Preservers of Maximally Entangled States

Edward Poon
Department of Mathematics
Embry-Riddle Aeronautical University
Prescott, AZ, USA 86301
edward.poon@erau.edu

July 29, 2013

Abstract

The linear structure of the real space spanned by maximally entangled states is investigated, and used to completely characterize those linear maps preserving the set of maximally entangled states on $M_m \otimes M_m$, where M_m denotes the space of $m \times m$ complex matrices. Aside from a degenerate rank one map, such preservers are generated by a change of orthonormal basis in each tensor factor, interchanging the two tensor factors, and the transpose operator.

2000 Mathematics Subject Classification. 15A86, 15B57, 46N50.
Keywords. Maximally entangled state, linear preserver, quantum state, density matrix.

1 Introduction and Notation

Let $M_{n,m}$ be the space of $n \times m$ complex matrices, and let $M_n = M_{n,n}$. H_n will denote the real space of $n \times n$ (complex) Hermitian matrices. On a finite-dimensional Hilbert space $\mathcal{H}$ of dimension n, a quantum state ρ is simply a density matrix in H_n (that is, ρ is a positive semi-definite $n \times n$ matrix of trace one). A state ρ is said to be *pure* if it has rank one (in other words, ρ is a rank one (orthogonal) projection).

In quantum information theory, one of the most important concepts is that of entanglement, which occurs when dealing with a multipartite system. We shall restrict our attention to a bipartite system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are Hilbert spaces of dimension m and n respectively. In this case, a state ρ is said to be *separable* if one can write $\rho = \sum_{i=1}^{r} p_i \rho_i \otimes \sigma_i$ for some states $\rho_i \in H_m$, $\sigma_i \in H_n$, and positive scalars p_i summing to one. Otherwise we say the state is *entangled*.

Entanglement is considered a valuable resource, responsible for the power of quantum computing (see [8] for a standard reference) and for applications such as superdense coding (see [3]) and quantum teleportation (see [2]). There are various ways to measure how much entanglement a state has; those states possessing maximal entanglement are of particular importance, and a natural question is: what types of state transformations will preserve maximal entanglement, that is, will map the maximally entangled states back to themselves? Answering this question is the main result of this paper.

Questions of this type have a long history, and fall under the broader purview of linear preserver problems (two useful surveys are [5, 6]). Recently there has been work done on finding and classifying linear preservers of various properties or sets related to quantum information theory. One paper of particular relevance is [4], in which the authors classify linear preservers of separable states (a related paper is [7]). However, they work under the more restrictive assumption that the linear map is surjective, an assumption we shall not require.

This paper shall be organized as follows. Section 1 will conclude by introducing some notation. Section 2 will define what a maximally entangled state is, and investigate the real linear span of such states. Section 3 will prepare for the final section by stating and proving a number of technical lemmas. Finally, section 4 will contain the statement and proof of our main theorem, where we completely characterize the linear maps preserving maximally entangled states on $M_m \otimes M_m$.

We close this section by fixing some additional notation.

We write I_m and 0_m for the $m \times m$ identity and zero matrices, respectively (omitting the subscript if the size is clear from the context). We let e_i denote the (column) vector whose only nonzero entry is a 1 in the ith position (we do not specify the length of e_i in advance, leaving that to be determined by context), and let $E_{ij} = e_i e_j^*$. The group of $n \times n$ unitary matrices is denoted by U_n.

We shall abbreviate maximally entangled state(s) by MES, and will abuse notation by allowing MES to be both singular and plural, depending on the context (for example, we might say a state ρ is a MES, or we might refer to the set of all maximally entangled states as MES). The convex hull of MES is co(MES); the (real) linear span of MES is Span(MES). Given a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$, with $\dim \mathcal{H}_A = m$ and $\dim \mathcal{H}_B = n$, the partial trace over system B is the linear map $\mathrm{Tr}_B : M_m \otimes M_n \to M_m$ defined by $\mathrm{Tr}_B(A \otimes B) = (\mathrm{Tr}\, B)A$, where $A \in M_m$, $B \in M_n$, and Tr is the usual trace. The partial trace over the first system, Tr_A, is defined similarly.

2 Structure of Maximally Entangled States

Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite system, where the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ have dimension m and n respectively, with $m \leq n$. A pure state ρ on $\mathcal{H}$ is a *maximally entangled state* (or *MES* for short) if $\rho = \psi\psi^*$ where $\psi = \frac{1}{\sqrt{m}} \sum_{i=1}^m u_i \otimes v_i$ for some orthonormal basis $\{u_i\}$ of $\mathcal{H}_A$ and some orthonormal set $\{v_i\}$ of $\mathcal{H}_B$. Let $\psi_0 = \frac{1}{\sqrt{m}} \sum_{i=1}^m e_i \otimes e_i$. Then clearly

$$\mathrm{MES} = \{\psi\psi^* : \psi = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} (Ue_i \otimes Ve_i) \text{ where } U \in M_m \text{ is unitary}, V \in M_n \text{ is unitary}\}$$

is the similarity orbit of $\psi_0\psi_0^*$ under the action of the unitary subgroup $U_m \otimes U_n$, and hence is a compact, connected set of rank 1 projections.

Note that if ρ is a MES, then $\mathrm{Tr}_B\, \rho = \frac{1}{m} I_m$ and $\mathrm{Tr}_A\, \rho$ is $\frac{1}{m}$ times a rank m projection in M_n. In fact, this essentially characterizes the real linear span of MES. Let

$$\mathcal{S}_{m,n} = \{X \in H_m \otimes H_n : \mathrm{Tr}_B\, X = 0\}$$

and

$$\mathcal{S}_m = \{A \in H_m \otimes H_m : \mathrm{Tr}_B\, X = \mathrm{Tr}_A\, X = 0\}.$$

Note that these are real vector spaces of dimension $m^2(n^2 - 1)$ and $(m^2 - 1)^2$ respectively.

Proposition 2.1. *The real linear span of MES, denoted by Span(MES), is* $\mathbb{R}I_{mn} + \mathcal{S}_{m,n}$ *if* $m < n$, *or* $\mathbb{R}I_{m^2} + \mathcal{S}_m$ *if* $m = n$.

Proof. Note that if ρ is a MES, then $\rho - \frac{1}{mn} I_m \otimes I_n$ lies in $S_{m,n}$ or S_m according to whether $m < n$ or $m = n$. So it suffices to show that $I_m \otimes I_n$ and $S_{m,n}$ (or S_m if $m = n$) lie in Span(MES). We shall repeatedly use the fact that MES, and hence Span(MES), is invariant under conjugation by $U \otimes V \in U_m \otimes U_n$.

If $W_k = -2E_{kk} + \sum_{i=1}^m E_{ii}$, then

$$X = \psi_0\psi_0^* - (W_1 \otimes I_n)\psi_0\psi_0^*(W_1^* \otimes I_n) = \frac{2}{m}\left(\sum_{j\neq 1} e_1e_j^* \otimes e_1e_j^* + \sum_{i\neq 1} e_ie_1^* \otimes e_ie_1^*\right)$$

lies in Span(MES), and hence so does

$$Y = \frac{m}{4}[X - (W_2 \otimes I_n)X(W_2^* \otimes I_n)] = E_{12} \otimes E_{12} + E_{21} \otimes E_{21}.$$

Conjugating by $I_m \otimes V$ for arbitrary unitary $V \in U_n$ shows that $E_{12} \otimes A + E_{21} \otimes A^*$ is in Span(MES) for any rank one nilpotent A of norm one. By linearity, $E_{12} \otimes A + E_{21} \otimes A^*$ is in Span(MES) for all $A \in M_n$ with trace zero. Conjugating by $U \otimes I_n$ for arbitrary permutations $U \in U_m$ shows that $E_{ij} \otimes A + E_{ji} \otimes A^*$ is in Span(MES) for all indices $i \neq j$, and all $A \in M_n$ with trace zero.

Then

$$Z = \sum_{i=1}^m E_{ii} \otimes E_{ii} = m\left(\psi_0\psi_0^* - \sum_{i\neq j} E_{ij} \otimes E_{ij}\right)$$

lies in Span(MES), and hence so does

$$\sum_{j=1}^m (Q^j \otimes I_n)Z(Q^{-j} \otimes I_n) = I_m \otimes \sum_{i=1}^m E_{ii}$$

where $Q \in U_m$ is a cyclic permutation on m symbols. Thus $I_m \otimes I_m$ lies in Span(MES) if $m = n$. If $m < n$, let V be the permutation mapping e_i to e_{i+1} for $i < n$, and mapping e_n to e_1. Then $\frac{1}{m}\sum_{j=1}^n (I_m \otimes V^j)(I_m \otimes \sum_{i=1}^m E_{ii})(I_m \otimes V^{-j}) = I_m \otimes I_n$ lies in Span(MES).

If $m < n$ let $Q_k \in U_n$ be the transposition swapping e_k and e_n while leaving all other e_i fixed. Then $Z - (I_m \otimes Q_k)Z(I_m \otimes Q_k^*) = E_{kk} \otimes (E_{kk} - E_{nn})$ lies in Span(MES) for all k. Conjugating by $I_m \otimes V$ for arbitrary $V \in U_n$ and using linearity shows that $E_{kk} \otimes B \in$ Span(MES) for all $k = 1, \dots, m$ and all $B \in H_n$ with trace zero. Thus $\mathcal{S}_{m,n}$ lies in Span(MES) as desired.

If $m = n$ then

$$Z - (I_m \otimes Q_k)Z(I_m \otimes Q_k^*) = E_{kk} \otimes (E_{kk} - E_{mm}) + E_{mm} \otimes (E_{mm} - E_{kk})$$

lies in Span(MES) for all $k = 1, \dots, m-1$. Conjugating by $I_m \otimes V$ for arbitrary $V \in U_m$ and using linearity shows that $E_{kk} \otimes B + E_{mm} \otimes (-B) \in$ Span(MES) for all $k = 1, \dots, m-1$ and all $B \in H_m$ with trace zero. By linearity,

$$\sum_{i=1}^{m-1} E_{ii} \otimes B_i + E_{mm} \otimes \left(-\sum_{i=1}^{m-1} B_i\right)$$

lies in Span(MES) for any $B_1, \dots, B_{m-1} \in H_m$ with trace zero. Thus $\mathcal{S}_m$ lies in Span(MES) as desired. □

In general, the real linear span of an arbitrary set of projections contains additional projections not in the original set. This is not the case for MES.

