ENDOMORPHISMS AND QUANTUM OPERATIONS

Stan Gudder
Department of Mathematics
University of Denver
Denver, Colorado 80208
stan.gudder@nsm.du.edu

Abstract

We define a quantum operation as a special type of endomorphism between spaces of matrices. Representations of endomorphisms are considered and an isomorphism between higher dimensional matrices and endomorphisms is derived. We then employ this isomorphism to prove various results for endomorphisms and quantum operations. For example, an endomorphism is completely positive if and only if its corresponding matrix is positive. Although a few new results are proved, this is primarily a survey article that simplifies and unifies previous work on the subject.

Keywords: endomorphisms, quantum operations, quantum computation.

PACS: 02.10.Yn, 02.30.Tb, 03.67.Lx.

1 Introduction

Quantum operations play a very important role in quantum computation, quantum information and quantum measurement theory [2, 3, 5, 8, 11, 14, 15, 16]. They describe discrete quantum dynamics, quantum measurements, noisy quantum channels, interactions with the environment and error correcting codes. Mathematically, a quantum operation is described by a completely positive map which, in finite dimensions, is a special type of endomorphism between spaces of matrices. In this survey article we derive representations of endomorphisms and an isomorphism between higher dimensional matrices and endomorphisms. We then employ this isomorphism to prove various results concerning endomorphisms and quantum operations. For example, an endomorphism is hermitian-preserving or completely positive if and only if the corresponding matrix is hermitian or positive, respectively.

This isomorphism was first suggested by Jamiolkowski [12], later exploited by Choi [4] and most recently used by Arrighi and Patricot [1]. However, we believe that our methods are simpler and more direct than previous ones and we also obtain a new type of isomorphism. Moreover, we shall derive some results that were not considered in [1]. Although most of our results are not new, we believe that the study of these endomorphisms provides a unifying theme for an important physical theory.

2 Matrix Spaces

Although there is a well developed theory of endomorphisms and quantum operations on infinite dimensional Hilbert spaces, our main concern here is with quantum computation and information theory which takes place in a finite dimensional setting. We shall use the notation M_d for the set of all $d \times d$ hermitian matrices and Herm_d for the set of all $d \times d$ hermitian matrices and Herm_d^+ for the set of all $d \times d$ positive matrices. If V_1, V_2 are complex linear spaces an **endomorphism** $\Omega\colon V_1 \to V_2$ is a linear map from V_1 to V_2. The set of endomorphisms from V_1 to V_2 is denoted $\mathrm{End}\,(V_1, V_2)$ and is a linear space in its own right. The spaces M_d are linear in the usual way and in this work, we are primarily interested in $\mathrm{End}\,(M_n, M_n)$.

Let $\mathbb{C}^n$ be the complex n-dimensional linear space of n-tuples of complex numbers with the usual inner product $\langle x \mid y\rangle$. We assume that $\langle x \mid y\rangle$ is linear in the second argument and employ Dirac notation $|x\rangle$ for "kets" and $\langle x|$ for "bras." Throughout the discussion we use a fixed canonical orthonormal basis $|i\rangle$ for $\mathbb{C}^n$, $i = 1, \dots, n$. In quantum computation and information theory, $\{|i\rangle\}$ is called the **computational basis**. Any ket $a \in \mathbb{C}^n$ has a unique representation $a = \sum a_i|i\rangle$ and the corresponding bra $a^\dagger$ is given by $a^\dagger = \sum a_i^*\langle i|$ where a_i^* is the complex conjugate of $a_i \in \mathbb{C}$. We denote the n-dimensional identity matrix in M_n by I_n. The space $\mathrm{End}(\mathbb{C}^n, \mathbb{C}^m)$ is identified with the space of complex $m \times n$ matrices in the usual way using the computational bases. If $\{|i\rangle\}$ is the orthonormal basis for $\mathbb{C}^m$ and $\{|k\rangle\}$ the orthonormal basis for $\mathbb{C}^n$, then any $m\times n$ matrix has the form $A=\sum a_{ij}|i\rangle\langle j|$ and its adjoint is given by $A^\dagger=\sum a_{ij}^*|j\rangle\langle i|$. We identify $\mathbb{C}^{mn}$ with the tensor product $\mathbb{C}^m\otimes\mathbb{C}^n$ and write the canonical basis $|i\rangle\otimes|j\rangle$ for $\mathbb{C}^{mn}$ as $|i\rangle|j\rangle$, $i=1,\dots,m$, $j=1,\dots,n$.

It is well known that the linear space $\mathrm{End}(\mathbb{C}^n,\mathbb{C}^m)$ is an inner product space under the Hilbert-Schmidt inner product $\langle A\mid B\rangle=\mathrm{tr}(A^\dagger B)$. For $A=\sum a_{ij}|i\rangle|j\rangle\in\mathbb{C}^{mn}$ define $\widehat{A}\in\mathrm{End}(\mathbb{C}^n,\mathbb{C}^m)$ by $\widehat{A}=\sum a_{ij}|i\rangle\langle j|$.

Theorem 2.1. *The map* $^\wedge\colon\mathbb{C}^{mn}\to\mathrm{End}(\mathbb{C}^n,\mathbb{C}^m)$ *is a unitary transformation.*

Proof. It is clear that $^\wedge$ is a linear bijection. To show that $^\wedge$ preserves inner products we have

$$\left\langle\widehat{A}\mid\widehat{B}\right\rangle=\mathrm{tr}(\widehat{A}^\dagger\widehat{B}=\sum\langle j|\widehat{A}^\dagger\widehat{B}|j\rangle=\sum a_{jk}^*b_{kj}=\langle A\mid B\rangle\qquad\square$$

Notice that $(|i\rangle|j\rangle)^\wedge=|i\rangle\langle j|$ so that $^\wedge$ maps the canonical basis for $\mathbb{C}^{mn}$ to the canonical basis for $\mathrm{End}(\mathbb{C}^n,\mathbb{C}^m)$. It is important to emphasize that the isomorphism $^\wedge$ is basis dependent. However, this is not a big disadvantage because in quantum computation and quantum information theory one usually sticks with the computational basis. Letting $|\beta\rangle=\sum|j\rangle|j\rangle$ be the canonical maximally entangled "state" of $\mathbb{C}^n\otimes\mathbb{C}^n$, the next lemma gives useful relationships between A and $\widehat{A}$.

Lemma 2.2. *For* $A\in\mathbb{C}^{mn}$ *we have that*

$$\widehat{A}=(I_m\otimes\langle\beta|)\,(A)\tag{2.1}$$

and

$$A=(\widehat{A}\otimes I_n)\langle\beta|\tag{2.2}$$

Proof. To prove (2.1) we have

$$\begin{aligned}(I_m\otimes\langle\beta|)\,(|i\rangle|j\rangle)&=\left(I_m\otimes\sum\langle k|\langle k|\right)(|i\rangle|j\rangle)\\&=|i\rangle\otimes\sum\langle k|\langle k\mid j\rangle=|i\rangle\langle j|=(|i\rangle|j\rangle)^\wedge\end{aligned}$$

and the result follows by linearity. To prove (2.2) we have

$$\left((|i\rangle|j\rangle)^\dagger \otimes I_n\right)|\beta\rangle = (|i\rangle\langle j| \otimes I_n)\sum |k\rangle|k\rangle$$
$$= \sum_k |i\rangle\langle j \mid k\rangle|k\rangle = |i\rangle|j\rangle$$

and the result follows by linearity. □

The next result will be useful in Section 4. If $A_i \in \mathbb{C}^d$, notice that $\sum A_iA_i^\dagger \in M_d$

Lemma 2.3. [15] *Let* $A_i, B_i \in \mathbb{C}^d$ $i = 1, \ldots, r$. *Then* $\sum A_iA_i^\dagger = \sum B_iB_i^\dagger$ *if and only if there exists a unitary matrix* $[u_{ij}]$ *such that* $B_k = \sum u_{jk}A_j$, $j, k = 1, \ldots, r$.

Proof. If $B_k = \sum u_{jk}A_j$ for a unitary matrix $[u_{jk}]$, we have that

$$\sum B_iB_i^\dagger = \sum u_{ji}A_ju_{ki}^*A_k^\dagger = \sum A_jA_k^\dagger\delta_{jk} = \sum A_jA_j^\dagger$$

Conversely, suppose that $S = \sum A_iA_i^\dagger = \sum B_iB_i^\dagger$. Then $S \in M_d$ is a positive matrix so by the spectral theorem we can write $S = \sum \lambda_k|k\rangle\langle k|$ where $|k\rangle$ is an orthonormal system and $\lambda_k > 0$. Letting $\left|\widetilde{k}\right\rangle = \left|\sqrt{\lambda_k}\, k\right\rangle$ we have that $S = \sum \left|\widetilde{k}\right\rangle\left\langle\widetilde{k}\right|$ where $\left|\widetilde{k}\right\rangle$ are mutually orthogonal vectors. Letting $|\psi\rangle$ be a vector that is orthogonal to all the $\left|\widetilde{k}\right\rangle$'s we have that

$$0 = \langle\psi|S|\psi\rangle = \sum |\langle\psi \mid A_i\rangle|^2$$

Hence, $\langle\psi \mid A_i\rangle = 0$, $i = 1, \ldots, r$, so that $A_i \in \left\{\left|\widetilde{k}\right\rangle\right\}^{\perp\perp}$. It follows that $A_i = \sum c_{ik}\left|\widetilde{k}\right\rangle$ for some $c_{ik} \in \mathbb{C}$. Hence,

$$\sum \left|\widetilde{k}\right\rangle\left\langle\widetilde{k}\right| = \sum A_iA_i^\dagger = \sum_{k,\ell}\left(\sum_i c_{ik}c_{i\ell}^*\right)\left|\widetilde{k}\right\rangle\left\langle\widetilde{\ell}\right|$$

Since the $\left|\widetilde{k}\right\rangle$ are mutually orthogonal, we conclude that $\sum_i c_{ik}c_{i\ell}^* = \delta_{k\ell}$. Hence, $c = [c_{ik}]$ is a unitary matrix. Similarly, we can find a unitary matrix $d = [d_{ik}]$ such that $B_i = \sum d_{ki}\left|\widetilde{k}\right\rangle$. Thus, $B_i = \sum u_{ji}A_j$ where $u = dc^\dagger$ is unitary. □

Let $|i\rangle$, $|k\rangle$ be elements of the canonical basis for $\mathbb{C}^m$ and $|j\rangle$, $|\ell\rangle$ be elements of the canonical basis for $\mathbb{C}^n$. Then $|i\rangle|j\rangle\langle\ell|\langle k| \in M_{mn}$, $|j\rangle\langle\ell| \in M_n$ and $|i\rangle\langle k| \in M_m$. We define the **partial traces** tr_1 and tr_2 by

$$\mathrm{tr}_1\left(|i\rangle|j\rangle\langle\ell|\langle k|\right) = |j\rangle\langle\ell|\delta_{ik}$$
$$\mathrm{tr}_2\left(|i\rangle|j\rangle\langle\ell|\langle k|\right) = |i\rangle\langle k|\delta_{j\ell}$$

and extend by linearity to obtain $\mathrm{tr}_1 \in \mathrm{End}(M_{mn}, M_n)$ and $\mathrm{tr}_2 \in \mathrm{End}(M_{mn}, M_m)$. In general, if $A \in M_{mn}$ with

$$A = \sum a_{ijk\ell}|i\rangle|j\rangle\langle\ell|\langle k|$$

we have that

$$\mathrm{tr}_1(A) = \sum a_{iji\ell}|j\rangle\langle\ell|$$

and

$$\mathrm{tr}_2(A) = \sum a_{ijkj}|i\rangle\langle k|$$

Notice that for $B \in M_m$, $C \in M_n$ we have that $\mathrm{tr}_1(B \otimes C) = \mathrm{tr}(B)C$. Indeed, if $B = \sum b_{ik}|i\rangle\langle k|$, $C = \sum c_{j\ell}|j\rangle\langle\ell|$ then

$$B \otimes C = \sum b_{ik}c_{j\ell}|i\rangle|j\rangle\langle k|\langle\ell|$$

and we have that

$$\mathrm{tr}_1(B \otimes C) = \sum b_{ii}c_{j\ell}|j\rangle\langle\ell| = \mathrm{tr}(B)C$$

In fact, tr_1 is the unique element of $\mathrm{End}(M_{mn}, M_n)$ satisfying $\mathrm{tr}_1(B \otimes C) = \mathrm{tr}(B)C$. In a similar way $\mathrm{tr}_2(B \otimes C) = \mathrm{tr}(C)B$.

