such that all states  $\sigma$  within a distance  $r$  from the normalized tracial state are separable, cf. Thm. 1 of Ref. 32. Every such state  $\sigma$  is an algebraic interior point of  $S$ , and so fails to have a unique decomposition.

Observe that Theorem 6 implies that  $V_k$  is also open and dense in the set of separable states of length equal to  $k$ .

#### IV. DESCRIPTION OF CONVEX DECOMPOSITIONS

Let  $e_1, e_2, \dots, e_p$  and  $f_1, f_2, \dots, f_p$  be unit vectors in  $\mathbb{C}^m$  and  $\mathbb{C}^n$  respectively, with  $f_1, \dots, f_p$  linearly independent. Suppose  $\omega$  is a convex combination of  $\{\omega_{e_i \otimes f_i} \mid 1 \leq i \leq p\}$ . In this section, we will describe all convex decompositions of  $\omega$  into pure product states.

Let  $\omega = \sum_i \lambda_i \omega_i$  be any convex decomposition of  $\omega$  into pure product states. Then following the notation of Theorem 4, each  $\omega_i$  is in  $\text{face}_S(\omega) \subset F$ . Since each  $\omega_i$  is an extreme point of  $S$ , and  $F$  is the direct convex sum of the faces  $F_i$ , then each  $\omega_i$  must be in some  $F_k$ . If we define  $\gamma_k = \sum_{\{i \mid \omega_i \in F_k\}} \lambda_i$  and  $\sigma_k = \gamma_k^{-1} \sum_{\{i \mid \omega_i \in F_k\}} \lambda_i \omega_i$ , then  $\omega$  has the convex decomposition

$$\omega = \sum_k \gamma_k \sigma_k \text{ with } \sigma_k \in F_k \text{ for each } k. \quad (6)$$

Since  $F$  is the direct convex sum of the  $F_k$ , the decomposition of  $\omega$  in (6) is unique.

All possible convex decompositions of  $\omega$  into pure product states can be found by starting with the unique decomposition  $\omega = \sum_k \gamma_k \sigma_k$  with  $\sigma_k \in F_k$ , and then decomposing each  $\sigma_k$  into pure states. (Every state in  $F_k$  is separable, so pure states are pure product states). Since  $F_k$  is affinely isomorphic to the state space of  $\mathcal{B}(L_k)$ , unless each  $\sigma_k$  is itself a pure state, this can be done in many ways, as we discussed in the introduction. The possibilities have been described in Refs. 10, 16, and 26.

A decomposition of a separable state  $\omega$  as a convex combination of pure product states can be interpreted as a representation of  $\omega$  as the barycenter of a probability measure on the extreme points of  $S$ . With this interpretation the statement above can be rephrased in terms of the concept of dilation of measures (as defined, e.g., on p. 25 of Ref. 1). If  $\omega$  is given as above, then the probability measures on pure product states that represent  $\omega$  are precisely those which are dilations of the uniquely determined probability measure  $\mu = \sum_k \gamma_k \mu_k$  obtained from (6) with  $\mu_k = \delta_{\sigma_k}$ .

## V. AFFINE AUTOMORPHISMS OF THE SPACE $S$ OF SEPARABLE STATES

*Notation.* Fix  $m, n$ . We denote the state space of  $\mathcal{B}(\mathbb{C}^m)$  by  $K_m$ , the state space of  $\mathcal{B}(\mathbb{C}^n)$  by  $K_n$ , and the state space of  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  by  $K$  or  $K_{m,n}$ . The convex set of separable states in  $K$  is denoted by  $S$  or  $S_{m,n}$ . We will sometimes deal with a second algebra  $\mathcal{B}(\mathbb{C}^{m'} \otimes \mathbb{C}^{n'})$ , whose state space and separable state spaces we will denote by  $K'$  or  $S'$  respectively.

From Theorem 4, the face of  $S$  generated by two distinct pure product states  $\omega_1 \otimes \sigma_1$  and  $\omega_2 \otimes \sigma_2$  is a line segment (if  $\omega_1 \neq \omega_2$  and  $\sigma_1 \neq \sigma_2$ ) or is isomorphic to the state space of  $\mathcal{B}(\mathbb{C}^2)$  and hence is a 3-ball (when  $\omega_1 = \omega_2$  but  $\sigma_1 \neq \sigma_2$ , or when  $\sigma_1 = \sigma_2$  but  $\omega_1 \neq \omega_2$ ). (By a 3-ball we mean a convex set affinely isomorphic to the closed unit ball of  $\mathbb{R}^3$ . The fact that the state space of  $\mathcal{B}(\mathbb{C}^2)$  is a 3-ball can be found in many places, e.g., Thm. 4.4 of Ref. 2.)