Remark 2.2. *The set of pure states in the real linear span of MES is precisely MES.*

Proof. Suppose $\psi\psi^*$ is a pure state in Span(MES). By the preceding proposition, $\mathrm{Tr}\,_B\psi\psi^* = \frac{1}{m}I_m$. Using the Schmidt decomposition for ψ shows that $\psi\psi^* \in$ MES as desired. □

Definition 2.3. *Let*

$$\psi_0 = \frac{1}{\sqrt{m}}\sum_{i=1}^m e_i \otimes e_i, \quad \rho_0 = \psi_0\psi_0^* = \frac{1}{m}\sum_{i,j=1}^m E_{ij} \otimes E_{ij},$$

and set

$$\psi_{U,V} = \sum_{i=1}^m Ue_i \otimes Ve_i, \quad \rho_{U,V} = \psi_{U,V}\psi_{U,V}^*.$$

Note that, if $m < n$, there is an obvious arbitrariness in the choice of V, if we treat V as a unitary matrix in M_n. (That is, $Ve_{m+1}, \dots, Ve_n$ play no role in determining $\psi_{U,V}$ and can be anything at all.) To eliminate such extraneous information, we shall henceforth treat $V \in M_{n,m}$ as an isometry from $\mathbb{C}^m$ to $\mathbb{C}^n$ (here we identify $\mathbb{C}^m$ with the subspace of $\mathbb{C}^n$ spanned by $\{e_1, \dots, e_m\}$).

Lemma 2.4. *Let $U \in U_m$ be unitary and let $V, W \in M_{n,m}$ be isometries. Then $\rho_{U,V} = \rho_{I,W}$ if and only if $W = e^{i\phi}VU^t$ for some $\phi \in \mathbb{R}$.*

Proof. Note $\rho_{U,V} = \rho_{I,W}$ if and only if $\psi_{U,V} = e^{i\theta}\psi_{I,W}$ for some $\theta \in \mathbb{R}$. But

$$\begin{aligned} e^{i\theta}\psi_{I,W} = \psi_{U,V} &\iff (e_j^* \otimes e_k^*)(e^{i\theta}\psi_{I,W}) = (e_j^* \otimes e_k^*)\psi_{U,V} \text{ for all } j = 1, \dots, m;\ k = 1, \dots, n \\ &\iff e^{i\theta}W_{kj} = \sum_{i=1}^m (e_j^*Ue_i)(e_k^*Ve_i) = \sum_{i=1}^m U_{ji}V_{ki} = (UV^t)_{jk} \\ &\iff W = e^{-i\theta}VU^t \end{aligned}$$

as asserted. □

Thus, every MES can be expressed as $\rho_{I,W}$ for an appropriate W, and clearly $\rho_{I,V} = \rho_{I,W}$ if and only if $W = e^{i\phi}V$ for some $\phi \in \mathbb{R}$. Note also that $\rho_{U,V} = \rho_0$ if and only if $UV^t = [e^{i\theta}I_m|0]$ for some $\theta \in \mathbb{R}$. The following lemma gives some insight into the linear structure of MES.

Lemma 2.5. *Fix $\lambda, \mu \in (0, 1)$ and an isometry $V_1 \in M_{n,m}$ such that $\rho_{I,V_1} \neq \rho_0$. Then there exist isometries $V_2, V_3 \in M_{n,m}$ satisfying*

$$\lambda\rho_0 + (1-\lambda)\rho_{I,V_1} = \mu\rho_{I,V_2} + (1-\mu)\rho_{I,V_3} \tag{1}$$

if and only if one of the following cases hold (for brevity, we shall write $\rho_i = \rho_{I,V_i}$):

1. *$\lambda = \mu$, $\rho_0 = \rho_2$, and $\rho_1 = \rho_3$.*
2. *$\lambda = 1 - \mu$, $\rho_0 = \rho_3$, and $\rho_1 = \rho_2$.*
3. *There exist $k \in \mathbb{R}$ and a complex unit ξ such that $\xi V_1 = W = \begin{bmatrix} K + kI \\ B \end{bmatrix}$ for some skew-hermitian matrix $K \in M_m$ and $B \in M_{n-m,m}$ (thus $k^2I_m - K^2 + B^*B = I_m$), and the conditions for the appropriate case (i) - (iv) below hold. Moreover, the states ρ_2 and ρ_3 must be given by $V_2 = a\begin{bmatrix} I_m \\ 0 \end{bmatrix} + bW$ and $V_3 = c\begin{bmatrix} I_m \\ 0 \end{bmatrix} + \delta W$, where $a, b, c > 0$ and $\delta < 0$ are given by (17), (16), (13), and (12) respectively. (See the proof for these equations.)*

(i) $k = 0$ and $\lambda \neq 1/2$: μ lies strictly between λ and $1-\lambda$. In this case $a = \sqrt{\frac{\lambda(1-\lambda-\mu)}{\mu(1-2\lambda)}}$.

(ii) $k = 0$ and $\lambda = 1/2$: $\mu = 1/2$. In this case $a = \cos\phi$, $b = \sin\phi$, $c = \sin\phi$, $\delta = -\cos\phi$ for $0 < \phi < \pi/2$ are all solutions.

(iii) $k \neq 0$ and $\mu = 1-\lambda$: $k(1-2\lambda) > 0$. In this case $a = \frac{2\lambda|k|}{\sqrt{(1-2\lambda)^2+4\lambda(1-\lambda)k^2}}$.

(iv) $k \neq 0$ and $\mu \neq 1-\lambda$: k, μ, and λ must be such that (11), (12), (13), and (15) all hold. In any case, there are at most two distinct solutions for a. (A particular example is $\mu = 1/2$, $\lambda \neq 1/2$: we get two distinct solutions for a in this case.)

Proof. Suppose (1) holds. Write $V_1 e_i = x_i$, $V_2 e_i = y_i$, and $V_3 e_i = z_i$, so $\{x_1, \ldots, x_m\}$, $\{y_1, \ldots, y_m\}$, $\{z_1, \ldots, z_m\}$ are orthonormal sets in $\mathbb{C}^n$. Since each term in equation (1) is positive semidefinite and of rank one, we must have that $\psi_{I,V_2}, \psi_{I,V_3}$ both lie in the span of ψ_0, ψ_{I,V_1}. Hence

$$\sum_{i=1}^{m} e_i \otimes y_i = a \sum_{i=1}^{m} e_i \otimes e_i + b \sum_{i=1}^{m} e_i \otimes x_i \tag{2}$$

and

$$\sum_{i=1}^{m} e_i \otimes z_i = c \sum_{i=1}^{m} e_i \otimes e_i + \delta \sum_{i=1}^{m} e_i \otimes x_i \tag{3}$$

for some constants a, b, c, δ. Since replacing V_i with $e^{i\theta_i} V_i$ does not affect equation (1), we may assume that $a, b, c \geq 0$ and write $\delta = de^{i\theta}$ with $d \geq 0$. Now if any of a, b, c, d are zero, then two of the states in (1) are identical (one from each side). The coefficients in front of these two states must match. (Otherwise, by re-arranging (1), we would obtain a linear combination of three pure states, with nonzero coefficients, equalling zero. This would imply that all the pure states ρ_i are identical, contradicting $\rho_1 \neq \rho_0$.) Thus we must have either the first or second case, and it is clear that both cases give a solution to (1). Henceforth, we assume $a, b, c, d > 0$.

Now since V_1, V_2, V_3 are isometries we have

$$x_i^* x_j = \delta_{ij} \quad \forall i.j = 1, \ldots, m \tag{4}$$

and similarly $y_i^* y_j = \delta_{ij}$, $z_i^* z_j = \delta_{ij}$ for all $i, j = 1, \ldots, m$. Using $y_i = ae_i + bx_i$ and $z_i = ce_i + de^{i\theta} x_i$, we see that these latter conditions are satisfied if and only if

$$\text{Re } (e_i^* x_i) = \frac{1 - a^2 - b^2}{2ab} \; \forall i \qquad \text{and} \qquad e_i^* x_j = -x_i^* e_j \; \forall i \neq j \tag{5}$$

and

$$\text{Re } (e^{i\theta} e_i^* x_i) = \frac{1 - c^2 - d^2}{2cd} \; \forall i \qquad \text{and} \qquad e^{2i\theta} e_i^* x_j = -x_i^* e_j \; \forall i \neq j. \tag{6}$$

We temporarily subdivide into two cases.

CASE I: Suppose x_i and e_i are linearly dependent for all i. From (4) we have $x_i = \omega_i e_i$ for some complex units ω_i, $i = 1, \ldots, m$, while (5) holds if and only if Re $\omega_i = (1 - a^2 - b^2)/2ab$ for all i. Thus there is some complex unit ω and subset $\mathcal{I} \subset \{1, \ldots, m\}$ such that $\omega_i = \omega$ for all $i \in \mathcal{I}$ and $\omega_i = \bar{\omega}$ for all $i \notin \mathcal{I}$. Since $\rho_1 \neq \rho_0$, $\mathcal{I}$ is a nonempty, proper subset and $\omega \notin \mathbb{R}$. For (6) to hold we must have Re $e^{i\theta}\omega$ = Re $e^{i\theta}\bar{\omega}$, implying that $e^{i\theta}$ is 1 or -1, and hence $\delta \in \mathbb{R}$.

On the other hand, (2) and (3) imply that $y_i = (a + b\omega)e_i$, $z_i = (c + \delta\omega)e_i$ for $i \in \mathcal{I}$, and $y_i = (a + b\bar{\omega})e_i$, $z_i = (c + \delta\bar{\omega})e_i$ for $i \notin \mathcal{I}$. Substituting these expressions for y_i and z_i into (1) gives

$$\lambda + (1-\lambda)\omega^2 = \mu(a + b\omega)^2 + (1-\mu)(c + \delta\omega)^2$$

as a necessary and sufficient condition for (1).

In summary, there is a solution to (1) in this case if and only if there exist a complex unit $\omega \neq \pm 1$, nonzero $\delta \in \mathbb{R}$, and $a, b, c > 0$ such that

$$\lambda + (1-\lambda)\omega^2 = \mu(a+b\omega)^2 + (1-\mu)(c+\delta\omega)^2, \tag{7}$$

$$\text{Re } \omega = \frac{1-a^2-b^2}{2ab} = \frac{1-c^2-\delta^2}{2c\delta}, \tag{8}$$

and $V_1 e_i = \omega e_i$ for all $i \in \mathcal{I}$ and $V_1 e_i = \bar{\omega} e_i$ for all $i \notin \mathcal{I}$.