When we speak of a **state** we are actually referring to an unnormalized state which is an element of Herm_d^+. A state of the form $|\alpha\rangle\langle\alpha|$ for $|\alpha\rangle \in \mathbb{C}^d$, $|\alpha\rangle \neq 0$ is called a **pure state**. The isomorphism Theorem 2.1 provides some interesting characterizations for various types of pure states in $\mathbb{C}^n \otimes \mathbb{C}^n$. We call $|\beta\rangle = \sum |i\rangle|i\rangle$ the **canonical maximally entangled** state. A state $|\alpha\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ is **maximally entangled** if $\mathrm{tr}_1\left(|\alpha\rangle\langle\alpha|\right) = I_n$ or $\mathrm{tr}_2\left(|\alpha\rangle\langle\alpha|\right) = I_n$. A state $|\alpha\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ is **totally entangled** if $\mathrm{tr}_1\left(|\alpha\rangle\langle\alpha|\right)$ or $\mathrm{tr}_2\left(|\alpha\rangle\langle\alpha|\right)$ is invertible.

Theorem 2.4. *Let $|\alpha\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ be a state.* (i) *$|\alpha\rangle$ is the canonical maximally entangled state if and only if $|\alpha\rangle^\wedge = I_n$.* (ii) *$|\alpha\rangle$ is maximally entangled if and only if $|\alpha\rangle^\wedge$ is unitary.* (iii) *$|\alpha\rangle$ is totally entangled if and only if $|\alpha\rangle^\wedge$ is invertible.*

Proof. (i) $|\alpha\rangle^\wedge = I_n = \sum |i\rangle\langle i|$ if and only if $|\alpha\rangle = \sum |i\rangle|i\rangle = |\beta\rangle$.
(ii) Suppose that $|\alpha\rangle = \sum a_{ij}|i\rangle|j\rangle$ so that

$$|\alpha\rangle\langle\alpha| = \sum a_{ij}a_{k\ell}^*|i\rangle|j\rangle\langle\ell|\langle k|$$

We then have that

$$\mathrm{tr}_1\left(|\alpha\rangle\langle\alpha|\right) = \sum a_{ij}a_{i\ell}^*|j\rangle\langle\ell| \tag{2.3}$$

Thus, $\mathrm{tr}_1\left(|\alpha\rangle\langle\alpha|\right) = I_n$ if and only if

$$\sum a_{ij}a_{k\ell}^*|i\rangle\langle\ell| = \sum |i\rangle\langle i|$$

This latter condition is equivalent to $|\alpha\rangle^\wedge = \sum a_{ij}|i\rangle\langle j|$ being unitary. A similar result holds if $\mathrm{tr}_2\left(|\alpha\rangle\langle\alpha|\right) = I_n$. (iii) As in (i) we have Eqn. (2.3). Moreover,

$$\begin{aligned}|\alpha\rangle^\dagger|\alpha\rangle &= \sum a_{ij}^*|j\rangle\langle i| \sum a_{k\ell}|k\rangle\langle\ell| \\ &= \sum a_{ij}^*a_{k\ell}\delta_{ik}|j\rangle\langle\ell| = \sum a_{ij}^*a_{i\ell}|j\rangle\langle\ell|\end{aligned}$$

Thus, $\mathrm{tr}_1\left(|\alpha\rangle\langle\alpha|\right)$ is invertible if and only if $|\alpha\rangle^\dagger|\alpha\rangle$ is invertible. But $|\alpha\rangle^\dagger|\alpha\rangle$ if and only if $|\alpha\rangle^\wedge$ is invertible. □

We close this section with a result that will be useful in the sequel.

Lemma 2.5. *If $A, B \in \mathbb{C}^{mn}$, then $\mathrm{tr}_1(AB^\dagger) = (\widehat{B}^\dagger\widehat{A})^t$ and $\mathrm{tr}_2(AB^\dagger) = \widehat{A}\widehat{B}^\dagger$.*

Proof. Let $A = \sum a_{ij}|i\rangle|j\rangle$ and $B = \sum b_{k\ell}|k\rangle|\ell\rangle$. Then

$$AB^\dagger = \sum a_{ij}b_{k\ell}^*|i\rangle|j\rangle\langle\ell|\langle k|$$

and we have that

$$\begin{aligned}\mathrm{tr}_2(AB^\dagger) &= \sum a_{ij}b_{k\ell}^*|i\rangle\langle k| = \left(\sum a_{ij}|i\rangle\langle j|\right)\left(\sum b_{k\ell}^*|\ell\rangle\langle k|\right) \\ &= \left(\sum a_{ij}|i\rangle\langle j|\right)\left(\sum b_{k\ell}|k\rangle\langle\ell|\right)^\dagger = \widehat{A}\widehat{B}^\dagger\end{aligned}$$

Moreover,

$$\begin{aligned}\left[\operatorname{tr}_1(AB^\dagger)\right]^t &= \left[\sum a_{ij}b_{i\ell}^*|j\rangle\langle\ell|\right]^t = \sum a_{ij}b_{i\ell}^*|\ell\rangle\langle j| \\ &= \left(\sum b_{k\ell}^*|\ell\rangle\langle k|\right)\left(\sum a_{ij}|i\rangle\langle j|\right) \\ &= \left(\sum b_{k\ell}|k\rangle\langle\ell|\right)^\dagger\left(\sum a_{ij}|i\rangle\langle j|\right) \\ &= \widehat{B}^\dagger\widehat{A}\end{aligned}$$

Hence, $\operatorname{tr}_1(AB^\dagger) = (\widehat{B}^\dagger\widehat{A})^t$. □

3 Endomorphisms

This section establishes two isomorphism theorems between M_{mn} and $\operatorname{End}(M_n, M_m)$. As in Section 2, we consider M_{mn} to be a complex linear space with inner product $\langle S \mid T\rangle = \operatorname{tr}(S^\dagger T)$, we let $|i\rangle, |k\rangle$ be elements of the canonical basis for $\mathbb{C}^m$ and $|j\rangle, |\ell\rangle$ be elements of the canonical basis for $\mathbb{C}^n$. Then

$$\{S_{ijk\ell}\colon i,k=1,\dots,m;\quad j,\ell=1,\dots,n\}$$

where $S_{ijk\ell} = |i\rangle|j\rangle\langle k|\langle\ell|$ becomes an orthonormal basis for M_{mn} and $\{E_{j\ell}\colon j,\ell=1,\dots,n\}$ where $E_{j\ell} = |j\rangle\langle\ell|$ becomes an orthonormal basis for M_n. Moreover, we define $\mathcal{S}_{ijk\ell} \in \operatorname{End}(M_n, M_m)$ by

$$\mathcal{S}_{ijk\ell}(\rho) = |i\rangle\langle j|\rho|\ell\rangle\langle k|$$

Finally, for $\mathcal{S}, \mathcal{T} \in \operatorname{End}(M_n, M_m)$ we define

$$\langle\mathcal{S} \mid \mathcal{T}\rangle = \sum_{r,s}\operatorname{tr}\left(\mathcal{S}(E_{rs})^\dagger\mathcal{T}(E_{rs})\right)$$

Lemma 3.1. *$\operatorname{End}(M_n, M_m)$ is an m^2n^2 dimensional inner product space with orthonormal basis $\mathcal{S}_{ijk\ell}$.*

Proof. Clearly $\operatorname{End}(M_n, M_m)$ is a linear space with dimension m^2n^2. It is also evident that $\langle\mathcal{S} \mid \mathcal{T}\rangle$ is sesquilinear and $\langle\mathcal{S} \mid \mathcal{S}\rangle \geq 0$. Suppose that $\langle\mathcal{S} \mid \mathcal{S}\rangle = 0$. Then

$$\sum_{r,s}\operatorname{tr}\left(\mathcal{S}(E_{rs})^\dagger\mathcal{S}(E_{rs})\right) = 0$$

so that $\operatorname{tr}\left(\mathcal{S}(E_{rs})^\dagger\mathcal{S}(E_{rs})\right) = 0$, $r,s = 1,\ldots,n$. Hence $\mathcal{S}(E_{rs}) = 0$, $r,s = 1,\ldots,n$, so by linearity $\mathcal{S} = 0$. Therefore, $\langle\mathcal{S}\mid\mathcal{T}\rangle$ is an inner product. To show that $\{\mathcal{S}_{ijk\ell}\}$ forms a basis we have

$$\begin{aligned}
\langle\mathcal{S}_{ijk\ell}\mid\mathcal{S}_{i'j'k'\ell'}\rangle &= \sum_{r,s}\operatorname{tr}\left(\mathcal{S}_{ijk\ell}(E_{rs})^\dagger\mathcal{S}_{i'j'k'\ell'}(E_{rs})\right)\\
&= \sum_{r,s}\operatorname{tr}\left((|i\rangle\langle k|)^\dagger\,|i'\rangle\langle k'|\right)\delta_{jr}\delta_{\ell s}\delta_{j'r}\delta_{\ell' s}\\
&= \delta_{jj'}\delta_{\ell\ell'}\operatorname{tr}\left((|k\rangle\langle i|)\,(|i'\rangle\langle k'|)\right)\\
&= \delta_{jj'}\delta_{\ell\ell'}\delta_{ii'}\delta_{kk'}
\end{aligned}$$

Hence, $\{\mathcal{S}_{ijk\ell}\}$ is an orthonormal system and since there are m^2n^2 of these elements, $\{\mathcal{S}_{ijk\ell}\}$ forms a basis. □

Define $^\wedge\colon M_{mn}\to\operatorname{End}(M_n,M_m)$ by $\widehat{S}_{ijk\ell} = \mathcal{S}_{ijk\ell}$ and extend by linearity.

Corollary 3.2. *The map* $^\wedge\colon M_{mn}\to\operatorname{End}(M_n,M_m)$ *is a unitary transformation.*

Proof. Since $^\wedge$ maps the orthonormal basis $\{S_{ijk\ell}\}$ onto the orthonormal basis $\{\mathcal{S}_{ijk\ell}\}$, it must be unitary. □

We denote the inverse of the unitary transformation $^\wedge$ by $^\vee\colon\operatorname{End}(M_n,M_m)\to M_{mn}$. We now present our two main isomorphism theorems.

