An Interpolation Problem by Completely Positive Maps and its Application in Quantum Cloning

Zhi-Hua Guo(郭志华)

College of Mathematics and Information Science, Shaanxi Normal University, Xi'an, China, 710062

gzhihua@tom.com

July 20, 2011

Introduction

The theory of quantum information is a result of the effort to generalize classical information theory to the quantum world. Quantum information theory aims to answer the following question: What happens if information is stored in a state of a quantum system? To characterize the way the information is processed consistent with the laws of quantum mechanics, in mathematics, a quantum operation is a trace preserving completely positive map from the set of density operators into itself. The completely positive maps play an important role in the description of quantum channels and time evolutions and have triggered an increasing interest.

Outline

1. Notations
2. An interpolation question
3. Some applications

Question

Denote by $\mathcal{M}_{M,N}$ the set of all $M \times N$ complex matrices, for brevity, write $\mathcal{M}_N$ when $M = N$ and let $\mathcal{H}_N$ be the set of Hermitian matrices in $\mathcal{M}_N$.

From *C. K. Li and Y. T. Poon, Interpolation problems by completely positive maps, arXiv: 1012. 1675v1.*

Question

Given $\{A_i\}_{i=1}^k \subseteq \mathcal{M}_N$ and $\{B_i\}_{i=1}^k \subseteq \mathcal{M}_M$, determine the necessary and sufficient condition for the existence of a completely positive map $\phi : \mathcal{M}_N \to \mathcal{M}_M$ such that $\phi(A_i) = B_i$ for every $1 \leq i \leq k$, and possibly with the additional properties that ϕ is unital or/and ϕ is trace preserving.

Question

Theorem. Let $\{A_i\}_{i=1}^k \subseteq \mathcal{H}_N$ and $\{B_i\}_{i=1}^k \subseteq \mathcal{H}_M$ be two commuting families. Then there exist unitary matrices $\mathbf{U} \in \mathcal{M}_N$ and $\mathbf{V} \in \mathcal{M}_M$ such that $\mathbf{U}^\dagger A_i \mathbf{U}$ and $\mathbf{V}^\dagger B_i \mathbf{V}$ are diagonals

$$\begin{pmatrix} a_{i1} & 0 & \dots & 0 \\ 0 & a_{i2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{iN} \end{pmatrix} \text{ and } \begin{pmatrix} b_{i1} & 0 & \dots & 0 \\ 0 & b_{i2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_{iM} \end{pmatrix},$$

respectively, for $i = 1, 2, \dots, k$. Then the following conditions are equivalent.

(a) There is a completely positive map $\phi : \mathcal{M}_N \to \mathcal{M}_M$ such that $\phi(A_i) = B_i$ for every $1 \leq i \leq k$.

(b) There is an $N \times M$ nonnegative matrix **M** such that $\mathbf{B} = \mathbf{AM}$, where

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1M} \\ b_{21} & b_{22} & \dots & b_{2M} \\ \dots & \dots & \dots & \dots \\ b_{k1} & b_{k2} & \dots & b_{kM} \end{pmatrix}, \quad \mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1N} \\ a_{21} & a_{22} & \dots & a_{2N} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kN} \end{pmatrix}.$$

Furthermore, (1) ϕ in (a) is unital if and only if **M** in (b) can be chosen to be column stochastic;

(2) ϕ in (a) is trace preserving if and only if **M** in (b) can be chosen to be row stochastic;

(3) ϕ in (a) is unital and trace preserving if and only if **M** in (b) can be chosen to be doubly stochastic.

Notations

Consider an $N \times M$ rectangular matrix $\mathbf{A} = [a_{ij}]$, we define the reshaping of $\mathbf{A}$ as

$$\mathbf{res}(\mathbf{A}) = (a_{11}, \ldots, a_{1M}, a_{21}, \ldots, a_{2M}, \ldots, a_{N1}, \ldots, a_{NM})^t, \quad (2.1)$$

where $\mathbf{X}^t$ denotes the transpose of a matrix $\mathbf{X}$. Clearly, the length of $\mathbf{res}(\mathbf{A})$ is NM.