We define a relation  $R$  on the pure product states of  $K$  by  $\rho R \tau$  if  $\text{face}_S(\rho, \tau)$  is a 3-ball. By the remarks above,  $(\omega_1 \otimes \sigma_1) R (\omega_2 \otimes \sigma_2)$  iff  $(\omega_1 = \omega_2$  but  $\sigma_1 \neq \sigma_2)$  or  $(\sigma_1 = \sigma_2$  but  $\omega_1 \neq \omega_2)$ . Note that an affine isomorphism  $\Phi : S \rightarrow S'$  will take faces of  $S$  to faces of  $S'$ , and will take 3-balls to 3-balls, so for pure product states  $\rho, \tau$  we have  $\rho R \tau$  iff  $\Phi(\rho) R \Phi(\tau)$ .

The idea of the following lemmas is to show that if  $\Phi(\omega \otimes \sigma) = \phi(\omega, \sigma) \otimes \psi(\omega, \sigma)$ , then  $\phi$  depends only on the first argument and  $\psi$  depends only on the second argument, or possibly vice versa. Although we are interested in affine automorphisms of a single space of separable states, it will be easier to establish the needed lemmas in the context of affine isomorphisms from  $S$  to  $S'$ .

We use the notation  $\partial_e C$  for the set of extreme points of a convex set  $C$ . For example,  $\partial_e K$  is the set of pure states on  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$ .

**Lemma 7.** *Let  $\Phi : S_{m,n} \rightarrow S_{m',n'}$  be an affine isomorphism. Let  $\omega_1, \omega_2$  be distinct pure states in  $K_m$  and  $\sigma_1, \sigma_2$  distinct pure states in  $K_n$ . Then the following four equations cannot hold simultaneously.*

$$\begin{aligned} \Phi(\omega_1 \otimes \sigma_1) &= \rho_1 \otimes \tau_1 \\ \Phi(\omega_1 \otimes \sigma_2) &= \rho_1 \otimes \tau_2 \\ \Phi(\omega_2 \otimes \sigma_1) &= \rho_2 \otimes \tau_3 \\ \Phi(\omega_2 \otimes \sigma_2) &= \rho_3 \otimes \tau_3 \end{aligned} \tag{7}$$

for  $\rho_1, \rho_2, \rho_3 \in \partial_e K_{m'}$  and  $\tau_1, \tau_2, \tau_3 \in \partial_e K_{n'}$ .

*Proof.* We assume for contradiction that all four equations hold. Since  $(\omega_1 \otimes \sigma_1) R (\omega_2 \otimes \sigma_1)$ , then  $(\rho_1 \otimes \tau_1) R (\rho_2 \otimes \tau_3)$ . Hence

$$\rho_1 = \rho_2 \text{ or } \tau_1 = \tau_3. \tag{8}$$

Similarly  $(\omega_1 \otimes \sigma_2) R (\omega_2 \otimes \sigma_2)$ , so  $(\rho_1 \otimes \tau_2) R (\rho_3 \otimes \tau_3)$ . Hence

$$\rho_1 = \rho_3 \text{ or } \tau_2 = \tau_3. \tag{9}$$

Since we are assuming that  $\omega_1 \neq \omega_2$  and  $\sigma_1 \neq \sigma_2$ , the four states  $\{\omega_i \otimes \sigma_j \mid 1 \leq i, j \leq 2\}$  are distinct, so the four states on the right side of (7) must be distinct. Combining (8) and (9) gives four possibilities, each contradicting the fact that the states on the right side of (7) are distinct. Indeed:

$$\begin{aligned} (\rho_1 = \rho_2 \text{ and } \rho_1 = \rho_3) &\implies \rho_2 \otimes \tau_3 = \rho_3 \otimes \tau_3 \\ (\rho_1 = \rho_2 \text{ and } \tau_2 = \tau_3) &\implies \rho_1 \otimes \tau_2 = \rho_2 \otimes \tau_3 \\ (\tau_1 = \tau_3 \text{ and } \rho_1 = \rho_3) &\implies \rho_1 \otimes \tau_1 = \rho_3 \otimes \tau_3 \\ (\tau_1 = \tau_3 \text{ and } \tau_2 = \tau_3) &\implies \rho_1 \otimes \tau_1 = \rho_1 \otimes \tau_2. \end{aligned}$$