Theorem 3.3. (i) *If* $S\in M_{mn}$ *has the form* $S = AB^\dagger$ *for* $A,B\in\mathbb{C}^{mn}$, *then* $\widehat{S}(\rho) = \widehat{A}\rho\widehat{B}^\dagger$ *for every* $\rho\in M_n$. (ii) $\mathcal{S}\in\operatorname{End}(M_n,M_m)$ *if and only if* $\mathcal{S}$ *has the form*

$$\mathcal{S}(\rho) = \sum_s\widehat{A}_s\rho\widehat{B}_s^\dagger \tag{3.1}$$

for $A_s,B_s\in\mathbb{C}^{mn}$.

Proof. (i) Suppose $S = AB^\dagger$ for $A,B\in\mathbb{C}^{mn}$. Then for every $\rho\in M_n$ we have that

$$\begin{aligned}
\widehat{S}(\rho) = (AB^\dagger)^\wedge(\rho) &= \left[\sum a_{ij}|i\rangle|j\rangle\left(\sum b_{k\ell}|k\rangle|\ell\rangle\right)^\dagger\right]^\wedge(\rho)\\
&= \sum a_{ij}b_{k\ell}^*\left(|i\rangle|j\rangle\langle k|\langle\ell|\right)^\wedge(\rho) = \sum a_{ij}b_{k\ell}^*\widehat{S}_{ijk\ell}(\rho)\\
&= \sum a_{ij}b_{k\ell}^*\mathcal{S}_{ijk\ell}(\rho) = \sum a_{ij}b_{k\ell}^*|i\rangle\langle j|\rho|\ell\rangle\langle k|\\
&= \left(\sum a_{ij}|i\rangle\langle j|\right)\rho\left(\sum b_{k\ell}|k\rangle\langle\ell|\right)^\dagger = \widehat{A}\rho\widehat{B}^\dagger
\end{aligned}$$

(ii) It is clear that if $\mathcal{S}$ has the form (3.1) then $\mathcal{S} \in \mathrm{End}(M_n, M_m)$. Conversely, if $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ then by Corollary 3.2 $\mathcal{S} = \widehat{S}$ for some $S \in M_{mn}$. Now S has the form $S = \sum c_{rs} D_r B_s^\dagger$ so by (i) and linearity we have that

$$\mathcal{S}(\rho) = \widehat{S}(\rho) = \sum_{r,s} c_{rs} \widehat{D}_r \rho \widehat{B}_s^\dagger = \sum_s \widehat{A}_s \rho \widehat{B}_s^\dagger$$

where $A_s = \sum_r c_{rs} D_r$. □

Theorem 3.4. (i) *If $S \in M_{mn}$ has the form $S = A \otimes B$ for $A \in M_m$, $B \in M_n$, then $\widehat{S}(\rho) = \mathrm{tr}(B^t \rho) A$ for all $\rho \in M_m$.* (ii) *$\mathcal{S} \in \mathrm{End}(M_n, M_m)$ if and only if $\mathcal{S}$ has the form*

$$\mathcal{S}(\rho) = \sum_r \mathrm{tr}(B_r \rho) A_r \tag{3.2}$$

for $B_r \in M_n$, $A_r \in M_m$.

Proof. (i) Suppose $S = A \otimes B$ for $A \in M_m$, $B \in M_n$. Then for every $\rho \in M_n$ we have that

$$\begin{aligned} \widehat{S}(\rho) &= (A \otimes B)^\wedge(\rho) = \left(\sum a_{ik} |i\rangle\langle k| \otimes \sum b_{j\ell} |j\rangle\langle \ell|\right)^\wedge (\rho) \\ &= \sum a_{ik} b_{j\ell} \left(|i\rangle|j\rangle\langle k|\langle \ell|\right)^\wedge (\rho) = \sum a_{ik} b_{j\ell} |i\rangle\langle j|\rho|\ell\rangle\langle k| \\ &= \left(\sum b_{j\ell} \rho_{j\ell}\right) \sum a_{ik} |i\rangle\langle k| = \mathrm{tr}(B^t \rho) A \end{aligned}$$

(ii) It is clear that if $\mathcal{S}$ has the form (3.2), then $\mathcal{S} \in \mathrm{End}(M_n, M_m)$. Conversely, if $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ then by Corollary 3.2 $\mathcal{S} = \widehat{S}$ for some $S \in M_{mn}$. Now S has the form $S = \sum c_{rs} A_r \otimes D_s$ for $A_r \in M_m$, $D_s \in M_n$ so by (i) linearity we have that

$$\mathcal{S}(\rho) = \widehat{S}(\rho) = \sum_{r,s} c_{rs} \mathrm{tr}(D_s^t \rho) A_r = \sum_r \mathrm{tr}(B_r \rho) A_r$$

where $B_r = \sum_s c_{rs} D_s^t$. □

Corollary 3.5. *$\mathcal{S} \in \mathrm{End}(M_n, M_m)$ if and only if $\mathcal{S}$ has the form $\mathcal{S}(\rho) = \mathrm{tr}_2\left(D(I_m \otimes \rho)\right)$ for some $D \in M_{mn}$.*

Proof. It is clear that if $\mathcal{S}$ has the given form, then $\mathcal{S} \in \mathrm{End}(M_n, M_m)$. Conversely, if $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ then letting $D = \sum A_r \otimes B_r$ and applying (3.2) gives

$$\begin{aligned} \mathrm{tr}_2\left(D(I_m \otimes \rho)\right) &= \mathrm{tr}_2\left(\left(\sum A_r \otimes B_r\right)(I_m \otimes \rho)\right) = \sum \mathrm{tr}_2(A_r \otimes B_r \rho) \\ &= \sum \mathrm{tr}(B_r\rho)A_r = \mathcal{S}(\rho) \end{aligned}$$

□

The next result gives a different version of Corollary 3.5. We denote the identity endomorphism from M_n to M_n by $\mathcal{I}_n$.

Lemma 3.6. *For $S \in M_{mn}$ we have that*

$$\widehat{S}(\rho) = \mathrm{tr}_2\left(S(I_m \otimes \rho)\right) \tag{3.3}$$

and

$$S = (\widehat{S} \otimes \mathcal{I}_n)\left(|\beta\rangle\langle\beta|\right) = \sum \widehat{S}(E_{ij}) \otimes E_{ij} \tag{3.4}$$

Proof. Notice that (3.3) holds for $S = S_{ijk\ell}$. Hence, (3.3) holds in general by linearity. To verify (3.4), let $S = \sum s_{ij}A_iB_j^\dagger$ for $A_iB_j \in \mathbb{C}^{mn}$ and apply (2.2) to obtain

$$\begin{aligned} (\widehat{S} \otimes \mathcal{I}_n)\left(|\beta\rangle\langle\beta|\right) &= \sum s_{ij}(\widehat{A}_i \otimes I_n)|\beta\rangle\langle\beta|(\widehat{B}_j^\dagger \otimes I_n) \\ &= \sum s_{ij}A_iB_j^\dagger = S \end{aligned}$$

The last equality follows from $|\beta\rangle\langle\beta| = \sum E_{ij} \otimes E_{ij}$. □

For $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ define $\widetilde{\mathcal{S}} \in \mathrm{End}(M_n, M_m)$ by $\widetilde{\mathcal{S}}(\rho) = \mathcal{S}(\rho^\dagger)^\dagger$.

Lemma 3.7. *The map $\mathcal{S} \mapsto \widetilde{\mathcal{S}}$ is anti-linear, anti-unitary and $\widetilde{\mathcal{S}}_{ijk\ell} = \mathcal{S}_{k\ell ij}$.*

Proof. Clearly $\mathcal{S} \mapsto \widetilde{\mathcal{S}}$ is additive and to show it is anti-linear, we have for all $\lambda \in \mathbb{C}$

$$(\lambda\mathcal{S})^\sim(\rho) = \left[(\lambda\mathcal{S})(\rho^\dagger)\right]^\dagger = \lambda^*\mathcal{S}(\rho^\dagger)^\dagger = \lambda^*\widetilde{\mathcal{S}}(\rho)$$

Hence, $(\lambda\mathcal{S})^\sim = \lambda^*\widetilde{\mathcal{S}}$. To verify anti-unitary we have

$$\begin{aligned} \left\langle \widetilde{\mathcal{S}} \mid \widetilde{\mathcal{T}} \right\rangle &= \sum \mathrm{tr}\left(\widetilde{\mathcal{S}}(E_{rs})^\dagger \widetilde{\mathcal{T}}(E_{rs})\right) = \sum \mathrm{tr}\left(\mathcal{S}(E_{sr})\mathcal{T}(E_{sr})^\dagger\right) \\ &= \sum \mathrm{tr}\left(\mathcal{T}(E_{sr})^\dagger \mathcal{S}(E_{sr})\right) = \langle \mathcal{T} \mid \mathcal{S}\rangle = \langle \mathcal{S} \mid \mathcal{T}\rangle^* \end{aligned}$$

The last statement follows from

$$\widetilde{\mathcal{S}}_{ijk\ell}(\rho) = \left(|i\rangle\langle j|\rho^\dagger|\ell\rangle\langle k|\right)^\dagger = \langle j|\rho^\dagger\langle \ell|^*|k\rangle\langle i|$$
$$= \langle \ell|\rho|j\rangle\langle k|\langle i| = \mathcal{S}_{k\ell ij}(\rho) \qquad \square$$

Lemma 3.8. (i) *For* $S \in M_{mn}$ *we have* $(S^\dagger)^\wedge(E_{rs}) = \left[\widehat{S}(E_{sr})\right]^\dagger$. (ii) *For* $S \in M_{mn}$ *we have* $(S^\dagger)^\wedge = (\widehat{S})^\sim$.

Proof. (i) For $S = \sum a_{ijk\ell}|i\rangle|j\rangle\langle\ell|\langle k|$ we have

$$S^\dagger = \sum a_{ijk\ell}^*|k\rangle|\ell\rangle\langle j|\langle i|$$

Hence,

$$\begin{aligned}
(S^\dagger)^\wedge(E_{rs}) &= \sum a_{ijk\ell}^*|k\rangle\langle\ell|E_{rs}|j\rangle\langle i| \\
&= \sum a_{ijk\ell}^*|k\rangle\langle\ell|\left(|r\rangle\langle s|\right)|j\rangle\langle i| \\
&= \sum a_{iskr}^*|k\rangle\langle i| = \left(\sum a_{iskr}|i\rangle\langle k|\right)^\dagger \\
&= \left(\sum a_{ijk\ell}|i\rangle\langle j|\left(|s\rangle\langle r|\right)|\ell\rangle\langle k|\right)^\dagger \\
&= \left(\sum a_{ijk\ell}|i\rangle\langle j|E_{sr}|\ell\rangle\langle k|\right)^\dagger \\
&= \left[\widehat{S}(E_{sr})\right]^\dagger
\end{aligned}$$

(ii) Let $\rho = \sum c_{rs}E_{rs} \in M_n$ and apply (i) to obtain

$$\begin{aligned}
(S^\dagger)^\wedge(\rho) &= (S^\dagger)^\wedge\left(\sum c_{rs}E_{rs}\right) = \sum c_{rs}(S^\dagger)^\wedge(E_{rs}) \\
&= \sum c_{rs}\left[\widehat{S}(E_{sr})\right]^\dagger = \sum c_{rs}\left[\widehat{S}(E_{rs}^\dagger)\right]^\dagger \\
&= \left[\sum c_{rs}^*\widehat{S}(E_{rs}^\dagger)\right]^\dagger = \left[\widehat{S}\left(\sum c_{rs}^*E_{rs}^\dagger\right)\right]^\dagger \\
&= \left[\widehat{S}(\rho^\dagger)\right]^\dagger = (\widehat{S})^\sim(\rho)
\end{aligned}$$

Hence, $(S^\dagger)^\wedge = (\widehat{S})^\sim$. $\square$

We say that $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ is **hermitian-preserving** if $\mathcal{S}(\rho)$ is hermitian whenever ρ is hermitian.