Conversely, any vector of length NM may be reshaped into an $N \times M$ rectangular matrix. For example,

$$(a_1, a_2, a_3, a_4) \mapsto \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Notations

For arbitrary $MN \times ST$ matrix $\mathbf{C}$, usually we use both indices to denote $\mathbf{C} = [a_{ij}]$, but more conveniently, we will use the block-form of $\mathbf{C}$ as

$$\mathbf{C} = [C_{m,n}] \in \mathcal{M}_{M,N}(\mathcal{M}_{S,T})$$

and then write as

$$\mathbf{C} = [C_{m,n}] = [c_{\substack{m,\mu \\ n,\nu}}], \qquad (2.2)$$

where $c_{\substack{m,\mu \\ n,\nu}}$ denotes the (μ, ν)-entry of (m, n)-block matrix $C_{m,n}$.

Notations

For example,

$$\mathbf{C} = \left(\begin{array}{c|c} C_{11} & C_{12} \\ \hline C_{21} & C_{22} \end{array}\right) = \left(\begin{array}{cc|cc} c_{\substack{1,1\\1,1}} & c_{\substack{1,1\\1,2}} & c_{\substack{1,1\\2,1}} & c_{\substack{1,1\\2,2}} \\ c_{\substack{1,2\\1,1}} & c_{\substack{1,2\\1,2}} & c_{\substack{1,2\\2,1}} & c_{\substack{1,2\\2,2}} \\ \hline c_{\substack{2,1\\1,1}} & c_{\substack{2,1\\1,2}} & c_{\substack{2,1\\2,1}} & c_{\substack{2,1\\2,2}} \\ c_{\substack{2,2\\1,1}} & c_{\substack{2,2\\1,2}} & c_{\substack{2,2\\2,1}} & c_{\substack{2,2\\2,2}} \end{array}\right) = [c_{\substack{m,\mu\\n,\nu}}].$$

Especially, when $\mathbf{C} = \mathbf{A} \otimes \mathbf{B}$, $\mathbf{A} = [a_{mn}] \in \mathcal{M}_{M,N}$, $\mathbf{B} = [b_{\mu\nu}] \in \mathcal{M}_{S,T}$, we have $c_{\substack{m,\mu\\n,\nu}} = a_{mn} b_{\mu\nu}$.

Notations

For arbitrary $MN \times ST$ matrix **C** defined by Eq.(2.2), we define a block-matrix

$$\mathbf{C}^{\kappa} = [C^{\kappa}_{m,\mu}] = [c^{m,n}_{\mu,\nu}], \tag{2.3}$$

where $c^{m,n}_{\mu,\nu}$ denotes the (n,ν)-entry of (m,μ)-block matrix $C^{\kappa}_{m,\mu}$.

For instance, if $\mathbf{C} = \left(\begin{array}{c|c} C_{11} & C_{12} \\ \hline C_{21} & C_{22} \end{array}\right) = \begin{pmatrix} c^{1,1}_{1,1} & c^{1,1}_{1,2} & \underline{c^{1,1}_{2,1}} & \underline{c^{1,1}_{2,2}} \\ \underline{c^{1,2}_{1,1}} & \underline{c^{1,2}_{1,2}} & c^{1,2}_{2,1} & c^{1,2}_{2,2} \\ c^{2,1}_{1,1} & c^{2,1}_{1,2} & \underline{c^{2,1}_{2,1}} & \underline{c^{2,1}_{2,2}} \\ \underline{c^{2,2}_{1,1}} & \underline{c^{2,2}_{1,2}} & c^{2,2}_{2,1} & c^{2,2}_{2,2} \end{pmatrix},$

$$\text{then } \mathbf{C}^{\kappa} = \begin{pmatrix} c^{1,1}_{1,1} & c^{1,1}_{1,2} & \underline{c^{1,2}_{1,1}} & \underline{c^{1,2}_{1,2}} \\ \underline{c^{1,1}_{2,1}} & \underline{c^{1,1}_{2,2}} & c^{1,2}_{2,1} & c^{1,2}_{2,2} \\ c^{2,1}_{1,1} & c^{2,1}_{1,2} & \underline{c^{2,2}_{1,1}} & \underline{c^{2,2}_{1,2}} \\ \underline{c^{2,1}_{2,1}} & \underline{c^{2,1}_{2,2}} & c^{2,2}_{2,1} & c^{2,2}_{2,2} \end{pmatrix}.$$