We conclude that the four equations in (7) cannot hold simultaneously.  $\square$

*Definition.* Recall that we identify  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  with  $\mathcal{B}(\mathbb{C}^m) \otimes \mathcal{B}(\mathbb{C}^n)$ . The *swap isomorphism*  $(\alpha_{m,n})_* : \mathcal{B}(\mathbb{C}^n \otimes \mathbb{C}^m) \rightarrow \mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  is the \*-isomorphism that satisfies  $(\alpha_{m,n})_*(A \otimes B) = B \otimes A$ . If operators in  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  are identified with matrices, the swap isomorphism is the same as the ‘‘canonical shuffle’’ discussed in Chapter 8 of Ref. 21. The dual map  $\alpha_{m,n}$  is an affine isomorphism from the state space of  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  to the state space of  $\mathcal{B}(\mathbb{C}^n \otimes \mathbb{C}^m)$ , with  $\alpha_{m,n}(\omega \otimes \sigma) = \sigma \otimes \omega$ . This restricts to an affine isomorphism from  $S_{m,n}$  to  $S_{n,m}$ , which we also refer to as the swap isomorphism. If  $m = n$ , then  $(\alpha_{m,m})_*$  is a \*-automorphism of  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^m)$ ,  $\alpha_{m,m}$  is an affine automorphism of the state space  $K$ , and restricts to an affine automorphism of the space  $S$  of separable states.

**Lemma 8.** *Let  $\Phi : S_{m,n} \rightarrow S_{m',n'}$  be an affine isomorphism. At least one of the following two possibilities occurs:*

- (i) *For every  $\omega \in \partial_e K_m$  there exists  $\rho \in \partial_e K_{m'}$  such that  $\Phi(\omega \otimes K_n) = \rho \otimes K_{n'}$ , and for every  $\sigma \in \partial_e K_n$  there exists  $\tau \in \partial_e K_{n'}$  such that  $\Phi(K_m \otimes \sigma) = K_{m'} \otimes \tau$ .*
- (ii) *For each  $\omega \in \partial_e K_m$  there exists  $\tau \in \partial_e K_{n'}$  such that  $\Phi(\omega \otimes K_n) = K_{m'} \otimes \tau$ , and for every  $\sigma \in \partial_e K_n$  there exists  $\rho \in \partial_e K_{m'}$  such that  $\Phi(K_m \otimes \sigma) = \rho \otimes K_{n'}$ .*

If (i) occurs, then  $m = m'$  and  $n = n'$ . If (ii) occurs, then  $m = n'$  and  $n = m'$ .

*Proof.* For fixed  $\omega \in \partial_e K_m$  and distinct  $\sigma_1, \sigma_2 \in \partial_e K_n$  we have  $(\omega \otimes \sigma_1) \text{ R } (\omega \otimes \sigma_2)$ , so  $\Phi(\omega \otimes \sigma_1) \text{ R } \Phi(\omega \otimes \sigma_2)$ . Thus either there exist  $\rho_1 \in \partial_e K_{m'}$  and distinct  $\tau_1, \tau_2 \in \partial_e K_{n'}$  such that

$$\Phi(\omega \otimes \sigma_i) = \rho_1 \otimes \tau_i \text{ for } i = 1, 2, \quad (10)$$

or there exist distinct  $\rho_1, \rho_2 \in \partial_e K_{m'}$  and  $\tau_3 \in \partial_e K_{n'}$  such that

$$\Phi(\omega \otimes \sigma_i) = \rho_i \otimes \tau_3 \text{ for } i = 1, 2. \quad (11)$$

We will show that (10) implies (i), and (11) implies (ii).

Suppose that (10) holds. Let  $\sigma \in \partial_e K_n$  with  $\sigma \neq \sigma_1$  and  $\sigma \neq \sigma_2$ , and let  $\Phi(\omega \otimes \sigma) = \rho \otimes \tau$ . Since  $(\omega \otimes \sigma) \text{ R } (\omega \otimes \sigma_i)$  for  $i = 1, 2$ , then  $(\rho \otimes \tau) \text{ R } (\rho_1 \otimes \tau_i)$  for  $i = 1, 2$ . Hence  $(\rho = \rho_1 \text{ or } \tau = \tau_1)$  and  $(\rho = \rho_1 \text{ or } \tau = \tau_2)$ . Since  $\tau_1 \neq \tau_2$ , then  $\rho = \rho_1$ . It follows that  $\Phi(\omega \otimes K_n) \subset \rho_1 \otimes K_{n'}$ . Thus

$$\Phi(\omega \otimes \sigma_i) = \rho_1 \otimes \tau_i \text{ for } i = 1, 2 \implies \Phi(\omega \otimes K_n) \subset \rho_1 \otimes K_{n'}. \quad (12)$$