Lemma 3.9. *$\mathcal{S}$ is hermitian-preserving if and only if $\mathcal{S}(E_{ij})^\dagger = \mathcal{S}(E_{ji})$ for all i, j.*

Proof. Suppose that $\mathcal{S}$ is hermitian-preserving. Since $E_{ij} + E_{ji}$ is hermitian we have that

$$\begin{aligned}\mathcal{S}(E_{ij})^\dagger + \mathcal{S}(E_{ji})^\dagger &= [\mathcal{S}(E_{ij} + E_{ji})]^\dagger = \mathcal{S}(E_{ij} + E_{ji}) \\ &= \mathcal{S}(E_{ij}) + \mathcal{S}(E_{ji})\end{aligned} \tag{3.5}$$

Since $i(E_{ij} - E_{ji})$ is hermitian we have that

$$\begin{aligned}-i\mathcal{S}(E_{ij})^\dagger + i\mathcal{S}(E_{ji})^\dagger &= [\mathcal{S}(iE_{ij} - iE_{ji})]^\dagger = \mathcal{S}(iE_{ij} - iE_{ji}) \\ &= i\mathcal{S}(E_{ij}) - i\mathcal{S}(E_{ji})\end{aligned}$$

Thus,

$$\mathcal{S}(E_{ij})^\dagger - \mathcal{S}(E_{ji})^\dagger = -\mathcal{S}(E_{ij}) + \mathcal{S}(E_{ji}) \tag{3.6}$$

Adding (3.5) and (3.6) gives $\mathcal{S}(E_{ij})^\dagger = \mathcal{S}(E_{ji})$.

Conversely, suppose that $\mathcal{S}(E_{ij})^\dagger = \mathcal{S}(E_{ji})$ for every i, j. If $\rho = \sum a_{ij} E_{ij}$ is hermitian, we have that

$$\begin{aligned}\mathcal{S}(\rho)^\dagger &= \left[\sum a_{ij}\mathcal{S}(E_{ij})\right]^\dagger = \sum a_{ij}^*\mathcal{S}(E_{ij})^\dagger = \sum a_{ji}\mathcal{S}(E_{ji}) \\ &= \mathcal{S}(\rho)\end{aligned}$$

Hence, $\mathcal{S}(\rho)$ is hermitian so $\mathcal{S}$ is hermitian-preserving. □

Theorem 3.10. *For $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ the following statements are equivalent.* (i) *$\mathcal{S}$ is hermitian-preserving.* (ii) *$\mathcal{S}(\rho)^\dagger = \mathcal{S}(\rho^\dagger)$ for every $\rho = M_n$.* (iii) *$\mathcal{S} = \widetilde{\mathcal{S}}$.* (iv) *$\mathcal{S} = \widehat{S}$ where $S \in \mathrm{Herm}_{mn}$.*

Proof. (i) ⇒ (ii) Suppose $\mathcal{S}$ is hermitian-preserving and $\rho = \sum c_{ij} E_{ij}$. Then by Lemma 3.9

$$\begin{aligned}\mathcal{S}(\rho^\dagger) &= \sum c_{ij}^*\mathcal{S}(E_{ji}) = \sum c_{ij}^*\left[\mathcal{S}(E_{ij})\right]^\dagger = \left[\sum c_{ij}\mathcal{S}(E_{ij})\right]^\dagger \\ &= \mathcal{S}(\rho)^\dagger\end{aligned}$$

(ii) ⇒ (iii) If (ii) holds, then for every $\rho \in M_n$ we have that

$$\widetilde{\mathcal{S}}(\rho) = \mathcal{S}(\rho^\dagger)^\dagger = \left[\mathcal{S}(\rho)^\dagger\right]^\dagger = \mathcal{S}(\rho)$$

(iii) $\Rightarrow$ (iv) By Corollary 3.2 $\mathcal{S} = \widehat{S}$ for some $S \in M_{mn}$. If (iii) holds then by Lemma 3.8(ii) we have that

$$(S^\dagger)^\wedge = (\widehat{S})^\sim = \widetilde{\mathcal{S}} = \mathcal{S} = \widehat{S}$$

Since $^\wedge$ is injective, $S = S^\dagger$ so S is hermitian.
(iv) $\Rightarrow$ (i) Suppose (iv) holds and $\rho \in \mathrm{Herm}_n$. Then by Lemma 3.8(ii) we have that

$$\mathcal{S}(\rho)^\dagger = \widehat{S}(\rho)^\dagger = \widehat{S}(\rho^\dagger)^\dagger = (\widehat{S})^\sim(\rho) = (S^\dagger)^\wedge(\rho) = \widehat{S}(\rho) = \mathcal{S}(\rho)$$

Hence, $\mathcal{S}(\rho)$ is hermitian so that $\mathcal{S}$ is hermitian-preserving. $\square$

Corollary 3.11. (i) *Any $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ has a unique representation $\mathcal{S} = \mathcal{S}_1 + i\mathcal{S}_2$ where $\mathcal{S}_1, \mathcal{S}_2 \in \mathrm{End}(M_n, M_m)$ are hermitian-preserving.* (ii) *Any $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ has a unique representation $\mathcal{S} = \widehat{S} + i\widehat{T}$ where $S, T \in \mathrm{Herm}_{mn}$.*

Proof. (i) If $\mathcal{S} = \mathcal{S}_1 + i\mathcal{S}_2$ where $\mathcal{S}_1, \mathcal{S}_2 \in \mathrm{End}(M_n, M_m)$ are hermitian-preserving, then by Lemma 3.7 and Theorem 3.10 we have that

$$\widetilde{\mathcal{S}} = \widetilde{\mathcal{S}}_1 - i\widetilde{\mathcal{S}}_2 = \mathcal{S}_1 - i\mathcal{S}_2$$

We conclude that $\mathcal{S}_1 = (\mathcal{S} + \widetilde{\mathcal{S}})/2$ and $\mathcal{S}_2 = (\mathcal{S} - \widetilde{\mathcal{S}})/2i$. Since the right sides of these equations are hermitian-preserving, this proves existence and uniqueness. (ii) This follows from (i) and Theorem 3.10. $\square$

We denote by $\mathcal{E}(\mathbb{C}^d)$ the set of all $S \in M_d^+$ with $S \leq I_d$ and call $\mathcal{E}(\mathbb{C}^d)$ the set of **quantum effects** [3, 5, 6, 7, 9, 10, 14]. We have seen in Theorem 3.10(iv) that $\mathcal{S}$ is hermitian-preserving if and only if $\mathcal{S}^\vee \in \mathrm{Herm}_{mn}$. The next result characterizes other properties of $\mathcal{S}$ in terms of properties of $\mathcal{S}^\vee$.

Theorem 3.12. *Let $\mathcal{S} \in \mathrm{End}(M_n, M_m)$.* (i) *$\mathcal{S}(\rho) = \sum \widehat{A}_i \rho \widehat{A}_i^\dagger$ with $\mathrm{tr}(\widehat{A}_i^\dagger \widehat{A}_j) = 0$, $i \neq j$, if and only if $\mathcal{S}^\vee \in \mathrm{Herm}_{mn}^+$.* (ii) *$\mathcal{S}(\rho) = \sum \widehat{A}_i \rho \widehat{A}_i^\dagger$ with $\mathrm{tr}(\widehat{A}_i^\dagger \widehat{A}_j) = \delta_{ij}$ if and only if $\mathcal{S}^\vee$ is an orthogonal projection.* (iii) *$\mathcal{S}(\rho) = \sum \widehat{A}_i \rho \widehat{A}_i^\dagger$ with $\mathrm{tr}(\widehat{A}_i^\dagger A_j) = 0$, $i \neq j$ and $\mathrm{tr}(\widehat{A}_i^\dagger \widehat{A}_i) \leq 1$ if and only if $\mathcal{S}^\vee \in \mathcal{E}(\mathbb{C}^{mn})$.* (iv) *$\mathcal{S}(\rho) = \mathrm{tr}(\rho) I_m$ if and only if $\mathcal{S}^\vee = I_{mn}$.*

Proof. (i) By the spectral theorem $\mathcal{S}^\vee \in \mathrm{Herm}_{mn}^+$ if and only if $\mathcal{S}^\vee = \sum A_i A_i^\dagger$ where $A_i \in \mathbb{C}^{mn}$ and $A_i \perp A_j$ for $i \neq j$. Applying Theorem 3.3(i) this is equivalent to $\mathcal{S}(\rho) = \sum \widehat{A}_i \rho \widehat{A}_i^\dagger$ with $\operatorname{tr}(\widehat{A}_i^\dagger \widehat{A}_j) = 0$, $i \neq j$. (ii) By the spectral theorem $\mathcal{S}^\vee \in M_{mn}$ is an orthogonal projection if and only if $\mathcal{S}^\vee = \sum A_i A_i^\dagger$ where $A_i \in \mathbb{C}^{mn}$ and $\langle A_i \mid A_j \rangle = \delta_{ij}$. Applying Theorem 3.3(i) this is equivalent to $\mathcal{S}(\rho) = \sum \widehat{A}_i \rho \widehat{A}_i^\dagger$ where $\operatorname{tr}(\widehat{A}_i^\dagger \widehat{A}_j) = \delta_{ij}$. (iii) This is similar to the proof of (i). (iv) $\mathcal{S}(\rho) = \operatorname{tr}(\rho) I_m$ if and only if

$$\mathcal{S}(\rho) = \sum |i\rangle\langle j|\rho|j\rangle\langle i| = \sum \mathcal{S}_{ijij}(\rho)$$

Since $I_{mn} = \sum |i\rangle|j\rangle\langle i|\langle j|$ we have that

$$\sum \mathcal{S}_{ijij} = \sum \widehat{S}_{ijij} = \sum \left(|i\rangle|j\rangle\langle i|\langle j|\right)^\wedge = \widehat{I}_{mn}$$

Hence, $\mathcal{S}^\vee = I_{mn}$. □

If $\mathcal{S} \in \operatorname{End}(M_n, M_m)$, $\mathcal{T} \in \operatorname{End}(M_r, M_s)$ we define $\mathcal{S} \otimes \mathcal{T} \in \operatorname{End}(M_{nr}, M_{ms})$ by

$$\mathcal{S} \otimes \mathcal{T}(\rho \otimes \sigma) = \mathcal{S}(\rho) \otimes \mathcal{S}(\sigma)$$

$\rho \in M_n$, $\sigma \in M_r$ and extend by linearity.