Notations

$$\mathbf{C} = \left(\begin{array}{ccc|ccc}
z^{1,1}_{1,1} & z^{1,1}_{1,2} & z^{1,1}_{1,3} & z^{1,1}_{2,1} & z^{1,1}_{2,2} & z^{1,1}_{2,3} \\
z^{1,2}_{1,1} & z^{1,2}_{1,2} & z^{1,2}_{1,3} & z^{1,2}_{2,1} & z^{1,2}_{2,2} & z^{1,2}_{2,3} \\
z^{1,3}_{1,1} & z^{1,3}_{1,2} & z^{1,3}_{1,3} & z^{1,3}_{2,1} & z^{1,3}_{2,2} & z^{1,3}_{2,3} \\ \hline
z^{2,1}_{1,1} & z^{2,1}_{1,2} & z^{2,1}_{1,3} & z^{2,1}_{2,1} & z^{2,1}_{2,2} & z^{2,1}_{2,3} \\
z^{2,2}_{1,1} & z^{2,2}_{1,2} & z^{2,2}_{1,3} & z^{2,2}_{2,1} & z^{2,2}_{2,2} & z^{2,2}_{2,3} \\
z^{2,3}_{1,1} & z^{2,3}_{1,2} & z^{2,3}_{1,3} & z^{2,3}_{2,1} & z^{2,3}_{2,2} & z^{2,3}_{2,3}
\end{array}\right),$$

$$\mathbf{C}^{\kappa} = \left(\begin{array}{ccc|ccc|ccc}
z^{1,1}_{1,1} & z^{1,1}_{1,2} & z^{1,1}_{1,3} & z^{1,2}_{1,1} & z^{1,2}_{1,2} & z^{1,2}_{1,3} & z^{1,3}_{1,1} & z^{1,3}_{1,2} & z^{1,3}_{1,3} \\
z^{1,1}_{2,1} & z^{1,1}_{2,2} & z^{1,1}_{2,3} & z^{1,2}_{2,1} & z^{1,2}_{2,2} & z^{1,2}_{2,3} & z^{1,3}_{2,1} & z^{1,3}_{2,2} & z^{1,3}_{2,3} \\ \hline
z^{2,1}_{1,1} & z^{2,1}_{1,2} & z^{2,1}_{1,3} & z^{2,2}_{1,1} & z^{2,2}_{1,2} & z^{2,2}_{1,3} & z^{2,3}_{1,1} & z^{2,3}_{1,2} & z^{2,3}_{1,3} \\
z^{2,1}_{2,1} & z^{2,1}_{2,2} & z^{2,1}_{2,3} & z^{2,2}_{2,1} & z^{2,2}_{2,2} & z^{2,2}_{2,3} & z^{2,3}_{2,1} & z^{2,3}_{2,2} & z^{2,3}_{2,3}
\end{array}\right).$$

Notations

Let **C** be as in Eq.(2.2). Then $(\mathbf{C}^{\kappa})^{\kappa} = \mathbf{C}$.

Theorem [Choi, 1975]

Let $\phi : \mathcal{M}_N \rightarrow \mathcal{M}_M$ be a linear map. Then ϕ is completely positive if and only if ϕ is of the form $\phi(\rho) = \sum_{i=1}^{k} V_i \rho V_i^{\dagger}$ for all ρ in $\mathcal{M}_N$ where V_i is an $M \times N$ matrix for each $1 \leq i \leq k$.

Remark

Note that $\{V_i\}_{i=1}^{k}$ is not uniquely determined by ϕ. If there exists another family $\{W_i\}_{i=1}^{\ell}$ such that $\phi(\rho) = \sum_i^{\ell} W_i \rho W_i^{\dagger}$ for all ρ in $\mathcal{M}_N$, then there must be a unitary $U = [u_{ij}]$ such that $W_i = \sum_{j=1}^{k} u_{ij} V_j$ for every $1 \leq i \leq \ell$.

Notations

For a completely positive map $\phi : \mathcal{M}_N \to \mathcal{M}_M$, let it be represented as

$$\phi(\rho) = \sum_{i=1}^{k} V_i \rho V_i^{\dagger}, \quad \forall \rho \in \mathcal{M}_N, \tag{2.4}$$

Let the $M \times N$ matrix V_i satisfy Eq.(2.4) be written as $V_i = [a_{mn}^i]$ for $i = 1, 2, \ldots, k$. Define a Kraus matrix **M** of ϕ as

$$\mathbf{M} = \Big[\sum_{i=1}^{k} |a_{mn}^i|^2\Big]. \tag{2.5}$$

Notations

Remark

In fact, $\mathbf{M} = \sum_{i=1}^{k} [a^i_{mn}] \circ [\overline{a^i_{mn}}]$, where $\circ$ denotes the Hadamard product of V_i and $\overline{V_i}$, $\overline{a^i_{mn}}$ is the conjugate of a^i_{mn}. Even though Kraus operators of ϕ are not unique, by Remark 1 and Eq. (2.5), the Kraus matrix $\mathbf{M}$ is unique and written $\mathbf{M}_\phi$, clearly, it is a non-negative(its entries ≥ 0) matrix.