To solve these equations, we write $\omega = e^{i\phi}$. Taking the real and imaginary parts of (7) gives

$$0 = \mu a^2 + (1-\mu)c^2 - \lambda + \cos\phi[2ab\mu + 2c\delta(1-\mu)] + \cos 2\phi[\mu b^2 + (1-\mu)\delta^2 - (1-\lambda)] \tag{9}$$

and, after dividing by $2\sin\phi$ (note $\sin\phi \neq 0$ since $\omega \neq \pm 1$),

$$0 = [ab\mu + c\delta(1-\mu)] + \cos\phi[\mu b^2 + (1-\mu)\delta^2 - (1-\lambda)] \tag{10}$$

respectively. Substituting $2ab\cos\phi = 1 - a^2 - b^2$ and $2c\delta\cos\phi = 1 - c^2 - \delta^2$ from (8) into (9), simplifying, and dividing by $\cos 2\phi - 1$, gives

$$\mu b^2 + (1-\mu)\delta^2 = 1 - \lambda, \tag{11}$$

whence

$$ab\mu + c\delta(1-\mu) = 0 \tag{12}$$

from (10), and thus

$$\mu a^2 + (1-\mu)c^2 = \lambda \tag{13}$$

from (9). Note that (12) implies that $\delta < 0$.

<u>CASE II</u>: Suppose that for some i, x_i and e_i are linearly independent. Substituting (2) and (3) into (1) and simplifying shows that (1) holds if and only if

$$\begin{aligned} 0 = e_i e_j^*[\mu a^2 + (1-\mu)c^2 - \lambda] + x_i x_j^*[\mu b^2 + (1-\mu)d^2 - (1-\lambda)] \\ + e_i x_j^*[\mu ab + (1-\mu)cde^{-i\theta}] + x_i e_j^*[\mu ab + (1-\mu)cde^{i\theta}] \end{aligned} \tag{14}$$

for all $i, j = 1, \ldots, m$. But x_i and e_i are linearly independent for some i, whence $e_i e_i^*$, $x_i x_i^*$, $e_i x_i^*$, $x_i e_i^*$ are linearly independent, so (14) holds if and only if the coefficients are all zero; that is, if and only if (11), (12), and (13) hold, with $e^{i\theta}$, and hence δ, real.

Now the isometry conditions (4), (5), (6) hold if and only if the isometry V_1 satisfies

$$\text{Re } (V_1)_{ii} = \frac{1-a^2-b^2}{2ab} = \frac{1-c^2-\delta^2}{2c\delta}$$

for all $i = 1, \ldots, m$ and $(V_1)_{ij} = -\overline{(V_1)_{ji}}$ for all $i \neq j$, $i, j = 1, \ldots, m$.

<u>Combining Case I and II</u>: Thus, we see that in both cases, there exist isometries V_2, V_3 satisfying (1) if and only if there exist $a, b, c > 0$ and $\delta < 0$ such that (11), (12), and (13) hold (this ensures (1) holds) and $V_1 = \begin{bmatrix} K + kI \\ B \end{bmatrix}$ for some skew-hermitian matrix $K \in M_m$ and $B \in M_{n-m}$, where

$$2abk = (1 - a^2 - b^2) \tag{15}$$

(this ensures (5), (6) hold, so that V_2, V_3 are isometries). Note that (11), (12), (13) automatically imply that

$$\begin{aligned}\frac{1-c^2-\delta^2}{2c\delta} &= \frac{1-c^2-\delta^2}{-2ab\mu}(1-\mu) \quad \text{using (12)}\\ &= \frac{1-a^2-b^2}{2ab}\end{aligned}$$

by adding (11) and (13) together and substituting for $(1-\mu)(c^2+\delta^2)$.

Solving for c^2 in (13) and δ^2 in (11) and substituting into (12) gives, after squaring and simplifying,

$$\lambda(1-\lambda) - \mu(1-\lambda)a^2 - \mu\lambda b^2 = 0. \tag{16}$$

By solving for b^2 in (16) and substituting into (15), then squaring and simplifying, we obtain the quadratic equation

$$\tilde{a}(a^2)^2 + \tilde{b}a^2 + \tilde{c} = 0 \tag{17}$$

where

$$\begin{aligned}\tilde{a} &= \mu^2[(1-2\lambda)^2 + \lambda(1-\lambda)4k^2],\\ \tilde{b} &= 2\lambda\mu[(1-2\lambda)(\mu-1+\lambda) - \lambda(1-\lambda)2k^2],\\ \tilde{c} &= \lambda^2(\mu-1+\lambda)^2,\end{aligned}$$

and the discriminant is

$$16\mu^2\lambda^3(1-\lambda)k^2[\lambda(1-\lambda)k^2 - (\mu-\lambda)(\mu-(1-\lambda))].$$

The maximum value of the factor in square brackets (as a function of μ) is attained when $\mu = 1/2$, and equals $(1/4) - \lambda(1-\lambda)(1-k^2)$. Since $\lambda(1-\lambda) \leq 1/4$ and $k^2 < 1$ (since V_1 is an isometry and $\rho_1 \neq \rho_0$), this factor is positive when $\mu = 1/2$. The minimum value of the factor in square brackets (as a function of $\mu \in [0,1]$) is attained when $\mu = 0$ or 1, and equals $\lambda(1-\lambda)(k^2-1) < 0$, so the discriminant is negative for values of μ sufficiently close to 0 or 1 (provided $k \neq 0$).

So, for a solution to exist, (17) must have a positive root for a^2; one can then solve for $b > 0$, $c > 0$, and $\delta < 0$ from (16), (13), and (12) respectively. Conversely, if one solves for $a, b, c > 0$ and $\delta < 0$ in this manner, then one can readily verify that (11) automatically holds, as does the square of (15). To have $b^2 > 0$ and $c^2 > 0$ from (16) and (13) though, it is necessary and sufficient that $a^2 < \lambda/\mu$. We now consider some special cases where the analysis is simplified.

Subcase 1: $k = 0$ and $\lambda \neq 1/2$.

The only solution to (17) is

$$a^2 = -\frac{\tilde{b}}{2\tilde{a}} = \frac{\lambda(1-\lambda-\mu)}{\mu(1-2\lambda)},$$

so we get a solution $a > 0$ if and only if $\lambda < 1/2$ and $\mu < 1-\lambda$, or $\lambda > 1/2$ and $\mu > 1-\lambda$. One can then uniquely determine b, c, and δ by using (16), (13), and (12) respectively. As already noted, (11) and (15) will also hold, and to ensure $b^2, c^2 > 0$ in (16) and (13), we need $\lambda - \mu a^2 > 0$ as well. Coupled with the preceding conditions, we find a (unique) solution for $a, b, c > 0$ if and only if μ lies strictly between λ and $1-\lambda$ (that is, the vector $\begin{bmatrix}\mu & 1-\mu\end{bmatrix}^t$ is strictly majorized by $\begin{bmatrix}\lambda & 1-\lambda\end{bmatrix}^t$).

Subcase 2: $k = 0$ and $\lambda = 1/2$.

In this case, (17) reduces to $\mu = 1/2$. Thus (11), (12), (13), and (15) become

$$b^2 + \delta^2 = 1, \quad ab + c\delta = 0, \quad a^2 + c^2 = 1, \text{ and } a^2 + b^2 = 1.$$

There are infinitely many solutions: $a = \cos\phi$, $b = \sin\phi$, $c = \sin\phi$, and $\delta = -\cos\phi$ for $0 < \phi < \pi/2$.

Subcase 3: $k \neq 0$ and $\mu = 1 - \lambda$.

In this case $\tilde{c} = 0$, so the only nonzero solution for a is given by

$$a^2 = -\frac{\tilde{b}}{\tilde{a}} = \frac{4\lambda^2(1-\lambda)k^2}{\mu[(1-2\lambda)^2 + 4\lambda(1-\lambda)k^2]} = \frac{4\lambda^2 k^2}{(1-2\lambda)^2 + 4\lambda(1-\lambda)k^2}.$$

One can then uniquely determine b, c, and δ by using (16), (13), and (12) respectively. To ensure $b^2, c^2 > 0$ in (16) and (13), we need $a^2 < \lambda/\mu$ which occurs if and only if $\lambda \neq 1/2$. Also, (15) holds if and only if $k(1-2\lambda) > 0$. Thus we get a (unique) solution for $a, b, c > 0$ if and only if $k(1-2\lambda) > 0$. (In particular, there is no solution if $\lambda = 1/2$.)

Subcase 4: $k \neq 0$ and $\mu \neq 1 - \lambda$.

We simply note that there are at most two solutions for $a > 0$, and that, for certain values of μ and λ, one can obtain two solutions. For example, if $\mu = 1/2$, then the discriminant is positive. Since $\tilde{a}, \tilde{c} > 0$ and $\tilde{b} < 0$, both roots of (17) are positive, and one can readily verify that $a^2 < \lambda/\mu$ for both roots. □

We shall refer to the solutions to (1) obtained in the first two cases of Lemma 2.5 as *trivial* solutions. In the nontrivial third case, there are always at least two choices for W (since $-\xi V_1 = -W$ is also of the correct form). More precisely, if $K + kI$ is a scalar multiple of I (note $B \neq 0$ in this case, since $\rho_1 \neq \rho_0$), then there are infinitely many choices for W (any complex unit ξ works). Otherwise, if $K + kI$ is not a scalar multiple of I, then there are exactly two choices for W. So, in order to have infinitely many solutions to (1), we are either in case 3(ii), or there are infinitely many choices for W. In either event it is possible to choose ξ so that $k = 0$. For future reference, we note and extend these observations in the following remark.