Lemma 3.13. (i) $(\mathcal{S} \otimes \mathcal{T})^\sim = \widetilde{\mathcal{S}} \otimes \widetilde{\mathcal{T}}$. (ii) *If $\mathcal{S}$ and $\mathcal{T}$ are hermitian-preserving, then so is $\mathcal{S} \otimes \mathcal{T}$.*

Proof. (i) For $\rho \in M_n$, $\sigma \in M_r$ we have that

$$\begin{aligned}(\mathcal{S} \otimes \mathcal{T})^\sim(\rho \otimes \sigma) &= (\mathcal{S} \otimes \mathcal{T})(\rho^\dagger \otimes \sigma^\dagger)^\dagger = \left[\mathcal{S}(\rho^\dagger) \otimes \mathcal{T}(\rho^\dagger)\right]^\dagger \\ &= \mathcal{S}(\rho^\dagger)^\dagger \otimes \mathcal{T}(\sigma^\dagger)^\dagger = \widetilde{\mathcal{S}}(\rho) \otimes \widetilde{\mathcal{T}}(\sigma) \\ &= (\widetilde{\mathcal{S}} \otimes \widetilde{\mathcal{T}})(\rho \otimes \sigma)\end{aligned}$$

The result follows by linearity. (ii) Since $\mathcal{S}$ and $\mathcal{T}$ are hermitian-preserving, by Theorem 3.10, $\mathcal{S} = \widetilde{\mathcal{S}}$ and $\mathcal{T} = \widetilde{\mathcal{T}}$. Applying (i) we obtain

$$(\mathcal{S} \otimes \mathcal{T})^\sim = \widetilde{\mathcal{S}} \otimes \widetilde{\mathcal{T}} = \mathcal{S} \otimes \mathcal{T}$$

and the result follows from Theorem 3.10. □

Corollary 3.14. *If $\mathcal{S} \in \operatorname{End}(M_n, M_m)$ is hermitian-preserving then so is $\mathcal{S} \otimes \mathcal{I}_r \in \operatorname{End}(M_{nr}, M_{mr})$.*

4 Positive-Preserving Endomorphisms

We say that $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ is **positive-preserving** if $\mathcal{S}(\rho) \in \mathrm{Herm}_m^+$ for every $\rho \in \mathrm{Herm}_n^+$. Positive-preserving endomorphisms are important because they map states into state. However, they are not as important in applications as quantum operations which have the property that $\mathcal{S} \otimes \mathcal{I}_r$ is positive-preserving for every $r \in \mathbb{N}$. We shall consider quantum operations in Section 5. A positive-preserving endomorphism $\mathcal{S}$ is hermitian-preserving. Indeed, any $\rho \in \mathrm{Herm}_n$ has the form $\rho_1 - \rho_2$ where $\rho_1, \rho_2 \in \mathrm{Herm}_n^+$. Hence,

$$\mathcal{S}(\rho) = \mathcal{S}(\rho_1 - \rho_2) = \mathcal{S}(\rho_1) - \mathcal{S}(\rho_2) \in \mathrm{Herm}_m$$

so that $\mathcal{S}$ is hermitian-preserving.

In contrast to Corollary 3.14, if $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ is positive-preserving, then $\mathcal{S} \otimes \mathcal{I}_r \in \mathrm{End}(M_{nr}, M_{mr})$ need not be positive-preserving. The standard example for this is $\mathcal{S} \in \mathrm{End}(M_2, M_2)$ given by $\mathcal{S}(\rho) = \rho^t$. It is clear that $\mathcal{S}$ is positive-preserving. To show that $\mathcal{S} \otimes \mathcal{I}_2 \in \mathrm{End}(M_4, M_4)$ is not positive-preserving, let $|0\rangle, |1\rangle$ be the canonical basis for $\mathbb{C}^2$ and let $|xy\rangle = |x\rangle|y\rangle$ for $x, y \in \{0, 1\}$. Define the entangled states $|\alpha\rangle, |\beta\rangle \in \mathbb{C}^4$ by $|\alpha\rangle = |01\rangle - |10\rangle$, $|\beta\rangle = |00\rangle + |11\rangle$. Then $|\beta\rangle\langle\beta| \in \mathrm{Herm}_4^+$ and we have that

$$\begin{aligned}
\mathcal{S} \otimes \mathcal{I}_2 \left(|\beta\rangle\langle\beta|\right) &= \mathcal{S} \otimes \mathcal{I}_2 \left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right) \\
&= \mathcal{S} \otimes \mathcal{I}_2 \left(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1|\right. \\
&\quad \left. + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\right) \\
&= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| \\
&\quad + |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \\
&= |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|
\end{aligned}$$

But then

$$\begin{aligned}
&\langle\alpha|\mathcal{S} \otimes \mathcal{I}_2 \left(|\beta\rangle\langle\beta|\right)|\alpha\rangle \\
&\quad = \langle\alpha \mid 00\rangle\langle 00 \mid \alpha\rangle + \langle\alpha \mid 10\rangle\langle 01 \mid \alpha\rangle + \langle\alpha \mid 01\rangle\langle 10 \mid \alpha\rangle + \langle\alpha \mid 11\rangle\langle 11 \mid \alpha\rangle \\
&\quad = 0 + (-1) + (-1) + 0 = -2
\end{aligned}$$

Hence, $\mathcal{S} \otimes \mathcal{I}_2 \left(|\beta\rangle\langle\beta|\right) \notin \mathrm{Herm}_4^\dagger$.

We shall need the following two technical results. The first result shows that tr_1 and $^\wedge$ commute in a certain sense.

Lemma 4.1. *If $S \in M_{rmn}$ then $[\mathrm{tr}_1(S)]^\wedge = \mathrm{tr}_1 \circ \widehat{S}$, where tr_1 is the partial trace over the r-dimensional system.*

Proof. Let $|i\rangle, |k\rangle \in \mathbb{C}^m$, $|j\rangle, |\ell\rangle \in \mathbb{C}^n$, $|p\rangle, |q\rangle \in \mathbb{C}^r$ be elements of the corresponding canonical bases. Letting $\rho \in M_n$ we have that

$$\widehat{S}(\rho) = \sum S_{ijk\ell pq} |p\rangle|i\rangle\langle j|\rho|\ell\rangle\langle k|\langle q| \in M_{rm}$$

Then

$$(\mathrm{tr}_1 \circ \widehat{S})(\rho) = \sum S_{ijk\ell pp} \langle j|\rho|\ell\rangle|i\rangle\langle k| \in M_m$$

On the other hand

$$\mathrm{tr}_1(S) = \sum S_{ijk\ell pp} |i\rangle|j\rangle\langle \ell|\langle k|$$

so that

$$[\mathrm{tr}_1(S)]^\wedge(\rho) = \sum S_{ijk\ell pp} |i\rangle\langle j|\rho|\ell\rangle\langle k| = (\mathrm{tr}_1 \circ \widehat{S})(\rho)$$ □

Lemma 4.2. *For $S \in M_{mn}$, $\rho, \sigma \in M_n$, $\mu, \nu \in M_m$ we have that*

$$\mu\widehat{S}(\rho\sigma)\nu = \mathrm{tr}_2\left[(\mu \otimes \rho^t) S (\nu \otimes \sigma^t)\right]$$

Proof. We can write

$$\mu \otimes \rho^t = \sum \mu_{ij}\rho_{\ell k} |i\rangle\langle j| \otimes |k\rangle\langle \ell|$$
$$\nu \otimes \sigma^t = \sum \nu_{i'j'}\sigma_{\ell' k'} |i'\rangle\langle j'| \otimes |k'\rangle\langle \ell'|$$

Letting $S = \sum S_{rstu}|r\rangle|s\rangle\langle t|\langle u|$, we obtain

$$(\mu \otimes \rho^t) S (\nu \otimes \sigma^t) = \sum \mu_{ij}\rho_{\ell k} S_{j\ell k' i'} \nu_{i'j'}\sigma_{\ell' k'} |i\rangle|k\rangle\langle j'|\langle \ell'|$$

Hence,

$$\mathrm{tr}_2\left[(\mu \otimes \rho^t) S (\nu \otimes \sigma^t)\right] = \sum \mu_{ij}\rho_{\ell k} S_{j\ell k' i'} \nu_{i'j'}\sigma_{kk'} |i\rangle\langle j'|$$

On the other hand, we have that

$$\widehat{S}(\rho\sigma) = \widehat{S}\left(\sum \rho_{\ell k}\sigma_{kk'} |\ell\rangle\langle k'|\right) = \sum S_{r\ell k' u}\rho_{\ell k}\sigma_{kk'} |r\rangle\langle u|$$

Hence,

$$\begin{aligned}\mu\widehat{S}(\rho\sigma)\nu &= \sum \mu_{ij}|i\rangle\langle j|\widehat{S}(\rho\sigma)\sum \nu_{i'j'}|i'\rangle\langle j'| \\ &= \sum \mu_{ij}\rho_{\ell k} S_{j\ell k' i'}\nu_{i'j'}\sigma_{kk'} |i\rangle\langle j'|\end{aligned}$$ □

Corollary 4.3. *For $S \in M_{mn}$, $\rho \in M_m$, $\mu \in M_m$ we have that*

$$\operatorname{tr}\left(\mu\widehat{S}(\rho)\right) = \operatorname{tr}\left((\mu \otimes \rho^t)S\right)$$

Proof. In Lemma 4.2 let $\nu = I_m$, $\sigma = I_n$ and take the total trace to obtain

$$\operatorname{tr}\left(\mu\widehat{S}(\rho)\right) = \operatorname{tr}\left[\operatorname{tr}_2(\mu \otimes \rho^t)S\right] \qquad \square$$

A state $\rho \in \mathrm{Herm}_{mn}^+$ is **separable** if it has the form $\rho = \sum \lambda_i \rho_i \otimes \sigma_i$ for $\lambda_i \geq 0$, $\rho_i \in \mathrm{Herm}_m^+$, $\sigma_i \in \mathrm{Herm}_n^+$.

Theorem 4.4. *A map $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ is positive-preserving if and only if $\mathcal{S}^\vee \in \mathrm{Herm}_{mn}$ and $\operatorname{tr}(\rho\mathcal{S}^\vee) \geq 0$ for every separable state ρ.*

Proof. By Theorem 3.12, $\mathcal{S}^\vee \in \mathrm{Herm}_{mn}$. Now $\mathcal{S}$ is positive-preserving if and only if $\operatorname{tr}\left(\mu\mathcal{S}(\rho)\right) \geq 0$ for every $\rho \in \mathrm{Herm}_n^+$, $\mu \in \mathrm{Herm}_m^+$. By Corollary 4.3, this is equivalent to $\operatorname{tr}\left((\mu \otimes \rho^t)\mathcal{S}^\vee\right) \geq 0$. But this last inequality is equivalent to $\operatorname{tr}(\rho\mathcal{S}^\vee) \geq 0$ for every separable state ρ. $\square$

A map $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ is **trace-preserving** if $\operatorname{tr}\left[\mathcal{S}(\rho)\right] = \operatorname{tr}(\rho)$ for all $\rho \in M_n$ and $\mathcal{S}$ is **unital** if $\mathcal{S}(I_n) = I_m$.