Now (10) also implies

$$\Phi^{-1}(\rho_1 \otimes \tau_i) = \omega \otimes \sigma_i \text{ for } i = 1, 2. \quad (13)$$

If (10) holds (and hence also (13)), then applying the implication (12) to (13) with  $\Phi^{-1}$  in place of  $\Phi$  shows  $\Phi^{-1}(\rho_1 \otimes K_{n'}) \subset \omega \otimes K_n$ , so by (12) equality holds. Hence we have shown

$$\Phi(\omega \otimes \sigma_i) = \rho_1 \otimes \tau_i \text{ for } i = 1, 2 \implies \Phi(\omega \otimes K_n) = \rho_1 \otimes K_{n'}. \quad (14)$$

Now suppose instead that (11) holds. Let  $\alpha_{m',n'}$  be the swap affine isomorphism defined above, so that  $\alpha_{m',n'} : S_{m',n'} \rightarrow S_{n',m'}$ . Then

$$(\alpha_{m',n'} \circ \Phi)(\omega \otimes \sigma_i) = \alpha_{m',n'}(\rho_i \otimes \tau_3) = \tau_3 \otimes \rho_i \text{ for } i = 1, 2. \quad (15)$$

By the implication (14) applied to  $\alpha_{m',n'} \circ \Phi$  we conclude that

$$(\alpha_{m',n'} \circ \Phi)(\omega \otimes K_n) = \tau_3 \otimes K_{m'},$$

so

$$\Phi(\omega \otimes K_n) = \alpha_{m',n'}^{-1}(\tau_3 \otimes K_{m'}) = K_{m'} \otimes \tau_3.$$

Thus we have proven the implication

$$\Phi(\omega \otimes \sigma_i) = \rho_i \otimes \tau_3 \text{ for } i = 1, 2 \implies \Phi(\omega \otimes K_n) = K_{m'} \otimes \tau_3. \quad (16)$$

By Lemma 7 and the implications (14) and (16), either (10) must hold for all  $\omega \in \partial_e K_m$  or (11) must hold for all  $\omega \in \partial_e K_m$ . We conclude that either

$$\forall \omega \in \partial_e K_m \quad \exists \rho \in \partial_e K_{m'} \text{ such that } \Phi(\omega \otimes K_n) = \rho \otimes K_{n'} \quad (17)$$

or

$$\forall \omega \in \partial_e K_m \quad \exists \tau \in \partial_e K_{n'} \text{ such that } \Phi(\omega \otimes K_n) = K_{m'} \otimes \tau. \quad (18)$$

Similarly, either

$$\forall \sigma \in \partial_e K_n \quad \exists \tau' \in \partial_e K_{n'} \text{ such that } \Phi(K_m \otimes \sigma) = K_{m'} \otimes \tau' \quad (19)$$

or

$$\forall \sigma \in \partial_e K_n \quad \exists \rho' \in \partial_e K_{m'} \text{ such that } \Phi(K_m \otimes \sigma) = \rho' \otimes K_{n'}. \quad (20)$$

Suppose that (17) and (20) both held. For  $\omega \in K_m$  and  $\sigma \in K_n$  note that  $\omega \otimes \sigma$  is in both  $\omega \otimes K_n$  and  $K_m \otimes \sigma$ , so  $\rho \otimes K_{n'}$  and  $\rho' \otimes K_{n'}$  are not disjoint. This implies  $\rho = \rho'$ , so  $\Phi(\omega \otimes K_n) = \Phi(K_m \otimes \sigma)$ . Since  $\Phi$  is bijective,  $\omega \otimes K_n = K_m \otimes \sigma$  follows. This is possible only if  $m = n = 1$ . If  $m = n = 1$ , then all of (17), (18), (19), (20) hold. Similarly if (18) and (19) both held then  $m = n = 1$  is again forced. Thus the possibilities are that (17) and (19) both hold (which is the same as statement (i) of the lemma), or that (18) and (20) hold (equivalent to (ii)), or that  $m = n = 1$ , in which case both (i) and (ii) hold.