Remark 2.6. *Equation (1) has infinitely many solutions (for ρ_{I,V_2} and ρ_{I,V_3}) when $\lambda = \mu = 1/2$ if and only if $\xi V_1 = \begin{bmatrix} K \\ B \end{bmatrix}$ for some complex unit ξ and skew-hermitian $K \in M_m$. We can distinguish three cases:*

1. *K is not a scalar multiple of I. In this case, there are finitely many solutions to (1) when $\lambda = 3/4$ and $\mu = 1/2$ (we must have $W = \pm\begin{bmatrix} K \\ B \end{bmatrix}$ in case 3(i)). There is no nontrivial solution when $\lambda = 3/4$ and $\mu = 1 - \lambda = 1/4$.*

2. *K is a nonzero scalar multiple of I. There are infinitely many nontrivial solutions when $\lambda = 3/4$ and $\mu = 1 - \lambda = 1/4$ (take $W = e^{i\theta}\begin{bmatrix} K \\ B \end{bmatrix}$ with $0 < \theta < \pi$ or $-\pi < \theta < 0$ as appropriate in case 3(iii)).*

3. *$K = 0$. In this case, there are infinitely many solutions to (1) when $\lambda = 3/4$ and $\mu = 1/2$. There is no nontrivial solution when $\lambda = 3/4$ and $\mu = 1 - \lambda = 1/4$.*

Let us now focus on the special case $m = n$. Lemma 2.5 shows that MES of the form $\rho_{I,U}$, with U skew-hermitian, play a special role in the linear structure of Span(MES). A natural question is: does this smaller set of special MES span all of Span(MES)? The answer is no. First note that

$$\mathcal{T}_0 = \{\rho_{I,U} : U^* = -U \text{ is unitary}\} = \{\rho_{I,U} : U^* = U \text{ is unitary}\}$$

since, by Lemma 2.4, there is freedom in choosing a complex phase for U. We claim that $iE_{12} \otimes E_{12} - iE_{21} \otimes E_{21}$ lies in Span(MES) but does not lie in Span($\mathcal{T}_0$). To see the latter assertion, suppose H is a hermitian unitary. Then the entry in the $E_{12} \otimes E_{12}$ position of

$$\rho_{I,H} = \frac{1}{m} \sum_{i,j=1}^{m} E_{ij} \otimes HE_{ij}H^*$$

is $e_1^* He_1 e_2^* H^* e_2$, which is always real. Hence the entry in the $E_{12} \otimes E_{12}$ position of any matrix in Span($\mathcal{T}_0$) is real, so $iE_{12} \otimes E_{12} - iE_{21} \otimes E_{21} \notin$ Span($\mathcal{T}_0$).

Also from Lemma 2.5, one observes that $\mathcal{T} = \{\rho_{I,U} : U \in \Omega\}$, where

$$\Omega = \{e^{i\theta}(xI + iyH) : H \in H_m \cap U_m; x, y, \theta \in \mathbb{R}; x^2 + y^2 = 1\},$$

also plays a distinguished role in the linear structure of Span(MES). It requires a little more effort, but one can also show that $iE_{12}\otimes E_{12} - iE_{21}\otimes E_{21} \notin$ Span($\mathcal{T}$) either when $m > 2$, and so Span($\mathcal{T}$) $\neq$ Span(MES) if $m > 2$. (They are equal, however, when $m = 2$; this follows since Ω is precisely the set of unitaries with at most two distinct eigenvalues.) We are close, though; one can in fact extend $\mathcal{T}$ slightly to obtain a spanning set for Span(MES).

Lemma 2.7. *Let $m = n > 2$. The real linear span of*

$$\mathcal{T}_+ = \{\rho_{I,U} : U \in U_n \textit{ has at most 2 distinct eigenvalues or is unitarily similar to } \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \oplus I_{n-2}\}$$

is Span(MES).

Proof. Let $P_1, \ldots, P_n \in H_n$ be orthogonal rank 1 projections. Set $U = I - 2P_k$, $V = I - 2P_l$, and $W = I - 2P_k - 2P_l$ where $k \neq l$. Then

$$\rho_{I,U} - \rho_0 = \frac{1}{m} \sum_{i,j=1}^{m} E_{ij} \otimes (-2P_k E_{ij} - 2E_{ij}P_k + 4P_k E_{ij} P_k);$$

summing over k, adding $4\rho_0$, and then dividing by $4/m$ shows that

$$\sum_{i,j=1}^{m} E_{ij} \otimes \sum_{k=1}^{n} P_k E_{ij} P_k \in \text{Span}(\mathcal{T}_0) \subset \text{Span}(\mathcal{T}_+). \tag{18}$$

We also have

$$\rho_{I,W} - \rho_0 - (\rho_{I,U} - \rho_0) - (\rho_{I,V} - \rho_0) = \frac{4}{m} \sum_{i,j=1}^{m} E_{ij} \otimes (P_k E_{ij} P_l + P_l E_{ij} P_k).$$

This shows that, for any orthogonal rank 1 projections P and Q,

$$\sum_{i,j=1}^{m} E_{ij} \otimes (PE_{ij}Q + QE_{ij}P) \in \text{Span}(\mathcal{T}_0) \subset \text{Span}(\mathcal{T}_+). \tag{19}$$

Given an arbitrary unitary $\hat{U}$ we can use the spectral decomposition to write $\hat{U} = \sum_{k=1}^{n} \alpha_k P_k$ for some orthogonal rank 1 projections $P_1, \dots, P_n$ with $|\alpha_k| = 1$ for all k. Note

$$\begin{aligned} m\rho_{I,\hat{U}} &= \sum_{i,j=1}^{m} E_{ij} \otimes \sum_{k,l=1}^{n} \alpha_k \bar{\alpha}_l P_k E_{ij} P_l \\ &= \sum_{i,j=1}^{m} E_{ij} \otimes \sum_{k=1}^{n} P_k E_{ij} P_k + \sum_{i,j=1}^{m} E_{ij} \otimes \sum_{k \neq l} \alpha_k \bar{\alpha}_l P_k E_{ij} P_l \end{aligned}$$

We must show that $\rho_{I,\hat{U}} \in \mathrm{Span}(\mathcal{T}_+)$.

By (18), we see it suffices to show

$$\sum_{i,j=1}^{m} E_{ij} \otimes (e^{i\theta} P_k E_{ij} P_l + e^{-i\theta} P_l E_{ij} P_k) \in \mathrm{Span}(\mathcal{T}_+) \quad \forall k \neq l;$$

by (19), it suffices to show

$$\sum_{i,j=1}^{m} E_{ij} \otimes (iP_k E_{ij} P_l - iP_l E_{ij} P_k) \in \mathrm{Span}(\mathcal{T}_+) \quad \forall k \neq l. \tag{20}$$

Let $U = I - 2P_k$, $V = I - 2P_l$, and $X = iP_k - iP_l + (I - P_k - P_l)$. A computation gives

$$\begin{aligned} &\rho_{I,X} - \frac{1}{2}\rho_{I,U} - \frac{1}{2}\rho_{I,V} \\ &\qquad = \frac{1}{m} \sum_{i,j=1}^{m} E_{ij} \otimes i[2(P_l E_{ij} P_k - P_k E_{ij} P_l) + (P_k E_{ij} - E_{ij} P_k) - (P_l E_{ij} - E_{ij} P_l)]. \end{aligned}$$

Since $\rho_{I,X}$, $\rho_{I,U}$, $\rho_{I,V}$ all lie in $\mathcal{T}_+$, the above equation shows that (20) will hold if

$$\sum_{i,j=1}^{m} E_{ij} \otimes i(PE_{ij} - E_{ij}P) = \sum_{i,j=1}^{m} E_{ij} \otimes [(iP)E_{ij} + E_{ij}(iP)^*] \in \mathrm{Span}(\mathcal{T}_+) \tag{21}$$

for all rank 1 projections P.

Given any skew-hermitian unitary K and $x, y > 0$ satisfying $x^2 + y^2 = 1$, $xI + yK$ is a unitary matrix with at most two distinct eigenvalues. Since

$$\rho_{I,xI+yK} = x^2 \rho_0 + y^2 \rho_{I,K} + xy \frac{1}{m} \sum_{i,j=1}^{m} E_{ij} \otimes (KE_{ij} + E_{ij}K^*),$$

we have that

$$\sum_{i,j=1}^{m} E_{ij} \otimes (KE_{ij} + E_{ij}K^*) \in \mathrm{Span}(\mathcal{T}_+) \tag{22}$$

for all skew-hermitian unitary K. By linearity, and since the set of skew-hermitian unitaries spans the space of skew-hermitian matrices, we see that (22) holds for all skew-hermitian K, in particular $K = iP$, where P is a projection. Thus (21) holds for all projections P, and the proof is complete. □

3 Technical Lemmas

In this section we state and prove a number of lemmas which will be needed to prove our main theorem in the next section.

Our first result is a simple one; it will allow us to define a linear map on a quotient space in the proof of the main theorem.

Lemma 3.1. *For $A \in M_m$, $AE_{ij} + E_{ij}A^* = 0$ for all $i, j = 1, \dots, m$ if and only if $A = ikI$ for some $k \in \mathbb{R}$.*

Proof.

$$AE_{ij} + E_{ij}A^* = 0\ \forall i, j \iff e_k^*(AE_{ij} + E_{ij}A^*)e_l = 0 \quad \forall i, j, k, l \iff A_{ki}\delta_{jl} + \delta_{ik}(A^*)_{jl} = 0$$

Thus all off-diagonal entries of A are zero, and the diagonal entries A_{kk} are all equal and pure imaginary, as claimed. □

The next two results will allow us to extend a linear map on a quotient space of H_n to a very nice linear map on H_n.

Lemma 3.2. *Let $r \in \mathbb{N}$. There do not exist four rank r projections $Q_1, Q_2, Q_3, Q_4 \in H_{2r}$ such that, for any $i \neq j$, $Q_i + Q_j$ equals a projection plus a real scalar multiple of I.*

Proof. Suppose, by way of contradiction, that for any $i \neq j$, $Q_i + Q_j + kI$ is a projection for some $k \in \mathbb{R}$ (which may depend on the pair $\{i, j\}$). We can use the CS-decomposition to find an orthonormal basis such that, with respect to this basis,

$$Q_i = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}, \quad Q_j = \begin{bmatrix} C^2 & CS \\ CS & S^2 \end{bmatrix}$$

where $C, S \in M_r$ are nonnegative diagonal matrices satisfying $C^2 + S^2 = I_r$. By equating block-entries in $(Q_i + Q_j + kI)^2 = Q_i + Q_j + kI$ and simplifying, we have

1. $2(1+k)C^2 = -k(1+k)I$ from the upper left block,
2. $(2k+1)CS = 0$ from the upper right block, and
3. $2kS^2 = k(1-k)I$ from the lower right block.

So, from the second equation, we have either:

(a) $k = -1/2$ (in which case $C = \frac{1}{2}I$ and $S = \frac{\sqrt{3}}{2}I$ from the first and third equations), or

(b) $CS = 0$ (in which case the other equations imply $C = 0$).