Theorem 4.5. (i) *$\mathcal{S}$ is trace-preserving if and only if $\operatorname{tr}_1(\mathcal{S}^\vee) = I_n$.* (ii) *$\mathcal{S}$ is unital if and only if $\operatorname{tr}_2(\mathcal{S}^\vee) = I_m$.*

Proof. (i) Suppose $\mathcal{S}^\vee = \sum s_{ij} A_i B_j^\dagger$ for $A_i, B_j \in \mathbb{C}^{mn}$. Then for every $\rho \in M_n$ we have that

$$\operatorname{tr}\left(\mathcal{S}(\rho)\right) = \operatorname{tr}\left(\sum s_{ij}\widehat{A}_i\rho\widehat{B}_j^\dagger\right) = \operatorname{tr}\left(\sum s_{ij}\widehat{B}_j^\dagger A_i\rho\right)$$

Hence, $\operatorname{tr}\left(\mathcal{S}(\rho)\right) = \operatorname{tr}(\rho)$ for every $\rho \in M_n$ if and only if $\sum s_{ij}\widehat{B}_j^\dagger\widehat{A}_i = I_n$. Applying Lemma 2.5 this latter condition is equivalent to

$$\begin{aligned} I_n &= \left(\sum s_{ij}\widehat{B}_j^\dagger\widehat{A}_i\right)^t = \sum s_{ij}(\widehat{B}_j^\dagger\widehat{A}_i)^t = \sum s_{ij}\operatorname{tr}_1(A_iB_j^\dagger) \\ &= \operatorname{tr}_1\left(\sum s_{ij}A_iB_j^\dagger\right) = \operatorname{tr}_1(\mathcal{S}^\vee) \end{aligned}$$

(ii) Again, suppose that $\mathcal{S}^\vee = \sum s_{ij}A_iB_j^\dagger$ for $A_i, B_j \in \mathbb{C}^{mn}$. Then by Lemma 2.5, $\mathcal{S}(I_n) = I_m$ if and only if

$$\begin{aligned} I_m &= \sum s_{ij}\widehat{A}_i\widehat{B}_j^\dagger = \sum s_{ij}\operatorname{tr}_2(A_iB_j^\dagger) = \operatorname{tr}_2\left(\sum s_{ij}A_iB_j^\dagger\right) \\ &= \operatorname{tr}_2(\mathcal{S}^\vee) \end{aligned} \qquad \square$$

5 Quantum Operations

A map $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ is **completely positive** if for every $r \in \mathbb{N}$ and every $\rho \in \mathrm{Herm}^+_{mr}$ we have $\mathcal{S} \otimes \mathcal{I}_r(\rho) \in \mathrm{Herm}^+_{mr}$. Thus, $\mathcal{S}$ is completely positive if and only if $\mathcal{S} \otimes \mathcal{I}_r$ is positive-preserving for every $r \in \mathbb{N}$. It follows by definition that $\mathcal{S}$ is positive-preserving if $\mathcal{S}$ is completely positive. However, we have seen in Section 4 that the converse does not hold. A completely positive endomorphism is also called a **quantum operation** [2, 3, 5, 14, 15, 16]. We have already mentioned that quantum operations are important in quantum computation, quantum information and quantum measurement theory. Quantum operations are sometimes assumed to be trace-preserving or unital, but for generality we shall not make these assumptions here.

Theorem 5.1. *If $\mathcal{S}\colon M_n \to M_m$, then the following statements are equivalent.* (i) *$\mathcal{S}$ is a quantum operation* (ii) $\mathcal{S}^\vee \in \mathrm{Herm}^+_{mn}$. (iii) $\mathcal{S}(\rho) = \sum \widehat{A}_t \rho \widehat{A}_t^\dagger$, $A_i \in \mathbb{C}^{mn}$.

Proof. (i) $\Rightarrow$ (ii) Suppose $\mathcal{S}$ is a quantum operation. Since $|\beta\rangle\langle\beta| \in \mathrm{Herm}^+_{m^2}$, applying Lemma 3.6 we have

$$\mathcal{S}^\vee = (\mathcal{S} \otimes \mathcal{I}_n)\left(|\beta\rangle\langle\beta|\right) \in \mathrm{Herm}^+_{mn}$$

(ii) $\Rightarrow$ (iii) Since $\mathcal{S}^\vee \in \mathrm{Herm}^+_{mn}$ by Theorem 3.12(i) there exist $A_t \in \mathbb{C}^{mn}$ such that $\mathcal{S}(\rho) = \sum \widehat{A}_t \rho \widehat{A}_t^\dagger$.
(iii) $\Rightarrow$ (i) If (iii) holds then clearly $\mathcal{S} \in \mathrm{End}(M_n, M_m)$. If $\rho \in \mathrm{Herm}^+_{mr}$ we can write

$$\rho = \sum a_{ijk\ell} |i\rangle|j\rangle\langle k|\langle\ell|$$

where $|i\rangle$, $|k\rangle$ are elements of the basis of $\mathbb{C}^n$ and $|j\rangle$, $|\ell\rangle$ are elements of the basis of $\mathbb{C}^r$. We then have that

$$\begin{aligned}\rho &= \sum a_{ijk\ell}|i\rangle\langle k| \otimes |j\rangle\langle\ell| = \sum_{j,\ell}\left(\sum_{i,k} a_{ijk\ell}|i\rangle\langle k|\right) \otimes |j\rangle\langle\ell| \\ &= \sum_{j,\ell} T_{j\ell} \otimes |j\rangle\langle\ell|\end{aligned}$$

where $T_{j\ell} = \sum_{i,k} a_{ijk\ell}|i\rangle\langle k| \in M_n$. Hence,

$$(\mathcal{S} \otimes \mathcal{I}_r)(\rho) = \sum_{j,\ell} \mathcal{S}(T_{j\ell}) \otimes |j\rangle\langle\ell| = \sum_{j,\ell}\sum_t \widehat{A}_t T_{j\ell} \widehat{A}_t^\dagger \otimes |j\rangle\langle\ell|$$

Now by the Schmidt decomposition theorem [15, 16] any $|\psi\rangle \in \mathbb{C}^{mr}$ has the form $|\psi\rangle = \sum |u_s\rangle|v_s\rangle$ for $|u_s\rangle \in \mathbb{C}^m$, $|v_s\rangle \in \mathbb{C}^r$. We then have that

$$(\mathcal{S} \otimes \mathcal{I}_r)(\rho)|\psi\rangle = \sum \widehat{A}_t T_{j\ell} \widehat{A}_t^\dagger \langle \ell \mid v_s\rangle |u_s\rangle\langle j|$$

Defining $|\psi_t\rangle = \sum_i A_t^\dagger |u_i\rangle \otimes |v_i\rangle$ we obtain

$$\begin{aligned}\langle\psi|(\mathcal{S} \otimes \mathcal{I}_r)(\rho)|\psi\rangle &= \sum \langle u_i|\widehat{A}_t T_{j\ell} \widehat{A}_t^\dagger|u_s\rangle\langle \ell \mid v_s\rangle\langle v_i \mid j\rangle \\ &= \sum_{i,s,t} \left\langle \widehat{A}_t^\dagger u_i \otimes v_i \middle| \sum_{j,\ell} T_{j\ell} \otimes |j\rangle\langle\ell| \middle| \widehat{A}_t^\dagger u_s \otimes v_s \right\rangle \\ &= \sum \langle\psi_t|\rho|\psi_t\rangle \geq 0\end{aligned}$$

Hence, $(\mathcal{S} \otimes \mathcal{I}_r)(\rho)$ is positive so that $\mathcal{S}$ is a quantum operation. □

Theorem 5.1 shows that any quantum operation $\mathcal{S} \colon M_n \to M_m$ has the form

$$\mathcal{S}(\rho) = \sum A_i \rho A_i^\dagger \tag{5.1}$$

where $A_i \in \mathrm{End}(\mathbb{C}^n, \mathbb{C}^m)$. We call (5.1) an **operator-sum representation** of $\mathcal{S}$ and we call A_i the **operation elements** for the representation [13, 14]. We now show that the operation-sum representation (5.1) is not unique. That is, the operation elements for a quantum operation are not unique. Let $\mathcal{S}, \mathcal{T} \colon M_2 \to M_2$ be the quantum operations with the operator-sum representations

$$\begin{aligned}\mathcal{S}(\rho) &= A_1 \rho A_1^\dagger + A_2 \rho A_2^\dagger \\ \mathcal{T}(\rho) &= B_1 \rho B_1^\dagger + B_2 \rho B_2^\dagger\end{aligned}$$

where $A_1 = 2^{-1/2}\mathrm{diag}(1,1)$ $A_2 = 2^{-1/2}\mathrm{diag}(1,-1)$, $B_1 = \mathrm{diag}(1,0)$, $B_2 = \mathrm{diag}(0,1)$. Although $\mathcal{S}$ and $\mathcal{T}$ appear to be quite different, they are actually the same quantum operation. To see this , note that $B_1 = 2^{-1/2}(A_1 + A_2)$ and $B_2 = 2^{-1/2}(A_1 - A_2)$. Thus,

$$\begin{aligned}\mathcal{T}(\rho) &= \frac{(A_1 + A_2)\rho(A_1 + A_2) + (A_1 - A_2)\rho(A_1 - A_2)}{2} \\ &= A_1 \rho A_1 + A_2 \rho A_2 = \mathcal{S}(\rho)\end{aligned}$$

Notice that in this example we could write $B_i = \sum u_{ij} A_j$ where $[u_{ij}]$ is the unitary matrix

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

In this sense, the two sets of operation elements are related by a unitary matrix. The next theorem shows that this is a general result.

Theorem 5.2. *Suppose $\{E_1, \dots, E_n\}$ and $\{F_1, \dots, F_m\}$ are operation elements giving rise to quantum operations $\mathcal{S}$ and $\mathcal{T}$, respectively. By appending zero operators to the shorter list of operation elements we may assume that $m = n$. Then $\mathcal{S} = \mathcal{T}$ if and only if there exist complex numbers u_{ij} such that $F_i = \sum_j u_{ij} E_j$ where$[u_{ij}]$ is an $m \times m$ unitary matrix.*

Proof. By Theorem 2.1 we may assume that $E_i = \widehat{A}_i$ and $F_i = \widehat{B}_i$ and by Lemma 4.1, $\mathcal{S} = \widehat{S}, \mathcal{T} = \widehat{T}$ where $S = \sum A_i A_i^\dagger$ and $T = \sum B_i B_i^\dagger$. Then $\mathcal{S} = \mathcal{T}$ if and only if $S = T$. Applying Lemma 2.3, $S = T$ if and only if there exists a unitary matrix $[u_{ij}]$ such that $B_i = \sum u_{ij} A_j$. The last condition is equivalent to

$$F_i = \widehat{B}_i = \sum u_{ij} \widehat{A}_j = \sum u_{ij} E_i \qquad \square$$

Let $\mathcal{S}$ have operation elements $\{A_1, \dots, A_r\}$. We say that $\{A_1, \dots, A_r\}$ is **orthogonal** if $\langle A_i \mid A_j \rangle = \mathrm{tr}(A_i^\dagger A_j) = 0$ for $i \neq j$, and is orthonormal if $\langle A_i \mid A_j \rangle = \delta_{ij}$, $i, j = 1, \dots, r$. We use the notation $\|A_i\| = \langle A_i \mid A_i \rangle^{1/2}$.