Finally, since the affine dimensions of  $K_p$  and  $K_q$  are different when  $p \neq q$ , the statement in the last sentence of the lemma follows.  $\square$

If  $\psi_1 : K_m \rightarrow K_m$  and  $\psi_2 : K_n \rightarrow K_n$  are affine automorphisms, then we can extend each to linear maps on the linear span, and form the tensor product  $\psi_1 \otimes \psi_2$ . This will be bijective, but not necessarily positive. (A well known example of this phenomenon occurs when  $\psi_1$  is the identity map and  $\psi_2$  is the transpose map.) However,  $\psi_1$  and  $\psi_2$  will map pure states to pure states, and hence  $\psi_1 \otimes \psi_2$  will map pure product states to pure product states. Thus  $\psi_1 \otimes \psi_2$  will map  $S$  onto  $S$ , and hence will be an affine automorphism of  $S$ . We will now see that all affine automorphisms of  $S$  are either such a tensor product of automorphisms or such a tensor product composed with the swap automorphism.

**Theorem 9.** *If  $m \neq n$ , and  $\Phi : S \rightarrow S$  is an affine automorphism, then there exist unique affine automorphisms  $\psi_1 : K_m \rightarrow K_m$  and  $\psi_2 : K_n \rightarrow K_n$  such that  $\Phi = \psi_1 \otimes \psi_2$ . If  $m = n$  then either we can write  $\Phi = (\psi_1 \otimes \psi_2)$  or  $\Phi = \alpha_{m,m} \circ (\psi_1 \otimes \psi_2)$ , where  $\psi_1, \psi_2$  are again unique affine automorphisms of  $K_m$  and  $K_n$  respectively, and  $\alpha_{m,m} : S \rightarrow S$  is the swap automorphism.*

*Proof.* We apply Lemma 8. For each  $\omega \in \partial_e K_m$  and  $\sigma \in \partial_e K_n$ , define  $\phi_\sigma : K_m \rightarrow K_m$  and  $\psi_\omega : K_n \rightarrow K_n$  by

$$\Phi(\omega \otimes \sigma) = \phi_\sigma(\omega) \otimes \psi_\omega(\sigma).$$

Suppose first that case (i) of Lemma 8 occurs. Then  $\psi_\sigma(\omega)$  is independent of  $\sigma$  and  $\psi_\omega(\sigma)$  is independent of  $\omega$ . Therefore there are functions  $\psi_1 : K_m \rightarrow K_m$  and  $\psi_2 : K_n \rightarrow K_n$  such that

$$\Phi(\omega \otimes \sigma) = \psi_1(\omega) \otimes \psi_2(\sigma).$$

Since  $\Phi$  is bijective and affine, so are  $\psi_1$  and  $\psi_2$ .

Suppose instead that case (ii) of Lemma 8 occurs. Then  $m = n$ . If we define  $\Phi' = \alpha_{m,m} \circ \Phi$ , then  $\Phi' : S \rightarrow S$  satisfies case (i) of Lemma 8. Then from the first paragraph we can choose affine automorphisms  $\psi_1 : K_m \rightarrow K_m$  and  $\psi_2 : K_n \rightarrow K_n$  such that  $\Phi' = \psi_1 \otimes \psi_2$ . Since  $\alpha_{m,m}^2$  is the identity map, then  $\Phi = \alpha_{m,m} \circ (\psi_1 \otimes \psi_2)$ .  $\square$

We review some well known facts about affine automorphisms of state spaces and maps on the underlying algebra. Let  $\psi$  be an affine automorphism of  $K_m$ . Then  $\psi$  extends uniquely to a linear map on the linear span of  $K_m$ , which we also denote by  $\psi$ , and this map is the dual of a unique linear map  $\psi_*$  on  $\mathcal{B}(\mathbb{C}^m)$ . By a result of Kadison<sup>12</sup>  $\psi_*$  will be a \*-isomorphism or a \*-anti-isomorphism. (Since the restriction of an affine automorphism to pure states preserves transition probabilities, this also follows from Wigner's theorem<sup>31</sup>). The map  $\psi_*$  will be a \*-isomorphism iff  $\psi_*$  is completely positive, which is equivalent to  $\psi$  being completely positive. If  $\psi_*$  is a \*-isomorphism, then  $\psi_*$  is implemented by a unitary, i.e., there is a unitary  $U \in \mathcal{B}(\mathbb{C}^m)$  such that  $\psi_*(A) = UAU^*$ .