Thus for $i \neq j$, we have $Q_iQ_jQ_i = \frac{1}{4}Q_i$ in case (a), or $Q_iQ_j = Q_jQ_i = 0$ in case (b). If case (b) occurs for every pairing of Q_i and Q_j, $i \neq j$, we get four orthogonal rank r projections Q_1, Q_2, Q_3, Q_4 in M_{2r}, a contradiction. Hence case (a) must occur at least once. Without loss of generality, we can write

$$Q_1 = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}, \quad Q_2 = \frac{1}{4}\begin{bmatrix} I_r & \sqrt{3}I_r \\ \sqrt{3}I_r & 3I_r \end{bmatrix}.$$

Note that Q_3 and Q_4 cannot both be orthogonal to Q_1; otherwise we would have $Q_3 = Q_4$ and then $Q_3 + Q_4$ could not equal a projection plus a scalar multiple of I, a contradiction. Without loss of generality case (a) occurs for the pairing Q_1 and Q_3; then $Q_1Q_3Q_1 = \frac{1}{4}Q_1$, so we can write

$$\begin{bmatrix} \frac{1}{4}I_r & B \\ B^* & D \end{bmatrix} = Q_3 = Q_3^2 = \begin{bmatrix} \frac{1}{16}I_r + BB^* & \frac{1}{4}B + BD \\ \frac{1}{4}B^* + DB^* & B^*B + D^2 \end{bmatrix}.$$

Equating the upper left blocks, we see that $B = \frac{\sqrt{3}}{4}U$ for some unitary U, whence $D = \frac{3}{4}I$ from equating the upper right blocks. But

$$Q_2 + Q_3 + kI = \begin{bmatrix} (\frac{1}{2} + k)I & \frac{\sqrt{3}}{4}(I + U) \\ \frac{\sqrt{3}}{4}(I + U^*) & (\frac{3}{2} + k)I \end{bmatrix}$$

is a projection for some $k \in \mathbb{R}$; comparing the upper right blocks of $(Q_2+Q_3+kI)^2 = Q_2+Q_3+kI$ gives $(2k + 1)(I + U) = 0$. If $k = -1/2$ then for $Q_2 + Q_3 + kI$ to be positive semidefinite we have $U = -I$. Thus $U = -I$ in any case, and Q_3 is uniquely determined.

Now if case (a) occurs for the pairing Q_1 and Q_4, the same argument shows that $Q_4 = Q_3$, giving a contradiction as before. Thus case (b) occurs for the pairing Q_1 and Q_4, whence $Q_4 = I - Q_1$. But then

$$Q_2 + Q_4 + kI = \begin{bmatrix} (\frac{1}{4} + k)I & \frac{\sqrt{3}}{4}I \\ \frac{\sqrt{3}}{4}I & (\frac{7}{4} + k)I \end{bmatrix}$$

is not idempotent for any k, giving our final contradiction. □

Lemma 3.3. *Let $\tilde{H}_n$ denote the quotient space $H_n/\mathbb{R}I = \{A + \mathbb{R}I : A \in H_n\}$, and for $A \in H_n$, let $\tilde{A} = A + \mathbb{R}I$. Suppose $\tilde{\psi} : \tilde{H}_n \to \tilde{H}_n$ is a (real) linear map such that, for any projection $P \in H_n$, $\tilde{\psi}(\tilde{P})$ contains a projection Q_P. Then there exists a linear map $\psi : H_n \to H_n$ such that $\tilde{\psi} \circ \pi = \pi \circ \psi$, where $\pi : H_n \to \tilde{H}_n$ is the canonical quotient map. Moreover, ψ has the form $\psi(A) = \epsilon UA^\sigma U^*$ for all $A \in H_n$, where U is a unitary matrix, $\epsilon \in \{-1, 0, 1\}$, and $A \mapsto A^\sigma$ denotes either the identity or the transpose map.*

Proof. Note that the only coset in $\tilde{H}_n$ containing more than one projection is $\tilde{0}$, which contains 0 and I. Let $\mathcal{P}_k$ denote the set of rank k projections in H_n, and let $\tilde{\mathcal{P}}_k = \pi(\mathcal{P}_k)$. Since $\tilde{\psi}$ is continuous and $\tilde{\mathcal{P}}_0 = \tilde{\mathcal{P}}_n, \tilde{\mathcal{P}}_1, \ldots, \tilde{\mathcal{P}}_{n-1}$ form n disjoint path-connected components, we have $\tilde{\psi}(\tilde{\mathcal{P}}_1) \subseteq \tilde{\mathcal{P}}_r$ for some $r \geq 0$. If $r = 0$ then, since $\tilde{\psi}$ is linear and the set of rank one projections span H_n, we have $\tilde{\psi} \equiv \tilde{0}$ and the lemma holds by taking $\psi \equiv 0$. So suppose $r > 0$. We split into two cases.

Case 1: Suppose $1 \leq r \leq n/2$. Let $P_1, \ldots, P_n$ be orthogonal rank 1 projections, and let Q_i be the unique projection (of rank r) in $\tilde{\psi}(\tilde{P}_i)$. Let $i \neq j$, so $P_i + P_j$ is a projection. Then there exists a projection in $\tilde{\psi}(\widetilde{P_i + P_j}) = \tilde{\psi}(\tilde{\mathcal{P}}_i) + \tilde{\psi}(\tilde{\mathcal{P}}_j) = \tilde{Q}_i + \tilde{Q}_j$, that is, $Q_i + Q_j + kI$ is a projection for some $k \in \mathbb{R}$.

If $r < n/2$, then $\operatorname{rank}(Q_i + Q_j) < n$, so 0 is an eigenvalue of $Q_i + Q_j$. For the spectrum of $Q_1 + Q_2 + kI$ to lie in $\{0, 1\}$, we must have $k = 0$. Thus $Q_i + Q_j$ is a projection, whence $Q_iQ_j = Q_jQ_i = 0$. Then $Q_1, \ldots, Q_n$ are orthogonal rank r projections, so we must have $rn \leq n$, whence $r = 1$. On the other hand, if $1 \neq r = n/2$, then we have $n \geq 4$. But this leads to a contradiction, since Lemma 3.2 says that it is impossible to have projections $Q_1, \ldots, Q_4$ of rank r such that $Q_i + Q_j + k_{ij}I$ is a projection for all $i \neq j$. Thus we must have $r = 1$, that is, $\tilde{\psi}(\tilde{\mathcal{P}}_1) \subseteq \tilde{\mathcal{P}}_1$.

We now construct the map ψ. Given $X \in H_n$, we may write $X = \sum_i a_i P_i$ for some real scalars a_i and rank 1 projections P_i. Define $\psi(X) = \sum_i a_i Q_{P_i}$. Provided ψ is well-defined, this clearly defines a linear map. Moreover,

$$(\pi \circ \psi)(X) = \sum_i a_i \tilde{\psi}(\tilde{P}_i) = \tilde{\psi}\left(\sum_i a_i \tilde{P}_i\right) = \tilde{\psi}(\tilde{X}) = (\tilde{\psi} \circ \pi)(X)$$

since $\tilde{\psi}$ is linear. Thus, it suffices to show that ψ is well-defined.

We must show that if $\sum_i a_i P_i = 0$, then $\sum_i a_i Q_{P_i} = 0$. Applying $\tilde{\psi} \circ \pi$ to both sides of $0 = \sum_i a_i P_i$ gives

$$\tilde{0} = \sum_i a_i \tilde{\psi}(\tilde{P}_i) = \sum_i a_i \tilde{Q}_{P_i},$$

that is, $\sum_i a_i Q_{P_i} \in \mathbb{R}I$. It follows that $\sum_i a_i Q_{P_i} = 0$ if and only if $\operatorname{Tr}\left(\sum_i a_i Q_{P_i}\right) = 0$. Thus, it suffices to show that $\operatorname{Tr} Q_P = \operatorname{Tr} P = 1$ for any rank 1 projection P. But this is true because $\tilde{\psi}(\tilde{\mathcal{P}}_1) \subseteq \tilde{\mathcal{P}}_1$.

Indeed, we also have $\psi(\mathcal{P}_1) \subseteq \mathcal{P}_1$. By [1, Corollary 1], ψ must have one of the following forms:

1. $\psi(A) = SAS^*$ for some $S \in M_n$,
2. $\psi(A) = SA^tS^*$ for some $S \in M_n$, or
3. $\psi(A) = L(A)B$ for some linear functional $L : H_n \to \mathbb{R}$ and $B \in H_n$ of rank 1.

We claim that the third case is inadmissable. Suppose, by way of contradiction, the third case occurs. We may assume that B is a rank 1 projection. Since $\psi(\mathcal{P}_1) \subseteq \mathcal{P}_1$, we have $L(A) = 1$ for all rank one projections; since $\mathcal{P}_1$ spans H_n, we have $L(A) = \operatorname{Tr} A$ for all $A \in H_n$. But then

$$\tilde{0} = \tilde{\psi}(\tilde{0}) = \tilde{\psi}(\tilde{I}) = \tilde{\psi} \circ \pi(I) = \pi \circ \psi(I) = n\tilde{B},$$

a contradiction.

So, either the first or second case must occur. Since $\psi(P)$ is a rank one projection for any rank one projection P, S must be invertible. Since $\psi(P)^2 = \psi(P)$ for all rank one projections P, we conclude that S must be unitary. Thus the lemma holds in this case.

Case 2: Suppose $n/2 < r < n$. Then the map $\tilde{\phi} = -\tilde{\psi}$ satisfies the hypotheses of the theorem and $\tilde{\phi}(\tilde{\mathcal{P}}_1) = -\tilde{\psi}(\tilde{\mathcal{P}}_1) \subseteq -\tilde{\mathcal{P}}_r = \tilde{\mathcal{P}}_{n-r}$ with $1 \leq n - r < n/2$. (Note that if P is a projection, then $-\tilde{P}$ contains the projection $I - P$.) Thus Case 1 applies to $\tilde{\phi}$ and the lemma holds. □

The final two lemmas will allow us to single out a particular unitary as being essentially unique.

Lemma 3.4. *Let $n \geq 3$ and $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. Let*

$$R_\alpha = \begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix}$$

and

$$\mathcal{R} = \{R_\alpha \oplus V : \alpha \in [0, 2\pi]; V \in H_{n-2} \cap U_{n-2}\}.$$

Then

$$\{U \in U_n : RU \in \mathbb{T}H_n \ \forall R \in \mathcal{R}\} = \mathbb{T}\left\{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \oplus I_{n-2} : \theta \in [0, 2\pi]\right\}$$

Proof. Suppose U is unitary and $RU \in \mathbb{T}H_n$ for all $R \in \mathcal{R}$. Set

$$U_0 = \left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \oplus I_{n-2}\right) U \quad \text{and write} \quad U = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

where $A \in M_2$, $D \in M_{n-2}$. We may remove an arbitrary complex phase by assuming that U_0 is hermitian. Suppose, by way of contradiction, that U_0 has a nonzero off-diagonal entry in the kth row for some $k \geq 3$. Let $V = I - 2e_{k-2}e_{k-2}^*$. Note that a matrix $X \in \mathbb{T}H_n$ if and only if $X^* = e^{i\theta}X$ for some $\theta \in \mathbb{R}$. Since

$$\left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \oplus V\right) U = (I_2 \oplus V)U_0 \in \mathbb{T}H_n$$

and $U_0 \in H_n$, we must have $U_0(I_2 \oplus V_0) = ((I_2 \oplus V)U_0)^* = -(I_2 \oplus V)U_0$. Thus, any entry of U_0 not in the kth row or column is zero—but then U_0 cannot be unitary, a contradiction. It follows that all off-diagonal entries of U_0 not in the (1,2)- or (2,1)-positions are zero. Thus $B = 0$, $C = 0$, A is unitary, and D is diagonal with ±1 on the diagonal. Without loss of generality we may assume $D_{11} = 1$.