Notations

Now we reshape V_i into a length MN column vector $\textbf{res}(V_i)$ following Eq.(2.1). Define $\mathbf{V} := \Big(\textbf{res}(V_1), \textbf{res}(V_2), \ldots, \textbf{res}(V_k)\Big)$, and put $\mathbf{D} = \mathbf{V}\mathbf{V}^\dagger$, namely,

$$\mathbf{V} = \begin{pmatrix} a_{11}^1 & a_{11}^2 & \ldots & a_{11}^k \\ \ldots & \ldots & \ldots & \ldots \\ a_{1N}^1 & a_{1N}^2 & \ldots & a_{1N}^k \\ \ldots & \ldots & \ldots & \ldots \\ a_{M1}^1 & a_{M1}^2 & \ldots & a_{M1}^k \\ \ldots & \ldots & \ldots & \ldots \\ a_{MN}^1 & a_{MN}^2 & \ldots & a_{MN}^k \end{pmatrix},$$

which is an $MN \times k$ matrix, and

Notations

$$\mathbf{D} = \begin{pmatrix} \sum_{i=1}^k a_{11}^i \overline{a_{11}^i} & \sum_{i=1}^k a_{11}^i \overline{a_{12}^i} & \cdots & \sum_{i=1}^k a_{11}^i \overline{a_{MN}^i} \\ \cdots & \cdots & \cdots & \cdots \\ \sum_{i=1}^k a_{1N}^i \overline{a_{11}^i} & \sum_{i=1}^k a_{1N}^i \overline{a_{12}^i} & \cdots & \sum_{i=1}^k a_{1N}^i \overline{a_{MN}^i} \\ \cdots & \cdots & \cdots & \cdots \\ \sum_{i=1}^k a_{M1}^i \overline{a_{11}^i} & \sum_{i=1}^k a_{M1}^i \overline{a_{12}^i} & \cdots & \sum_{i=1}^k a_{M1}^i \overline{a_{MN}^i} \\ \cdots & \cdots & \cdots & \cdots \\ \sum_{i=1}^k a_{MN}^i \overline{a_{11}^i} & \sum_{i=1}^k a_{MN}^i \overline{a_{12}^i} & \cdots & \sum_{i=1}^k a_{MN}^i \overline{a_{MN}^i} \end{pmatrix}, \tag{2.6}$$

which is an $MN \times MN$ matrix.

Notations

Let $z_{\substack{m,\mu\\ n,\nu}} = \sum_{i=1}^{k} a_{mn}^{i}\overline{a_{\mu\nu}^{i}}$. Then **D** can be written as follows

$$\mathbf{D} = \left(\begin{array}{ccc|c|ccc}
z_{\substack{1,1\\1,1}} & \cdots & z_{\substack{1,1\\1,N}} & \cdots & z_{\substack{1,M\\1,1}} & \cdots & z_{\substack{1,M\\1,N}} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
z_{\substack{1,1\\N,1}} & \cdots & z_{\substack{1,1\\N,N}} & \cdots & z_{\substack{1,M\\N,1}} & \cdots & z_{\substack{1,M\\N,N}} \\
\hline
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\hline
z_{\substack{M,1\\1,1}} & \cdots & z_{\substack{M,1\\1,N}} & \cdots & z_{\substack{M,M\\1,1}} & \cdots & z_{\substack{M,M\\1,N}} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
z_{\substack{M,1\\N,1}} & \cdots & z_{\substack{M,1\\N,N}} & \cdots & z_{\substack{M,M\\N,1}} & \cdots & z_{\substack{M,M\\N,N}}
\end{array}\right). \qquad (2.7)$$

Notations

Also, **D** can be represented by following formalism

$$\mathbf{D} = \sum_{i=1}^{k} \Big(\mathbf{res}(V_i)\Big)\Big(\mathbf{res}(V_i)\Big)^{\dagger}. \tag{2.8}$$

The following gives a matrix representation of Eq.(2.4).