If  $\psi_*$  is a \*-anti-isomorphism, then the composition of  $\psi_*$  with the transpose map (in either order) gives a \*-isomorphism, and the map  $\psi_*$  is completely copositive. It follows that an affine automorphism  $\psi$  of  $K_m$  is either completely positive or completely copositive, and  $\psi$  is completely positive iff  $\psi^{-1}$  is completely positive. If  $t$  denotes the transpose map on  $\mathcal{B}(\mathbb{C}^m)$  or  $\mathcal{B}(\mathbb{C}^n)$ , then  $t$  is positive but  $t \otimes id$  and  $id \otimes t$  are not positive on  $\mathcal{B}(\mathbb{C}^m) \otimes \mathcal{B}(\mathbb{C}^n)$  if  $m, n > 1$ . Background can be found in Chapters 4 and 5 of Ref. 2.

Recall that a *local unitary* in  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  is a tensor product  $U_1 \otimes U_2$  of unitaries.

**Theorem 10.** *Every affine automorphism of the space  $S$  of separable states on  $\mathcal{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$  is the dual of conjugation by local unitaries, one of the two partial transpose maps, the swap map (if  $m = n$ ), or a composition of these maps. An affine automorphism  $\Phi$  of  $S$  extends uniquely to an affine automorphism of the full state space  $K$  iff it can be expressed as one of the compositions just mentioned with both or neither of the partial transpose maps involved.*

*Proof.* We note first that if  $m = 1$  or  $n = 1$ , the result is clear, so we assume hereafter that  $m \geq 2$  and  $n \geq 2$ .

We next show that if  $\psi_1 : K_m \rightarrow K_m$  and  $\psi_2 : K_n \rightarrow K_n$  are affine automorphisms, then  $\Phi = \psi_1 \otimes \psi_2$  is an affine automorphism of  $K$  iff  $\psi_1$  and  $\psi_2$  are both completely positive or both completely copositive.

If  $\psi_1$  and  $\psi_2$  are completely positive, then  $\Phi = \psi_1 \otimes \psi_2 = (id \otimes \psi_2) \circ (\psi_1 \otimes id)$  is positive; hence  $\Phi(K) \subset K$ . Furthermore,  $\psi_1^{-1}$  and  $\psi_2^{-1}$  will be completely positive, so  $\Phi^{-1}$  is positive, and hence  $\Phi(K) = K$ . If  $\psi_1$  and  $\psi_2$  are completely copositive, then  $(t \circ \psi_1) \otimes (t \circ \psi_2)$  is positive. Composing with  $t \otimes t$  shows  $\psi_1 \otimes \psi_2$  is positive and as above we conclude that  $\Phi(K) = K$ . On the other hand, if  $\psi_1$  is completely positive and  $\psi_2$  is completely copositive, then  $\psi_1 \otimes (t \circ \psi_2)$  is positive, so  $(id \otimes t) \circ (\psi_1 \otimes \psi_2)$  is positive. If  $(\psi_1 \otimes \psi_2)(K) = K$ , then  $id \otimes t$  would be positive, a contradiction since  $m, n \geq 2$ . Thus in this case  $\psi_1 \otimes \psi_2$  is not an affine automorphism of  $K$ .

If  $\psi_1$  and  $\psi_2$  are completely positive, then they are implemented by unitaries, so  $\Phi = \psi_1 \otimes \psi_2$  is implemented by a local unitary. If both are completely copositive, then  $t \circ \psi_1$  and  $t \circ \psi_2$  are implemented by unitaries, so  $(t \otimes t) \circ (\psi_1 \otimes \psi_2)$  is implemented by a local unitary. Then  $\Phi = (t \otimes t) \circ (t \otimes t) \circ (\psi_1 \otimes \psi_2)$  is the composition of the transpose map on  $K$  and conjugation by local unitaries.

The first statement of the theorem now follows from Theorem 9. Uniqueness follows from the fact that the linear span of  $S$  contains  $K$ .  $\square$

*Definition.* Let  $\Phi : K \rightarrow K$  be an affine automorphism. We say  $\Phi$  *preserves separability* if  $\Phi$  takes separable states to separable states, i.e., if  $\Phi(S) \subset S$ . A state  $\omega$  in  $K$  is *entangled* if  $\omega$  is not separable.  $\Phi$  *preserves entanglement* if  $\Phi$  takes entangled states to entangled states.