Suppose, by way of contradiction, that $D_{kk} = -1$ for some k. Let $V \in H_{n-2} \cap U_{n-2}$ be arbitrary. Since

$$\left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \oplus V\right) U \in \mathbb{T}H_n \text{ implies } VD \in \mathbb{T}H_{n-2},$$

we can use the same argument as before to conclude that PVP^t is either block-diagonal or block-off-diagonal (where P is a permutation such that $PDP^t = I_r \oplus (-I_{n-2-r})$). But V was arbitrary, so this is a contradiction. Thus $D = I_{n-2}$.

It follows that $R_\alpha A \in H_2$ for all $\alpha \in [0, 2\pi]$. Considering $\alpha = 0$ and $\alpha = \pi/2$, we see that all four entries of A must be real. Direct computation reveals that

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

for some $\theta \in [0, 2\pi]$, as asserted. □

Lemma 3.5. *Let $U \in M_n$, $n \geq 3$, be a unitary of the form*

$$U = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \oplus I_{n-2}$$

for some $\theta \in [0, 2\pi)$. Let

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \oplus iI_{n-2}, \quad B = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \oplus e^{i\pi/4}I_{n-2}.$$

If AU and BU each have at most two distinct eigenvalues, then $U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \oplus I_{n-2}$ or $U = I_n$.

Proof. The eigenvalues of AU are $e^{i(\pi/2-\theta)}$, $e^{-i(\pi/2-\theta)}$, i. Two of these three eigenvalues must be equal; considering all three cases we find that $\theta = 0$, $\pi/2$, π, or $3\pi/2$. When $\theta = \pi$ or $3\pi/2$, BU has three distinct eigenvalues: $e^{i\pi/4}$, $e^{i3\pi/4}$, $e^{-i3\pi/4}$. One can readily verify that, when $\theta = 0$ or $\pi/2$, AU and BU have two distinct eigenvalues, so the lemma holds. □

4 Linear Preservers of Maximally Entangled States

We would like to characterize the real linear maps on $H_m \otimes H_n$ which preserve the set of MES. Clearly there is a lot of freedom in devising such maps: if Φ is one such map, one can obtain another linear preserver $\tilde{\Phi}$ by setting $\tilde{\Phi}(X) = \Phi(X)$ for all $X \in \text{Span(MES)}$, and defining $\tilde{\Phi}$ however we like on a basis for the orthogonal complement of Span(MES). Thus we should restrict our attention to real linear maps on Span(MES) which preserve the set of MES. Note that such a restriction makes this problem significantly more difficult: often one can solve preserver problems by making use of existing nice results for preservers on entire matrix spaces like M_n or H_n. In our case we do not have recourse to such results, as there appears to be no natural way to extend a preserver on Span(MES) to a map on all of $H_m \otimes H_n$.

In practice, one may be concerned with affine maps on states which preserve MES. The following proposition shows that, to characterize affine maps of co(MES) preserving MES, it is sufficient to consider linear maps on Span(MES) preserving MES.

Proposition 4.1. *Let $\Phi : co(MES) \to co(MES)$ be an affine map such that $\Phi(MES) \subseteq MES$. Then Φ extends to a unique linear map $\Psi : Span(MES) \to Span(MES)$.*

Proof. Let

$$\mathcal{K} = \left\{ \sum_{i=1}^{k} \lambda_i \rho_i : k \in \mathbb{N}, \lambda_i \geq 0, \rho_i \in MES \right\}$$

be the cone of positive semidefinite matrices generated by MES. Since an element $A \in \mathcal{K}$ lies in co(MES) if and only if $\operatorname{Tr} A = 1$, we can extend Φ to a map $\Psi : \mathcal{K} \to \mathcal{K}$ by defining $\Psi(t\rho) = t\Phi(\rho)$ for any $t \geq 0$ and any $\rho \in co(MES)$. Clearly Ψ is affine and homogeneous. Given $A \in Span(MES)$, we can write $A = \rho_+ - \rho_-$ for some $\rho_+, \rho_- \in \mathcal{K}$. Set $\Psi(A) = \Psi(\rho_+) - \Psi(\rho_-)$. It is easy to check that this gives a well-defined linear map on Span(MES). It is clear that this extension is unique. □

We come to the main theorem of this paper. Henceforth, we restrict ourselves to the case $m = n$, but we do not assume that the preserver is surjective.

Theorem 4.2. *Let MES denote the set of maximally entangled states in $M_m \otimes M_m$. A linear map $\Phi : Span(MES) \to Span(MES)$ preserves MES if and only if it has one of the following forms:*

1. *$\Phi(A \otimes B) = UA^\sigma U^* \otimes VB^\sigma V^*$ for some unitaries $U, V \in M_m$.*

2. *$\Phi(A \otimes B) = UB^\sigma U^* \otimes VA^\sigma V^*$ for some unitaries $U, V \in M_m$.*

3. *$\Phi(X) = (Tr\, X)\rho$ for some $\rho \in MES$.*

Here the map $A \mapsto A^\sigma$ denotes either the identity or the transpose map.

Note that if the preserver Φ is surjective, only the first two cases can occur.

Proof. Sufficiency is clear. To prove necessity, suppose $\Phi(MES) \subseteq MES$. We may write $\Phi(\rho_0) = (U \otimes V)\rho_0(U \otimes V)^*$ for some unitaries $U, V \in M_m$. By replacing Φ with the map $X \mapsto (U \otimes V)^*\Phi(X)(U \otimes V)$ if necessary, we may assume $\Phi(\rho_0) = \rho_0$.

Step 1. Let $\mathcal{P}_{skew} = \{\rho_{I,V} : V \in M_m \text{ is skew-hermitian unitary}\}$. We claim $\Phi(\mathcal{P}_{skew}) \subseteq \mathcal{P}_{skew}$.

Let V_1 be a skew-hermitian unitary and write $\rho_1 = \rho_{I,V_1}$. Suppose, by way of contradiction, that $\Phi(\rho_1) \notin \mathcal{P}_{skew}$, so $\rho_1 \neq \rho_0$. By Lemma 2.5, case 3(ii), the equation

$$\frac{1}{2}\rho_0 + \frac{1}{2}\rho_1 = \frac{1}{2}\rho_2 + \frac{1}{2}\rho_3 \tag{23}$$

has infinitely many solutions for MES ρ_2, ρ_3; for example, one can take $\rho_2 = \rho_{I,V_2}$ where $V_2 = \cos\theta\, I + \sin\theta\, V_1$, $\theta \in [0, 2\pi]$. By applying Φ to both sides of (23), we see that the equation

$$\frac{1}{2}\rho_0 + \frac{1}{2}\Phi(\rho_1) = \frac{1}{2}\tilde{\rho_2} + \frac{1}{2}\tilde{\rho_3}. \tag{24}$$

has solutions $\tilde{\rho_2} = \Phi(\rho_{I,V_2})$. On the other hand, by Lemma 2.5 and our assumption, the only solutions to (24) are trivial, namely $\tilde{\rho_2} = \rho_0$ or $\Phi(\rho_1)$. Thus

$$\{\Phi(\rho_{I,\cos\theta\, I+\sin\theta\, V_1}) : \theta \in [0, 2\pi]\} \subseteq \{\rho_0, \Phi(\rho_1)\}.$$

Considering $\theta = 0, \pi/2$, we see that these two sets are equal. But the set on the left-hand side is connected, while the set on the right-hand side is not, unless $\Phi(\rho_1) = \rho_0$. But this contradicts $\Phi(\rho_1) \notin \mathcal{P}_{skew}$. Thus our claim holds.

Step 2. We claim there is a map g from the set of skew-hermitian unitaries back to itself satisfying

$$\Phi\left(\sum_{i,j=1}^{m} E_{ij} \otimes (KE_{ij} + E_{ij}K^*)\right) = \sum_{i,j=1}^{m} E_{ij} \otimes (g(K)E_{ij} + E_{ij}g(K)^*)$$

and

$$\Phi(\rho_{I,xI+yK}) = \rho_{I,xI+yg(K)}$$

for all skew-hermitian unitaries K and all $x, y \in \mathbb{R}$.

Set $g(iI) = iI$ and $g(-iI) = -iI$; from Lemma 3.1 and $\Phi(\rho_0) = \rho_0$, the asserted conditions hold. So now assume $K \in M_m$ is a skew-hermitian unitary that is not a scalar multiple of I. Write $\rho_1 = \rho_{I,K}$, and suppose $0 < \lambda < \mu < 1 - \lambda < 1$ with $\mu \neq 1/2$. By Lemma 2.5,

$$\lambda\rho_0 + (1-\lambda)\rho_1 = \mu\rho_2 + (1-\mu)\rho_3 \quad (*)$$

is satisfied for $\rho_2 = \rho_{I,aI+bK}$ and $\rho_3 = \rho_{I,cI+\delta K}$, where a, b, c, δ are as described in Lemma 2.5, case 3(i). Since Φ preserves $\mathcal{P}_{skew}$, we may write $\Phi(\rho_1) = \rho_{I,\tilde{K}}$ for some skew-hermitian unitary $\tilde{K} \in M_m$. Applying Φ to $(*)$, we have

$$\lambda\rho_0 + (1-\lambda)\rho_{I,\tilde{K}} = \mu\Phi(\rho_2) + (1-\mu)\Phi(\rho_3).$$

Now if $\rho_{I,\tilde{K}} \neq \rho_0$, then by Lemma 2.5 we must have $\Phi(\rho_2) = \rho_{I,aI+b\tilde{K}}$ (in which case set $g(K) = \tilde{K}$) or $\rho_{I,aI-b\tilde{K}}$ (in which case set $g(K) = -\tilde{K}$). On the other hand, if $\rho_{I,\tilde{K}} = \rho_0$ then we must have $\Phi(\rho_2) = \rho_0$ and $\tilde{K} = \pm iI$. In this case set $g(K) = iI$; since $a^2 + b^2 = 1$ (see (15) in the proof of Lemma 2.5), we have $\Phi(\rho_2) = \rho_0 = \rho_{I,(a+ib)I} = \rho_{I,aI+bg(K)}$.