Proposition

If ϕ satisfies Eq.(2.4), then $\mathbf{res}(\phi(\rho)) = \mathbf{D}_{\phi}^{\kappa}\mathbf{res}(\rho)$ *for each* $\rho \in \mathcal{M}_N$.

An interpolation question

Theorem

(1) If $\phi : \mathcal{M}_N \to \mathcal{M}_M$ is a completely positive map, then $\mathbf{D}_\phi \in \mathcal{M}_{MN}$ is positive semi-definite.

(2) If $\mathbf{D} \in \mathcal{M}_{MN}$ is positive semi-definite, then there exists a completely positive map $\phi : \mathcal{M}_N \to \mathcal{M}_M$ such that $\mathbf{D}_\phi = \mathbf{D}$.

(3) Suppose that ϕ is a completely positive map, then (i) ϕ is unital if and only if $\mathrm{tr}_2 \mathbf{D}_\phi := \sum_{\mu=1}^{N} z_{n,\mu}^{m,\mu} = I_M$; (ii) ϕ is trace preserving if and only if $\mathrm{tr}_1 \mathbf{D}_\phi := \sum_{m=1}^{M} z_{m,\mu}^{m,\nu} = I_N$.

Remark

The matrix $\mathbf{M}$ in (b) of Theorem in the beginning is just transpose $\mathbf{M}_\phi^t$ of the Kraus matrix of the completely positive map ϕ in (a).

The following theorem is an our main result considering the existence of completely positive maps ϕ sending a general family of matrices in $\mathcal{M}_N$ to another family in $\mathcal{M}_M$.

Theorem

Let $\{A_i\}_{i=1}^k \subseteq \mathcal{M}_N$ and $\{B_i\}_{i=1}^k \subseteq \mathcal{M}_M$. Then the following conditions are equivalent.

(a) There exists a completely positive map $\phi : \mathcal{M}_N \to \mathcal{M}_M$ *such that* $\phi(A_i) = B_i$ *for every* $1 \leq i \leq k$.

(b) There exists an $MN \times MN$ *positive semi-definite matrix* **E** *such that*

$$(\textbf{res}(B_1), \textbf{res}(B_2), \ldots, \textbf{res}(B_k)) = \textbf{E}^{\kappa}(\textbf{res}(A_1), \textbf{res}(A_2), \ldots, \textbf{res}(A_k)). \quad (3.1)$$

An interpolation question

Moreover, if one of (a) and (b) holds, then (1) ϕ in (a) is unital if and only if **E** in (b) satisfies $\text{tr}_2\mathbf{E} = I_M$;

(2) ϕ in (a) is trace preserving if and only if **E** in (b) satisfies $\text{tr}_1\mathbf{E} = I_N$.

(3) ϕ in (a) is unital trace preserving if and only if **E** in (b) satisfies $\text{tr}_1\mathbf{E} = I_N$ and $\text{tr}_2\mathbf{E} = I_M$.

An interpolation question

Corollary

Let $\{A_i\}_{i=1}^k \subseteq \mathcal{M}_N$ and $\{B_i\}_{i=1}^k \subseteq \mathcal{M}_M$ be two families consisting of diagonal matrices, for every $1 \leq i \leq k$, denote

$$A_i = \begin{pmatrix} a_{i1} & 0 & \dots & 0 \\ 0 & a_{i2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{iN} \end{pmatrix} \textit{ and } B_i = \begin{pmatrix} b_{i1} & 0 & \dots & 0 \\ 0 & b_{i2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_{iM} \end{pmatrix}.$$

Then the following conditions are equivalent.

(a) There is a completely positive map $\phi : \mathcal{M}_N \to \mathcal{M}_M$ such that $\phi(A_i) = B_i$ for every $1 \leq i \leq k$.

(b) There is an $N \times M$ nonnegative matrix **M** such that **B** = **AM**, where

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1M} \\ b_{21} & b_{22} & \dots & b_{2M} \\ \dots & \dots & \dots & \dots \\ b_{k1} & b_{k2} & \dots & b_{kM} \end{pmatrix}, \quad \mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1N} \\ a_{21} & a_{22} & \dots & a_{2N} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kN} \end{pmatrix}.$$

(c) There exists a positive semi-definite matrix **E** *with size* MN *satisfying Eq.(3.1).*

Denote by $\mathcal{D}_N$ the set of all density matrices in $\mathcal{M}_N$.