**Corollary 11.** *Let  $\Phi : K_{m,n} \rightarrow K_{m,n}$  be an affine automorphism. Then  $\Phi$  preserves entanglement and separability iff  $\Phi$  is a composition of maps of the types (i) conjugation by local unitaries, (ii) the transpose map, (iii) the swap automorphism (in the case that  $m = n$ ).*

*Proof.* If  $\Phi$  preserves entanglement and separability, then  $\Phi$  maps  $S$  into  $S$  and  $K \setminus S$  into  $K \setminus S$ , which is equivalent to  $\Phi(S) = S$ .  $\square$

**Corollary 12.** *If  $\Phi_t : S \rightarrow S$  is a one-parameter group of affine automorphisms, then there are one-parameter groups of unitaries  $U_t$  and  $V_t$  such that  $(\Phi_t \omega)(A) = \omega((U_t \otimes V_t)A(U_t^* \otimes V_t^*))$ .*

*Proof.* For each  $t$ , factor  $\Phi_t = \phi_t \otimes \psi_t$  or  $\Phi_t = \alpha \circ (\phi_t \otimes \psi_t)$ , where  $\alpha$  is the swap automorphism. In the latter case,

$$\begin{aligned} \Phi_{2t} &= \Phi_t \circ \Phi_t = \alpha \circ (\phi_t \otimes \psi_t) \circ \alpha \circ (\phi_t \otimes \psi_t) \\ &= (\phi_t \otimes \psi_t) \circ (\phi_t \otimes \psi_t) = (\phi_t \circ \phi_t) \otimes (\psi_t \circ \psi_t). \end{aligned}$$

It follows that the swap automorphism is not needed for  $\Phi_{2t}$ , and hence for  $\Phi_t$  for any  $t$ . Uniqueness of the factorization  $\Phi_t = \phi_t \otimes \psi_t$  shows that  $\phi_t$  and  $\psi_t$  are also one parameter groups of affine automorphisms. By a result



of Kadison<sup>13</sup>, such automorphisms are implemented by one parameter groups of unitaries.  $\square$

**Corollary 13.** *If  $\Phi_t : K \rightarrow K$  is a one-parameter group of entanglement preserving affine automorphisms, then there are one-parameter groups of unitaries  $U_t$  and  $V_t$  such that  $(\Phi_t \omega)(A) = \omega((U_t \otimes V_t)A(U_t^* \otimes V_t^*))$ .*

*Proof.* Since  $\Phi_t$  and  $(\Phi_t)^{-1} = \Phi_{-t}$  preserve entanglement, then  $\Phi_t$  maps  $S$  onto  $S$ , so this corollary follows from Corollary 12.  $\square$

## ACKNOWLEDGMENTS

We thank Mary Beth Ruskai and the referees for helpful comments and references.