Theorem 5.3. (i) *Any quantum operation has an orthogonal set of operation elements.* (ii) *If $\{A_1, \dots, A_r\}$ is an orthogonal set of operation elements with $\|A_i\| = \|A_j\| \neq 0$, $i, j = 1, \dots, r$, and $\{B_1, \dots, B_s\}$ is another set of operation elements for the same quantum operation with $s \leq r$, then $\{B_1, \dots, B_s\}$ is orthogonal, $s = r$ and $\|B_i\| = \|A_i\|$, $i = 1, \dots, r$.* (iii) *If $\{A_1, \dots, A_r\}$ is an orthonormal set of operation elements and $\{B_1, \dots, B_r\}$ is a set of operation elements for the same quantum operation, then $\{B_1, \dots, B_r\}$ is orthonormal.*

Proof. (i) This follows from Theorem 3.12(i). (ii) By Theorem 5.2 there exists a unitary matrix $[u_{ij}]$ such that $B_i = \sum u_{ij} A_j$. We then have that

$$\langle A_k \mid B_i \rangle = \mathrm{tr}(A_k^\dagger B_i) = u_{ik} \mathrm{tr}(A_k^\dagger A_k) = u_{ik} \|A_k\|^2$$

Hence, $u_{ik} = \langle A_k \mid B_i \rangle / \|A_k\|^2$. Since $[u_{ij}]$ is unitary, for $i \neq j$ we obtain

$$\begin{aligned}
0 &= \sum_k u_{ik} u_{jk}^* = \sum_k \frac{\langle A_k \mid B_i \rangle}{\|A_k\|^2} \frac{\langle B_j \mid A_k \rangle}{\|A_k\|^2} \\
&= \frac{1}{\|A_1\|^2} \sum_k \langle B_j \mid A_k' \rangle \langle A_k' \mid B_i \rangle
\end{aligned}$$

where A_k' is the unit norm operator $A_k/\|A_k\|$. It follows from Parseval's equality that $\langle B_j \mid B_i \rangle = 0$ for $i \neq j$. Moreover,

$$1 = \sum_k u_{ik} u_{ik}^* = \frac{1}{\|A_1\|^2} \sum_k \langle B_i \mid A_k' \rangle \langle A_k' \mid B_k \rangle = \frac{\|B_i\|^2}{\|A_1\|^2}$$

so that $\|B_i\|^2 = \|A_1\|^2$. Notice that $s = r$ because $\{B_i\}$ and $\{A_i\}$ form a basis for the same space. (iii) This follows from (ii). □

Examples. The bit flip channel is described by the trace-preserving quantum operation with operation elements $\left\{ p^{1/2} I_2, (1-p)^{1/2} X \right\}$ where $0 < p < 1$ and X is the Pauli matrix

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Notice that if $p = 1/2$ the operation elements are orthonormal and if $p \neq 1/2$ they are orthogonal.

The quantum operation with operation elements

$$\left\{ pI_2, \sqrt{p(1-p)}\, X, \sqrt{p(1-p)}\, Z, (1-p)Y \right\}$$

where Y, Z are the Pauli matrices

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

is trace-preserving. The operation elements are orthogonal and if $p = 1/2$ they all have norm $1/\sqrt{2}$.

Theorem 5.4. *Let $\mathcal{S} \colon M_n \to M_m$ be a quantum operation with operation elements $\{A_1, \ldots, A_r\}$.* (a) *The following statements are equivalent.* (i) *$\mathcal{S}$ is trace-preserving.* (ii) $\mathrm{tr}_1(\mathcal{S}^\vee) = I_n$. (iii) $\sum A_i^\dagger A_i = I_n$. (b) *The following statements are equivalent.* (i) *$\mathcal{S}$ is unital.* (ii) $\mathrm{tr}_2(S) = I_m$. (iii) $\sum A_i A_i^\dagger = I_m$.

Proof. (a)(i)and (ii) are equivalent by Theorem 4.5. If $\mathcal{S}$ is trace-preserving then for every $\rho \in M_n$ we have that

$$\operatorname{tr}(\rho) = \operatorname{tr}\left(\sum A_i \rho A_i^\dagger\right) = \operatorname{tr}\left(\sum A_i^\dagger A_i \rho\right)$$

which implies that $\sum A_i^\dagger A_i = I_n$. Conversely, suppose that $\sum A_i^\dagger A_i = I_n$. Then for every $\rho \in M_n$ we have that

$$\operatorname{tr}\left(\mathcal{S}(\rho)\right) = \operatorname{tr}\left(\sum A_i \rho A_i^\dagger\right) = \operatorname{tr}\left(\sum A_i^\dagger A_i \rho\right) = \operatorname{tr}(\rho)$$

(b) Again (i) and (ii) are equivalent by Theorem 4.5. Now $\mathcal{S}$ is unital if and only if

$$I_m = \mathcal{S}(I_n) = \sum A_i A_i^\dagger \qquad \square$$

The next result shows the interesting fact that traces and partial traces are completely positive.

Lemma 5.5. (i) *The map* $\operatorname{tr}\colon M_n \to M_1$ *is a trace-preserving quantum operation.* (ii) *The map* $\operatorname{tr}_1\colon M_{mn} \to M_n$ *is a trace-preserving quantum operation.*

Proof. (i) We understand M_1 to be the set of matrices on a one-dimensional Hilbert space spanned by a unit vector $|0\rangle$. Thus, $M_1 = \{\lambda|0\rangle\langle 0|\colon \lambda \in \mathbb{C}\}$. Then

$$\operatorname{tr}(\rho)|0\rangle\langle 0| = \sum_{i=1}^{n} |0\rangle\langle i|\rho|i\rangle\langle 0|$$

so $\operatorname{tr}(\rho)$ is a quantum operation with operation elements $|0\rangle\langle i|$. Since

$$\sum \left(|i\rangle\langle 0|\right)\left(|0\rangle\langle i|\right) = \sum |i\rangle\langle i| = I_n$$

tr is trace-preserving.
(ii) Define $A_i\colon \mathbb{C}^{mn} \to \mathbb{C}^n$ by

$$A_i\left(\sum c_{k\ell}|k\rangle|\ell\rangle\right) = \sum_{\ell} c_{i\ell}|\ell\rangle = \langle i|\sum c_{k\ell}|k\rangle|\ell\rangle$$

In a sense, $A_i = \langle i|$. Define $\mathcal{S}\colon M_{mn} \to M_n$ by $\mathcal{S}(\rho) = \sum A_i \rho A_i^\dagger$. We then have for every $\rho \in M_n$ that

$$\begin{aligned}\mathcal{S}\left(|i\rangle\langle i'| \otimes \rho\right) &= \sum A_j \left(|i\rangle\langle i'| \otimes \rho\right) A_j^\dagger \\ &= \delta_{ii'}\rho = \operatorname{tr}_1\left(|i\rangle\langle i'| \otimes \rho\right)\end{aligned}$$

By linearity of $\mathcal{S}$ and tr_1 it follows that $\mathcal{S} = \operatorname{tr}_1$. Hence, tr_1 is a quantum operation with operation elements A_i. To show that $\mathcal{S}$ is trace-preserving we have that

$$\sum A_i^\dagger A_i = \sum |i\rangle\langle i| = I_{mn} \qquad \square$$

In the theory of quantum information, quantum noise is frequently described by a trace-preserving quantum operation $\mathcal{S}\colon M_n \to M_n$ and quantum error correction is described by another trace-preserving quantum operation $\mathcal{T}\colon M_n \to M_n$ that satisfies $\mathcal{T} \circ \mathcal{S} = c\mathcal{I}_n$ for $c > 0$. It is thus important to find conditions under which $\mathcal{S}$ is invertible up to a multiplicative positive constant. These are called quantum error correction conditions.

Theorem 5.6. *Let $\mathcal{S}\colon M_n \to M_n$ be a quantum operation with operation elements $A_i \in M_n$, $i = 1, \dots, r$. Then there exists a trace-preserving quantum operation $\mathcal{T}\colon M_n \to M_n$ such that $\mathcal{T} \circ \mathcal{S} = c\mathcal{I}_n$, $c > 0$, if and only if $A_i^\dagger A_j = \alpha_{ij} I$, $i, j = 1, \dots, r$, for some $\alpha_{ij} \in \mathbb{C}$.*

Proof. Suppose there exists a trace-preserving quantum operation $\mathcal{T}$ such that $\mathcal{T} \circ \mathcal{S} = c\mathcal{I}_n$. Then $\mathcal{T}$ has the form $\mathcal{T}(\rho) = \sum B_j \rho B_j^\dagger$ and we have that

$$\sum B_j A_i \rho A_i^\dagger B_j^\dagger = \mathcal{T}\left(\mathcal{S}(\rho)\right) = c\rho$$

for all $\rho \in M_n$. By Theorem 5.2 there exist constants $c_{ji} \in \mathbb{C}$ such that $B_j A_i = c^{1/2} c_{ji} I_n$. Hence,

$$A_i^\dagger B_j^\dagger B_j A_k = c c_{ji}^* c_{jk} I_n$$

Since $\sum B_j^\dagger B_j = I_n$, summing over j gives

$$A_i^\dagger A_k = c \sum_j c_{ji}^* c_{jk} I_n = \alpha_{ik} I_n$$

Conversely, suppose that $A_i^\dagger A_j = \alpha_{ij} I_n$, $i, j = 1, \ldots, r$. Then

$$\alpha_{ij}^* I_n = A_j^\dagger A_i = \alpha_{ji} I_n$$

so that $\alpha_{ji} = \alpha_{ij}^*$. Hence, $\alpha = [\alpha_{ij}]$ is a hermitian matrix. By the spectral theorem there exists a unitary matrix $u = [u_{ij}]$ and a diagonal matrix $d = [d_{ij}]$ with real entries such that $d = u^\dagger \alpha u$. Define $B_k = \sum_i u_{ik} A_i$. By Theorem 5.2, $\mathcal{S}(\rho) = \sum B_i \rho B_i^\dagger$ and since $\mathcal{S}$ is trace-preserving $\sum B_i^\dagger B_i = I_n$. Now

$$\begin{aligned} B_k^\dagger B_\ell &= \sum u_{ki}^* u_{j\ell} A_i^\dagger A_j = \sum u_{ki}^* \alpha_{ij} u_{j\ell} I_n = d_{k\ell} I_n \\ &= \delta_{k\ell} d_{kk} I_n \end{aligned}$$

Hence,

$$I_n = \sum B_i^\dagger B_i = \sum d_{ii} I_n$$

so that $\sum d_{ii} = 1$. Since $B_i^\dagger B_i = d_{ii} I_n$, it follows that $B_i B_i^\dagger = d_{ii} I_n$. Hence,

$$\sum B_i B_i^\dagger = \sum d_{ii} I_n = I_n$$

Define $\mathcal{T}(\rho) = \sum B_j^\dagger \rho B_j$ we conclude that $\mathcal{T}$ is trace-preserving. Finally,

$$\mathcal{T}(\mathcal{S}(\rho)) = \sum B_j^\dagger B_i \rho B_i^\dagger B_j = \sum B_j^\dagger B_j \rho B_j^\dagger B_j = \left(\sum d_{jj}^2\right) \rho \qquad \square$$

We say that $\rho \in \mathrm{Herm}_d^+$ is **pure** if $\rho = AA^\dagger$ for some $A \in \mathbb{C}^d$. A quantum operation $\mathcal{S} \colon M_n \to M_m$ is **factorizable** if $\mathcal{S}(\rho) = \widehat{A} \rho \widehat{A}^\dagger$ for some $A \in \mathbb{C}^{mn}$. Notice that $\mathcal{S}$ is factorizable if and only if $\mathcal{S}^\vee$ is pure. The first part of the next theorem gives the usual characterization of pure states.