Definition

Let $\{\rho_i\}_{i=1}^k \subseteq \mathcal{D}_N$. If there exists a quantum operation $\phi : \mathcal{M}_N \otimes \mathcal{M}_N \to \mathcal{M}_N \otimes \mathcal{M}_N$ and a standard state $\Sigma \in \mathcal{D}_N$ such that

$$\phi(\rho_i \otimes \Sigma) = \rho_i \otimes \rho_i, i = 1, 2, \ldots, k,$$

then we call $\{\rho_1, \rho_2, \ldots, \rho_k\}$ is clonable.

It was essentially proved in [*H. Barnum, C. M. Caves, et al., Noncommuting Mixed States Cannot Be Broadcast*] that $\{\rho_1, \rho_2\}$ is clonable if and only if ρ_1 and ρ_2 are identical or orthogonal (i.e. $\rho_1\rho_2 = 0$). The following theorem generalizes this conclusion, which will be proved with a very simple way that is different from the old approach. Let we see the following properties of fidelity $F(\rho_1, \rho_2)$ of two arbitrary density matrices ρ_1, ρ_2 are needed.

Lemma

For all density matrices $\rho_i \in \mathcal{D}_N (i = 1, 2, 3, 4)$, the following are valid:

(1) $0 \le F(\rho_1, \rho_2) \le 1$;

(2) $F(\rho_1, \rho_2) = 0$ if and only if $\rho_1 \rho_2 = 0$;

(3) $F(\rho_1, \rho_2) = 1$ if and only if $\rho_1 = \rho_2$;

(4) $F(\rho_1 \otimes \rho_2, \rho_3 \otimes \rho_4) = F(\rho_1, \rho_3) F(\rho_2, \rho_4)$.

Applications

Theorem

Let $\{\rho_i\}_{i=1}^k \subseteq \mathcal{D}_N$ and $\rho_i \neq \rho_j$ if $i \neq j$. Then $\{\rho_i\}_{i=1}^k$ is clonable if and only if $\rho_i\rho_j = 0$ for $1 \leq i \neq j \leq k$.

Proof. *Necessity.* Suppose that $\{\rho_i\}_{i=1}^k$ is clonable, then we see that there exists a quantum operation $\phi : \mathcal{M}_N \otimes \mathcal{M}_N \to \mathcal{M}_N \otimes \mathcal{M}_N$ and a standard state Σ such that

$$\phi(\rho_i \otimes \Sigma) = \rho_i \otimes \rho_i, i = 1, 2, \ldots, k. \tag{4.1}$$

Since any quantum operation does not decrease the fidelity between two quantum states, for $1 \leq i \neq j \leq k$, we have

$$F(\rho_i, \rho_j) = F(\rho_i \otimes \Sigma, \rho_j \otimes \Sigma) \leq F(\rho_i \otimes \rho_i, \rho_j \otimes \rho_j) = F(\rho_i, \rho_j)^2,$$

so, $F(\rho_i, \rho_j) = 0$ or $F(\rho_i, \rho_j) = 1$. Since $\rho_i \neq \rho_j$, $F(\rho_i, \rho_j) \neq 1$. Therefore, $F(\rho_i, \rho_j) = 0$, this shows that $\rho_i\rho_j = 0$, for $1 \leq i \neq j \leq k$.

Sufficiency. Suppose that for $1 \leq i \neq j \leq k$, $\rho_i \rho_j = 0$, then there exists a unitary matrix U such that $\rho_i' = U \rho_i U^\dagger$ is diagonal for every $1 \leq i \leq k$. Take $\Sigma \in \mathcal{D}_N$ such that $\Sigma' = U \Sigma U^\dagger$ is diagonal (e.g., $\Sigma = N^{-1} I_N$) and write ρ_i', Σ' as

$$\rho_i' = \begin{pmatrix} a_1^i & 0 & \dots & 0 \\ 0 & a_2^i & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_N^i \end{pmatrix}, \ \Sigma' = \begin{pmatrix} c_1 & 0 & \dots & 0 \\ 0 & c_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & c_N \end{pmatrix},$$

respectively.