In any case, we have $\Phi(\rho_2) = \rho_{I,aI+bg(K)}$. Now compare the two sides of this equation:

$$\begin{aligned} m\rho_{I,aI+bg(K)} &= \sum_{i,j=1}^{m} E_{ij} \otimes (aI + bg(K))E_{ij}(aI + bg(K))^* \\ &= a^2\rho_0 + b^2\rho_{I,\tilde{K}} + ab\sum_{i,j=1}^{m} E_{ij} \otimes (g(K)E_{ij} + E_{ij}g(K)^*) \end{aligned}$$

whereas m$\Phi(\rho_2)$ equals

$$\Phi\left(\sum_{i,j=1}^{m} E_{ij}\otimes(aI+bK)E_{ij}(aI+bK)^*\right) = \Phi\left(a^2\rho_0 + b^2\rho_1 + ab\sum_{i,j=1}^{m} E_{ij}\otimes(KE_{ij}+E_{ij}K^*)\right)$$

$$= a^2\rho_0 + b^2\rho_{I,\tilde{K}} + ab\Phi\left(\sum_{i,j=1}^{m} E_{ij}\otimes(KE_{ij}+E_{ij}K^*)\right).$$

Since $a,b>0$, we have

$$\Phi\left(\sum_{i,j=1}^{m} E_{ij}\otimes(KE_{ij}+E_{ij}K^*)\right) = \sum_{i,j=1}^{m} E_{ij}\otimes(g(K)E_{ij}+E_{ij}g(K)^*);$$

it then follows that $\Phi(\rho_{I,xI+yK}) = \rho_{I,xI+yg(K)}$ for all $x,y\in\mathbb{R}$, as claimed.

Step 3: We claim that either

(a) $\Phi(\rho_{I,xI+iyH}) = \rho_0$ for all hermitian unitary H and all $x,y\in\mathbb{R}$ satisfying $x^2+y^2=1$, or

(b) there is a *linear* map $\psi: H_m\to H_m$ such that $\Phi(\rho_{I,xI+iyH}) = \rho_{I,xI+iy\psi(H)}$ for all hermitian unitary H and all $x,y\in\mathbb{R}$.

Moreover, ψ has the form $\psi(A)=\epsilon UA^\sigma U^*$ for all $A\in H_m$, where U is a unitary matrix, $\epsilon\in\{-1,1\}$, and $A\mapsto A^\sigma$ denotes either the identity or the transpose map.

Since the real linear span of skew-hermitian unitaries is the space of skew-hermitian matrices, and since Φ is linear, Step 2 shows that for each skew-hermitian K we have

$$\Phi\left(\sum_{i,j=1}^{m} E_{ij}\otimes(KE_{ij}+E_{ij}K^*)\right) = \sum_{i,j=1}^{m} E_{ij}\otimes(\hat{K}E_{ij}+E_{ij}\hat{K}^*)$$

for some skew-hermitian $\hat{K}$ (depending on K). This allows us to define a real linear map $\tilde{\psi}:\tilde{H}_m\to\tilde{H}_m$ (here $\tilde{H}_m$ denotes the quotient space $\tilde{H}_m = H_m/\mathbb{R}I = \{A+\mathbb{R}I : A\in H_m\}$) as follows. Given $X\in H_m$, let $\tilde{X}$ denote its coset in $\tilde{H}_m$ and define $\tilde{\psi}(\tilde{X})=\tilde{Y}$ where

$$\Phi\left(\sum_{i,j=1}^{m} E_{ij}\otimes(iXE_{ij}-iE_{ij}X)\right) = \sum_{i,j=1}^{m} E_{ij}\otimes(iYE_{ij}-iE_{ij}Y).$$

By Lemma 3.1, this map is well-defined, and it is clearly linear. Moreover, if H is a hermitian unitary we have $\tilde{\psi}(\tilde{H}) = \widetilde{-ig(iH)}$, where g is as in Step 2. Since $P\in H_m$ is a projection if and only if $2P-I$ is a hermitian unitary, it follows that for any projection P there exists a projection Q_P such that $\tilde{\psi}(\tilde{P}) = \widetilde{Q_P}$.

By Lemma 3.3, $\tilde{\psi}\circ\pi = \pi\circ\psi$ for a linear map $\psi: H_m\to H_m$ of a particular form. This implies that, for any hermitian unitary H, $\widetilde{\psi(H)} = \widetilde{-ig(iH)}$, so that $g(iH) = i\psi(H) + ik_HI$ for some $k_H\in\mathbb{R}$.

Case (a): If $\psi=0$ we have $g(K)\in\{\pm iI\}$ for all skew-hermitian unitary K. In this case

$$\Phi(\rho_{I,xI+yK}) = \rho_{I,xI+yg(K)} = \rho_{I,(x+iy)I} = \rho_{I,(x-iy)I} = \rho_0$$

for all skew-hermitian unitary K and $x, y \in \mathbb{R}$ satisfying $x^2 + y^2 = 1$.

Case (b): If $\psi \neq 0$, then ψ has the form $\psi(A) = \epsilon U A^\sigma U^*$ for all $A \in H_m$, where U is a unitary matrix, $\epsilon \in \{-1, 1\}$, and $A \mapsto A^\sigma$ denotes either the identity or the transpose map. Thus any hermitian unitary H that is not a multiple of I is mapped to a hermitian unitary $\psi(H)$ that is not a multiple of I. Since $g(iH)$ must be a skew-hermitian unitary it follows that $k_H = 0$ for such H. Since setting $g(iI) = i\psi(I) = \pm iI$ does not affect $\Phi(\rho_{I,xI+yK}) = \rho_{I,xI+yg(K)}$, we have

$$\Phi(\rho_{I,xI+iyH}) = \rho_{I,xI+yg(iH)} = \rho_{I,xI+iy\psi(H)}$$

for all hermitian unitary H and all $x, y \in \mathbb{R}$. The claim holds.

Step 4: We normalize Φ in the following sense. If case (b) in Step 3 holds, there is a linear map L on the real space $\mathbb{R}I + iH_m$ such that

$$\Phi(\rho_{I,xI+iyH}) = \rho_{I,L(xI+iyH)}$$

for all hermitian unitary H and all $x, y \in \mathbb{R}$. More explicitly: if $\psi(A) = UA^\sigma U^*$ then $L(B) = UB^\sigma U^*$; if $\psi(A) = -UA^\sigma U^*$ then $L(B) = U(B^*)^\sigma U^*$ (here $A \mapsto A^\sigma$ denotes either the identity or the transpose map). Thus L is a composition of unitary similarity, transpose, and/or complex conjugation. Each of these maps (acting on unitary matrices) give rise to maps on Span(MES) that are of the form asserted by the main theorem; we list the correspondences below.

Let $f : U_m \to U_m$ and define a map ϕ on MES by $\phi(\rho_{I,A}) = \rho_{I,f(A)}$.

1. Let $f(A) = UA$ for some unitary U. Then $\phi(\rho) = (I \otimes U)\rho(I \otimes U^*)$.
2. Let $f(A) = AV$ for some unitary V. Then

   $$\phi(\rho_{I,A}) = \rho_{I,AV} = \rho_{V^t,A}$$

   by Lemma 2.4, so

   $$\phi(\rho) = (V^t \otimes I)\rho(V^t \otimes I)^*.$$

3. Let $f(A) = \bar{A}$. Consider the map on $H_m \otimes H_m$ given by $B \otimes C \mapsto (B \otimes C)^t = B^t \otimes C^t$. Under this map, we have

   $$\rho_{U,V} = \frac{1}{m}\sum_{i,j=1}^m UE_{ij}U^* \otimes VE_{ij}V^* \mapsto \frac{1}{m}\sum_{i,j=1}^m \bar{U}E_{ji}U^t \otimes \bar{V}E_{ij}V^t = \rho_{\bar{U},\bar{V}}.$$

   Setting $U = I$ we see that this is identical to the map $\phi(\rho_{I,V}) = \rho_{I,f(V)}$.

4. Let $f(A) = A^t$. Consider the map $U \otimes V \mapsto V \otimes U$. Under this map, we have

   $$\rho_{U,V} = \frac{1}{m}\sum_{i,j=1}^m UE_{ij}U^* \otimes VE_{ij}V^* \mapsto \frac{1}{m}\sum_{i,j=1}^m VE_{ij}V^* \otimes UE_{ij}U^* = \rho_{V,U} = \rho_{I,UV^t}$$

   by Lemma 2.4. Setting $U = I$ we see that this is identical to the map $\phi(\rho_{I,V}) = \rho_{I,f(V)}$.

It follows that Φ is equal to an invertible map Ψ of the desired form when restricted to the set

$$\mathcal{T} = \{\rho_{I,xI+iyH} : H \in H_m \cap U_m;\ x, y \in \mathbb{R};\ x^2 + y^2 = 1\}.$$

Since Φ is of the desired form (on all of Span(MES)) if and only if $\Psi^{-1} \circ \Phi$ is, we may, without loss of generality, replace Φ with $\Psi^{-1} \circ \Phi$ and assume that Φ fixes each element of $\mathcal{T}$. Now, considering both cases from Step 3, we have either

(a) $\Phi(\rho) = \rho_0$ for all $\rho \in \mathcal{T}$, or

(b) $\Phi(\rho) = \rho$ for all $\rho \in \mathcal{T}$.

It is worth recalling that $\mathcal{T} = \{\rho_{I,U} : U \in \Omega\}$, where

$$\Omega = \{e^{i\theta}(xI + iyH) : H \in H_m \cap U_m; x, y, \theta \in \mathbb{R}; x^2 + y^2 = 1\}$$

is precisely the set of unitaries with at most two distinct eigenvalues. Thus, for $m = 2$, we have $\mathcal{T} = MES$. Since Φ is linear, Φ is either the identity map or the degenerate map $X \mapsto (\operatorname{Tr} X)\rho_0$ on Span(MES). In either case Φ is of the desired form and the theorem holds. Henceforth we assume $m > 2$.

Step 5: With the normalization from Step 4 (namely, $\Phi(\rho) = \rho_0$ for all $\rho \in \mathcal{T}$ or $\Phi(\rho) = \rho$ for all $\rho \in \mathcal{T}$), we claim that either

(a) $\Phi(\rho) = \rho_0$ for all $\rho \in \mathcal{T}_+$, or

(b) $\Phi(\rho) = \rho$ for all $\rho \in \mathcal{T}_+$ (note $\mathcal{T}_+$ is defined in Lemma 2.7).