Theorem 5.7. (i) $\rho \in \mathrm{Herm}_d^+$ *is pure if and only if* $\mathrm{tr}(\rho)^2 = \mathrm{tr}(\rho^2)$.
(ii) A quantum operation $\mathcal{S} \colon M_n \to M_m$ *is factorizable if and only if* $\|\mathcal{S}\| = \mathrm{tr}\left(\mathcal{S}(I_n)\right)$.

Proof. (i) If ρ is pure, then ρ has at most one nonzero eigenvalue so $\mathrm{tr}(\rho)^2 = \mathrm{tr}(\rho^2)$. Conversely, suppose that $\mathrm{tr}(\rho)^2 = \mathrm{tr}(\rho^2)$ and ρ has eigenvalues $\{\lambda_i\}$. The purity condition gives $\left(\sum \lambda_i\right)^2 = \sum \lambda_i^2$ which implies that $\sum_{i \neq j} \lambda_i \lambda_j = 0$. Since $\lambda_i \geq 0$ there is at most one value of i such that $\lambda_i \neq 0$. It follows that ρ has the form $\rho = AA^\dagger$.

(ii) Let $\mathcal{S} = \widehat{S}$ for $S \in \mathrm{Herm}_{mn}^{+}$. Then $\mathcal{S}$ is factorizable if and only if S is pure which by (i) is equivalent to

$$\mathrm{tr}(I_{mn}S)^2 = \mathrm{tr}(S^2) \tag{5.2}$$

Now $I_{mn} = \sum\limits_{k,\ell} |k\ell\rangle|k\ell\rangle$ so that $\widehat{I}_{mn}(\rho) = \sum E_{k\ell}\rho E_{k\ell}^{\dagger}$. Hence, $\widehat{I}_{mn}(E_{ij}) = \delta_{ij}I_m$. By Corollary 3.2, (5.2) is equivalent to

$$\begin{aligned}
\|\mathcal{S}\|^2 = \mathrm{tr}(S^2) = \mathrm{tr}(I_{mn}S)^2 = \langle I_{mn} \mid S\rangle^2 = \left\langle \widehat{I}_{mn} \mid \mathcal{S}\right\rangle^2 \\
= \left[\sum_{i,j} \mathrm{tr}\left(\widehat{I}_{mn}(E_{ij})^{\dagger}\mathcal{S}(E_{ij})\right)\right]^2 = \left[\sum_{i,j} \mathrm{tr}\left(\delta_{ij}I_m\mathcal{S}(E_{ij})\right)\right]^2 \\
= \left[\sum_{i} \mathrm{tr}\left(\mathcal{S}(E_{ii})\right)\right]^2 = \mathrm{tr}\left(\mathcal{S}(I_n)\right)^2
\end{aligned}$$

□

The next result shows that any $\rho \in \mathrm{Herm}_d^{+}$ is the partial trace of a pure state and is called a **purification**.

Lemma 5.8. *If $\rho \in \mathrm{Herm}_d^{+}$ then there is an $A \in \mathbb{C}^{rd}$ for some $r \in \mathbb{N}$ such that $\rho = \mathrm{tr}_1(AA^{\dagger})$.*

Proof. By the spectral theorem, $\rho = \sum_{i=1}^{r} A_iA_i^{\dagger}$ for $A_i \in \mathbb{C}^d$. Let

$$A = \sum_{i=1}^{r} |i\rangle \otimes A_i \in \mathbb{C}^{rd}$$

where $\{|i\rangle\}$ is the basis for $\mathbb{C}^r$. Then

$$AA^{\dagger} = \sum |i\rangle\langle j| \otimes A_iA_j^{\dagger}$$

and we have that

$$\mathrm{tr}_1(AA^{\dagger}) = \sum \langle j \mid i\rangle A_iA_j^{\dagger} = \sum A_iA_i^{\dagger} = \rho$$

□

Our next result gives another important characterization of quantum operations

Theorem 5.9. *A map $\mathcal{S}\colon M_n \to M_m$ is a quantum operation if and only if $\mathcal{S}$ can be written as $\mathcal{S}(\rho) = \operatorname{tr}_1(\widehat{A}\rho\widehat{A}^\dagger)$ where $\widehat{A} \in \operatorname{End}(\mathbb{C}^n, \mathbb{C}^{rm})$ and tr_1 traces out the first r-dimensional system. Moreover, if the operation elements of $\mathcal{S}$ are $\left\{\widehat{A}_i\right\}$, then we have that $\widehat{A}^\dagger\widehat{A} = \sum \widehat{A}_i^\dagger\widehat{A}_i$.*

Proof. If $\mathcal{S}$ is a quantum operation, then by Theorem 5.1, $\mathcal{S} = \widehat{S}$ for $S \in \operatorname{Herm}_{mn}^+$. By Lemma 5.8, $S = \operatorname{tr}_1(AA^\dagger)$ for $A \in \mathbb{C}^{rmn}$. Applying Lemma 4.1 we have that

$$\mathcal{S} = \widehat{S} = \left[\operatorname{tr}_1(AA^\dagger)\right]^\wedge = \operatorname{tr}_1 \circ (AA^\dagger)^\wedge$$

Hence, for every $\rho \in M_n$ we obtain $\mathcal{S}(\rho) = \operatorname{tr}_1(\widehat{A}\rho\widehat{A}^\dagger)$. Since $\mathcal{S} = \widehat{S}$ and the operation elements of $\mathcal{S}$ are $\left\{\widehat{A}_i\right\}$, we have that $S = \sum A_iA_i^\dagger$. Letting tr_2 be the trace over the second m-dimensional system, by Lemma 2.5 we have that

$$\begin{aligned}\sum(\widehat{A}_i^\dagger\widehat{A}_i)^t &= \sum \operatorname{tr}_2(A_iA_i^\dagger) = \operatorname{tr}_2\left(\sum A_iA_i^\dagger\right) = \operatorname{tr}_2(S)\\ &= \operatorname{tr}_2\operatorname{tr}_1(AA^\dagger) = (\widehat{A}^\dagger\widehat{A})^t\end{aligned}$$

Hence, $\widehat{A}^\dagger\widehat{A} = \sum \widehat{A}_i^\dagger\widehat{A}_i$.

Conversely, suppose that $\mathcal{S}(\rho) = \operatorname{tr}_1(\widehat{A}\rho\widehat{A}^\dagger)$. By Lemma 5.5, tr_1 is completely positive. If the operation elements of tr_1 are $\{A_i\}$ we have that

$$\mathcal{S}(\rho) = \sum A_i\widehat{A}\rho\widehat{A}^\dagger A_i^\dagger = \sum A_i\widehat{A}\rho(A_i\widehat{A})^\dagger$$

Hence, $\mathcal{S}$ is completely positive with operation elements $\left\{A_i\widehat{A}\right\}$. ☐

In Theorem 5.9, notice that if $\mathcal{S}$ is trace-preserving, then $\widehat{A}^\dagger\widehat{A} = I_n$ so that $\widehat{A}$ is isometric. Moreover, notice that the last part of Theorem 5.9 also follows from the fact that the composition of two completely positive maps is completely positive as can be seen from the operator-sum representation.

We close with a characterization of a special type of quantum operation that has recently appeared in the literature [17]. A quantum operation $\mathcal{S}\colon M_n \to M_m$ is called **entanglement breaking** if $\mathcal{S}$ can be written in the form

$$\mathcal{S}(\rho) = \sum_r \operatorname{tr}(B_r\rho)A_r \tag{5.3}$$

for $B_r \in \mathrm{Herm}_n^+$ and $A_r \in \mathrm{Herm}_m^+$. We will assume without loss of generality that $\mathrm{tr}(A_r) = 1$ for all r. Indeed, just replace A_r by $A_r/\mathrm{tr}(A_r)$ and B_r by $B_r\mathrm{tr}(A_r)$ in (5.3). It then follows that $\mathcal{S}$ is trace-preserving if and only if $\sum B_r = I$; that is, $\{B_r\}$ is a positive operator-valued measure. Recall that $S \in \mathrm{Herm}_{mn}^+$ is **separable** if $S = \sum c_{rs} A_r \otimes B_s$ for $C_{rs} \geq 0$, $A_r \in \mathrm{Herm}_m^+$, $B_s \in \mathrm{Herm}_n^+$.

Theorem 5.10. *A map $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ is an entanglement breaking quantum operation if and only if $\mathcal{S}^\vee \in \mathrm{Herm}_{mn}^+$ is separable.*

Proof. Suppose that $\mathcal{S}^\vee \in \mathrm{Herm}_{mn}^+$ is separable. Then $\mathcal{S}^\vee$ has the form $\mathcal{S}^\vee = \sum c_{rs} A_r \otimes D_s$ for $c_{rs} \geq 0$, $A_r \in \mathrm{Herm}_m^+$, $B_s \in \mathrm{Herm}_n^+$. By linearity and Theorem 3.4(i) we have that

$$\mathcal{S}(\rho) = \sum c_{rs} \mathrm{tr}(D_s^t \rho) A_r = \sum \mathrm{tr}(B_r \rho) A_r$$

where $B_r = \sum c_{rs} D_s^t$. Conversely, suppose $\mathcal{S} \in \mathrm{End}(M_n, M_m)$ is an entanglement breaking quantum operation. Then by (5.2) and Theorem 3.4(i) we have that

$$\mathcal{S}(\rho) = \sum (A_r \otimes B_r^t)^\wedge(\rho) = \left(\sum A_r \otimes B_r^t\right)^\wedge (\rho)$$

for all $\rho \in M_n$. Hence, $\mathcal{S}^\vee = \sum A_r \otimes B_r^t$ is separable. □

References

[1] P. Arrighi and C. Patricot, On quantum operations as quantum states, arxiv: quant-ph/0307024, Sept. 2003.

[2] M. Brooks, Quantum Computing and Communications, Springer-Verlag, London, 1999.

[3] P. Busch, P. J. Lahti and P. Middlestaedt, *The Quantum Theory of Measurements*, Springer-Verlag, Berlin, 1996.

[4] M. D. Choi, Completely positive linear maps on complex matrices, *Lin. Alg. Appl.* **10** (1975), 285–290.

[5] E. B. Davies, Quantum Theory of Open Systems, *Academic Press*, London, 1976.

[6] A. Dvurečenskij and S. Pulmannová, *New Trends in Quantum Structures*, Kluwer, Dordrecht, 2000.

[7] D. J. Foulis and M. K. Bennett, Effect algebras and unsharp quantum logics, *Found. Phys.* **24** (1994), 1325–1346.

[8] J. Gruska, Quantum Computing, *McGraw-Hill*, London, 1999.

[9] S. Gudder and R. Greechie, Sequential products on effect algebras, *Rep. Math. Phys.* **49** (2002), 87–111.

[10] S. Gudder and G. Nagy, Sequential quantum measurements, *J. Math. Phys.* **42** (2001), 5212–5222.

[11] M. Hirvensalo, Quantum Computing *Springer*, Berlin, 2001.

[12] A. Jamiolkowski, Linear transformations that preserve trace and positive semidifinite operators, *Rep. Mod. Phys.* **3** (1972), 275–278.

[13] K. Kraus, General States in Quantum Theory, *Ann. Phys.*, **64** (1971), 311–315.

[14] K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin, 1983.

[15] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[16] J. Preskill, *Quantum Computation and Information*, California Institute of Technology, Pasadena, CA, 1998.

[17] P. W. Shor, Additivity of the classical capacity of entanglement-breaking channels, *J. Math. Phys.* **43** (2002), 4334–4340.