- <sup>1</sup>E. M. Alfsen, *Compact convex sets and boundary integrals*, Ergebnisse der Mathematik und ihrer Grenzgebiete **57**, Springer-Verlag, New York, Heidelberg, 1971.
- <sup>2</sup>E. Alfsen and F. Shultz, *State spaces of operator algebras: basic theory, orientations, and  $C^*$ -products*, Mathematics: Theory & Applications, Birkhäuser Boston, 2001.
- <sup>3</sup>G. Aubrun, S. J. Szarek, Tensor products of convex sets and the volume of separable states on  $N$  qudits, *Phys. Rev. A* **73** 022109 (2006) (arXiv:quant-ph/0503221)
- <sup>4</sup>C. Bennett, D. DiVincenzo, T. Mor, P. Shor, J. Smolin, and B. Terhal, Unextendible Product Bases and Bound Entanglement, *Phys. Rev. Letters* **82** (1999) 5385–5388.
- <sup>5</sup>D. P. DiVincenzo, B. M. Terhal, and A. V. Thapliyal, Optimal Decompositions of Barely Separable States, *Journal of Modern Optics* **47** (2000) No. 213, 277–385.
- <sup>6</sup>M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: necessary and sufficient conditions, *Physics Letters A* **223** (1996) 1–8.
- <sup>7</sup>M. Horodecki, R. Horodecki, Information-theoretic aspects of quantum inseparability of mixed states, *Phys. Rev. A* **54**, 1838–1843 (1996) (arXiv:quant-ph/9607007v1)
- <sup>8</sup>P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, *Physics Letters A* **232** (1997) 333–339.
- <sup>9</sup>P. Horodecki, M. Lewenstein, G. Vidal, I. Cirac, Operational criterion and constructive checks for the separability of low-rank density matrices, *Phys. Rev. A* **62** (2000) 032310.
- <sup>10</sup>L. Hughston, R. Jozsa, W. Wootters, A complete classification of quantum ensembles having a given density matrix, *Physics Letters A* **183** (1993) 14–18.
- <sup>11</sup>F. Hulpke, U. V. Poulsen, A. Sanpera, A. Sen(de), U. Sen, and M. Lewenstein, Unitarity as preservation of entropy and entanglement in quantum systems, *Foundations of Physics* **36** 2006, 477–499.
- <sup>12</sup>R. V. Kadison, Isometries of operator algebras, *Ann. Math.* **54** (1951) 325–338.
- <sup>13</sup>R. V. Kadison, Transformations of states in operator theory and dynamics. *Topology* **3** (1965), suppl. 2, 177–198
- <sup>14</sup>S. Karnas and M. Lewenstein, Separability and entanglement in  $C^2 \otimes C^2 \otimes C^N$  composite quantum systems, *Phys. Rev. A* **64** (2001) 042313.
- <sup>15</sup>C. King and M. B. Ruskai, Minimal entropy of states emerging from noisy quantum channels, *IEEE Trans. Inf. Theory* **47** 192 (2001), (arXiv:quant-ph/11079).
- <sup>16</sup>K. A. Kirkpatrick, The Schrödinger-HJW Theorem, *Foundations of Physics Letters* **19** 2006, 95–102.
- <sup>17</sup>B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, Separability in  $2 \times N$  composite quantum systems, *Phys. Rev. A* **61** (2000) 062302.
- <sup>18</sup>M. Lewenstein and A. Sanpera, Separability and entanglement of composite quantum systems, *Phys. Rev. Letters* **80** (1998) 2261–2264.
- <sup>19</sup>R. B. Lockhart, Optimal ensemble length of mixed separable states, *J. Math. Phys.* **41**, 6766 (2000), (arXiv:quant-ph/9908050)
- <sup>20</sup>J.M. Leinaas, J. Myrheim, E. Ovrum, Geometrical aspects of entanglement, *Phys. Rev. A* **74** (2006) 012313, 13pp.
- <sup>21</sup>V. Paulsen, *Completely bounded maps and operator algebras*, Cambridge Studies in Advanced Mathematics **78**, Cambridge University Press, 2002.
- <sup>22</sup>A. Peres, Separability criterion for density matrices, *Phys. Rev. Lett.* **77** (1996) 1413–1415.
- <sup>23</sup>M. B. Ruskai, Qubit entanglement breaking channels, *Rev. Math. Phys.* **15** (2003), no. 6, 15–42 (arXiv:quant-ph/0302032).
- <sup>24</sup>M. B. Ruskai and E. Werner, Bipartite states of low rank are almost surely entangled, *J. Phys. A* **42** 095303 (2009).
- <sup>25</sup>A. Sanpera, R. Tarrach, G. Vidal, Local description of quantum inseparability, *Phys. Rev. A*, **58** (1998) 826–830.
- <sup>26</sup>E. Schrödinger, Probability relations between separated systems, *Proc. Camb. Phil. Soc.* **32** (1936) 446–452.
- <sup>27</sup>J. Stoer, C. Witzgall, *Convexity and Optimization in Finite Dimensions I*, Springer-Verlag, New York, 1970.
- <sup>28</sup>S. Szarek, The volume of separable states is super-doubly-exponentially small, *Phys. Rev. A* **72** (2005) 32304 (arXiv:quant-ph/0310061).
- <sup>29</sup>A. M. Vershik. Geometrical theory of states, the von Neumann boundary, and duality of  $C^*$ -algebras. *Zapiski Nauchn. Semin. POMI*, **29** (1972), 147–154. English translation: *J. Sov. Math.*, **3** (1975), 840–845.
- <sup>30</sup>J. Walgate and A. J. Scott, Generic local distinguishability and completely entangled subspaces, *J. Phys. A: Math. Theor.* **41** 375305 (2008) (arXiv:0709.4238)
- <sup>31</sup>E. P. Wigner, Gruppentheorie und ihre Anwendung, Braunschweig: Vieweg 1931. English translation by J.J. Griffin, Group Theory, Academic Press, New York, 1959.
- <sup>32</sup>K. Życzkowski, P. Horodecki, A. Sanpera, M. Lewenstein, Volume of the set of separable states. *Phys. Rev. A* (3) **58** (1998), no. 2, 883–892.