From this claim, combined with Lemma 2.7 and the linearity of Φ, the theorem follows immediately.

Case A: Suppose we are in the case where $\Phi(\rho) = \rho_0$ for all $\rho \in \mathcal{T}$. To show that $\Phi(\rho) = \rho_0$ for all $\rho \in \mathcal{T}_+$, it suffices to show that $\Phi(\rho_{I,Z}) = \rho_0$ where Z is any unitary matrix with eigenvalues $i, -i, 1, \ldots, 1$ (counting multiplicity). By choosing a suitable orthonormal basis, we may write

$$Z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \oplus I_{m-2}.$$

Let

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \oplus iI_{n-2}, \quad B = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \oplus e^{i\pi/4} I_{n-2}.$$

With the aid of Lemma 2.5, one can verify that the equation

$$\lambda\rho_0 + (1-\lambda)\rho_{I,AZ} = \mu\rho_{I,U_2} + (1-\mu)\rho_{I,U_3} \tag{25}$$

is satisfied for $\lambda = 1/2$ and $\mu = 1/6$ by $U_2 = aI + bW$, $U_3 = cI + \delta W$ where $W = -e^{-i\pi/4}AZ$, $a = 1$, $b = \sqrt{2}$, $c = \sqrt{2/5}$, and $\delta = -1/\sqrt{5}$. Applying the similarity transform $X \mapsto (I \otimes A^*)X(I \otimes A)$ to (25) gives

$$\lambda\rho_{I,A^*} + (1-\lambda)\rho_{I,Z} = \mu\rho_{I,A^*U_2} + (1-\mu)\rho_{I,A^*U_3}. \tag{26}$$

Applying Φ to (26), we get

$$\lambda\rho_0 + (1-\lambda)\Phi(\rho_{I,Z}) = \mu\rho_0 + (1-\mu)\rho_0$$

since

$$A^*, \quad A^*U_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \oplus (-I_{m-2}), \quad A^*U_3 = \begin{bmatrix} 0 & -\frac{3+i}{\sqrt{10}} \\ \frac{3+i}{\sqrt{10}} & 0 \end{bmatrix} \oplus \frac{1-3i}{\sqrt{10}} I_{m-2}$$

each have 2 distinct eigenvalues. Thus $\Phi(\rho_{I,Z}) = \rho_0$ as desired.

Case B: Suppose we are in the case where $\Phi(\rho) = \rho$ for all $\rho \in \mathcal{T}$. To show that $\Phi(\rho) = \rho$ for all $\rho \in \mathcal{T}_+$, it suffices to show that $\Phi(\rho_{I,Z}) = \rho_{I,Z}$ where Z is any unitary matrix with eigenvalues $i, -i, 1, \ldots, 1$ (counting multiplicity). As in Case A, we can choose a suitable orthonormal basis and write

$$Z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \oplus I_{m-2}.$$

We now make a few general observations.

Consider the equation

$$\lambda \rho_{I,U_0} + (1-\lambda)\rho_{I,U_1} = \mu \rho_{I,U_2} + (1-\mu)\rho_{I,U_3} \tag{27}$$

where $U_0, U_1, U_2, U_3 \in M_m$ are unitary and $\lambda, \mu \in (0,1)$. By applying the similarity transform $X \mapsto (I \otimes U_0^*)X(I \otimes U_0)$ to both sides of (27), we see that (27) holds if and only if

$$\lambda \rho_0 + (1-\lambda)\rho_{I,U_0^*U_1} = \mu \rho_{I,U_0^*U_2} + (1-\mu)\rho_{I,U_0^*U_3} \tag{28}$$

does. We may write $\Phi(\rho_{I,U}) = \rho_{I,f(U)}$ for some function $f : U_m \to U_m$. Then applying Φ to (27) gives

$$\lambda \rho_{I,f(U_0)} + (1-\lambda)\rho_{I,f(U_1)} = \mu \rho_{I,f(U_2)} + (1-\mu)\rho_{I,f(U_3)},$$

which in turn holds if and only if

$$\lambda \rho_0 + (1-\lambda)\rho_{I,f(U_0)^*f(U_1)} = \mu \rho_{I,f(U_0)^*f(U_2)} + (1-\mu)\rho_{I,f(U_0)^*f(U_3)} \tag{29}$$

does. From this we obtain two useful properties.

1. If $U_0^*U_1$ has two distinct eigenvalues, then, by Lemma 2.5, (28) has solutions for unitary U_2, U_3 when $\mu = 1/2$ and $\lambda = 1/4$. It follows that (27) and hence (29) also have solutions when $\mu = 1/2$ and $\lambda = 1/4$. By Lemma 2.5, $f(U_0)^*f(U_1)$ has at most two distinct eigenvalues.

2. If $U_0^*U_1$ is hermitian with two distinct eigenvalues, then, by Lemma 2.5, (28) has infinitely many solutions for U_2, U_3 when $\mu = \lambda = 1/2$. In particular, $U_2 = (\cos\theta)\, U_0 + (\sin\theta)\, U_1$ is a solution for any $\theta \in [0, \pi/2]$. It follows that these choices for U_2 will also give solutions to (29) when $\mu = \lambda = 1/2$.

   Suppose for the moment that $f(U_0)^*f(U_1) \notin \mathbb{T}H_m$, where $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. By Lemma 2.5, (29) has only the trivial solutions

   $$\rho_{I,f(U_0)^*f(U_2)} = \rho_0 \quad \text{or} \quad \rho_{I,f(U_0)^*f(U_2)} = \rho_{I,f(U_0)^*f(U_1)}.$$

   But then

   $$\begin{aligned}\{\rho_0, \rho_{I,f(U_0)^*f(U_1)}\} &\subseteq \{\rho_{I,f(U_0)^*f(U_2)} : U_2 = (\cos\theta)\, U_0 + (\sin\theta)\, U_1, 0 \le \theta \le \pi/2\} \\ &\subseteq \{\rho_0, \rho_{I,f(U_0)^*f(U_1)}\};\end{aligned}$$

   since the middle set is path connected, we have $\rho_{I,f(U_0)^*f(U_1)} = \rho_0$, whence $f(U_0)^*f(U_1) \in \mathbb{T}I$, contradicting our assumption that $f(U_0)^*f(U_1) \notin \mathbb{T}H_m$. Thus it is always the case that $f(U_0)^*f(U_1) \in \mathbb{T}H_m$.

By our assumption on Φ, if $U \in U_m$ has at most two distinct eigenvalues, $f(U) \in \mathbb{T}U$. If $V \in U_m$ and UV has at most two distinct eigenvalues then $Uf(V)$ has at most two distinct eigenvalues by property (1). Similarly, if $UV \in \mathbb{T}H_m$ then $Uf(V) \in \mathbb{T}H_m$ by property (2).

Using the notation

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \oplus iI_{n-2}, \quad B = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \oplus e^{i\pi/4} I_{n-2}$$

and the results from Lemmas 3.4 and 3.5, it follows that

$$\{U \in U_m : RU \in \mathbb{T}H_m \forall R \in \mathcal{R},\ AU \text{ and } BU \text{ have at most two distinct eigenvalues}\} = \{\mathbb{T}I, \mathbb{T}Z\};$$

on the other hand, if U lies in the set on the left-hand side, then so does $f(U)$. Thus $f(Z) \in \mathbb{T}I \cup \mathbb{T}Z$, or equivalently, $\Phi(\rho_{I,Z}) = \rho_0$ or $\rho_{I,Z}$.

Suppose, by way of contradiction, that $\Phi(\rho_{I,Z}) = \rho_0$. Applying Φ to (26), we get

$$\lambda \rho_{I,A^*} + (1-\lambda)\rho_0 = \mu \rho_{I,A^* U_2} + (1-\mu)\rho_{I,A^* U_3} \tag{30}$$

by our assumption and since A^*, A^*U_2, A^*U_3 each have 2 distinct eigenvalues. But by Lemma 2.5, since A^* is skew-hermitian (resulting in $k = 0$ in case 3), there is no solution to (30) when $\lambda = 1/2$ and $\mu = 1/6$. Hence Φ must fix $\rho_{I,Z}$ and our proof for is complete. □

Corollary 4.3. *Let $\Phi : M_m \otimes M_m$ be an affine map such that $\Phi(co(MES)) = co(MES)$. Then Φ has one of the following forms, when restricted to Span(MES):*

1. *$\Phi(A \otimes B) = UA^\sigma U^* \otimes VB^\sigma V^*$ for some unitaries $U, V \in M_m$.*
2. *$\Phi(A \otimes B) = UB^\sigma U^* \otimes VA^\sigma V^*$ for some unitaries $U, V \in M_m$.*

Here the map $A \mapsto A^\sigma$ denotes either the identity or the transpose map.

Proof. Since the extreme points of the convex hull of MES is MES, we must have $\Phi(MES) = MES$. By Proposition 4.1 and Theorem 4.2, the result follows. □

A final comment on the case of a bipartite system where the subsystems have different dimensions $m \neq n$: we conjecture that the linear preservers in this case must have either form (1) or (3) from our main Theorem 4.2. Unfortunately the case $m < n$ appears to be substantially different, and our methods seem to break down around step 3 of the proof. It would be interesting to verify or refute this conjecture; we hope that the structural Lemma 2.5 might be of some use in this regard.

Acknowledgments

The author would like to thank Professors Chi-Kwong Li and Yu Guo for some helpful discussions.

References

[1] E.M. Baruch and R. Loewy, Linear preservers on spaces of hermitian or real symmetric matrices, Linear Algebra Appl. 183 (1993) 89-102.

[2] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, Teleporting an unknown quantum state via dual classical and EPR channels, Phys. Rev. Lett. 70 (1993) 1895-1899.

[3] C.H. Bennett and S.J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, Phys. Rev. Lett. 69 (1992) 2881-2884.

[4] S. Friedland, C.-K. Li, Y.-T. Poon, and N.-S. Sze, The automorphism group of separable states in quantum information theory, J. Math. Phys. 52, 042203 (2011).

[5] A. Guterman, C.-K. Li, and P. Semrl, Some general techniques on linear preserver problems, Linear Algebra Appl. 315 (2000) 61-81.

[6] C.-K. Li and S. Pierce, Linear preserver problems, Amer. Math. Monthly 108 (2001) 591-605.

[7] C.-K. Li, Y.-T. Poon, and N.-S. Sze, Linear preservers of tensor product of unitary orbits, and product numerical range, Linear Algebra Appl. 438 (2013) 3797-3803.

[8] M. Nielsen and I. Chuang, Quantum computation and quantum information, Cambridge University Press, 2000.