Since

$$(\rho_i' \otimes \Sigma')(\rho_j' \otimes \Sigma') = (U\rho_i\rho_j U^\dagger) \otimes (\Sigma'\Sigma') = 0$$

and

$$(\rho_i' \otimes \rho_i')(\rho_j' \otimes \rho_j') = (U\rho_i\rho_j U^\dagger) \otimes (U\rho_i\rho_j U^\dagger) = 0,$$

for all $1 \leq i \neq j \leq k$, we know that both $\{\rho_i' \otimes \Sigma'\}_{i=1}^k$ and $\{\rho_i' \otimes \rho_i'\}_{i=1}^k$ are commuting families of Hermitian matrices.

Applications

Define

$$\mathbf{M} = \begin{pmatrix} M_{11} & M_{12} & M_{13} & \dots & M_{1N} \\ M_{21} & M_{22} & M_{23} & \dots & M_{2N} \\ M_{31} & M_{32} & M_{33} & \dots & M_{3N} \\ \dots & \dots & \dots & \dots & \dots \\ M_{N1} & M_{N2} & M_{N3} & \dots & M_{NN} \end{pmatrix},$$

where each M_{ij} is an $N \times N$ square matrix for $1 \leq i, j \leq N$ such that $M_{ij} = 0 (i \neq j)$ and

$$M_{jj} = \begin{pmatrix} a_1^i & a_2^i & \dots & a_N^i \\ a_1^i & a_2^i & \dots & a_N^i \\ \dots & \dots & \dots & \dots \\ a_1^i & a_2^i & \dots & a_N^i \end{pmatrix} \text{ if } a_j^i \neq 0 \text{ for some } i (1 \leq i \leq k);$$

Clearly, **M** is a row stochastic matrix. Since $\rho_i'\rho_j' = U\rho_i\rho_j U^\dagger = 0$ for $1 \leq i \neq j \leq k$, $\sum_{r=1}^N a_r^i a_r^j = 0$ and $a_r^i, a_r^j \geq 0$ implies $a_r^i a_r^j = 0$ for each $1 \leq r \leq N$ and $1 \leq i \neq j \leq k$. It follows from $\text{tr}(\rho_i') = \text{tr}(\Sigma') = 1$ that there must at least exist $1 \leq i_1, i_2, \ldots, i_k \leq N$ such that $a_{i_1}^1, a_{i_2}^2, \ldots, a_{i_k}^k \neq 0$, but $a_{i_s}^j = 0$ for all $j \neq s (s, j = 1, 2, \ldots, k)$. For fixed j, there exists at most some $1 \leq i \leq k$ such that $a_j^i = 0$.

Thus,

$$\begin{pmatrix} (a_1^1)^2 & \dots & a_1^1 a_N^1 & \dots & a_N^1 a_1^1 & \dots & (a_N^1)^2 \\ (a_1^2)^2 & \dots & a_1^2 a_N^2 & \dots & a_N^2 a_1^2 & \dots & (a_N^2)^2 \\ \dots \\ (a_1^k)^2 & \dots & a_1^k a_N^k & \dots & a_N^k a_1^k & \dots & (a_N^k)^2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1^1 c_1 & \dots & a_1^1 c_N & \dots & a_N^1 c_1 & \dots & a_N^1 c_N \\ a_1^2 c_1 & \dots & a_1^2 c_N & \dots & a_N^2 c_1 & \dots & a_N^2 c_N \\ \dots \\ a_1^k c_1 & \dots & a_1^k c_N & \dots & a_N^k c_1 & \dots & a_N^k c_N \end{pmatrix} \mathbf{M} \qquad (4.2)$$

is valid.

It follows that there exists a quantum operation $\phi' : \mathcal{M}_{N^2} \to \mathcal{M}_{N^2}$ satisfying

$$\phi'(\rho_i' \otimes \Sigma') = \rho_i' \otimes \rho_i'(i = 1, 2, \ldots, k). \tag{4.3}$$

Let $\phi'(\rho) = \sum_{i=1}^{\ell} V_i \rho V_i^\dagger, \forall \rho \in \mathcal{M}_{N^2}$, where $\sum_{i=1}^{\ell} V_i^\dagger V_i = I$. Now, we define

$$\phi(\rho) = \sum_{i=1}^{\ell} [(U \otimes U)^\dagger V_i (U \otimes U)] \rho [(U \otimes U)^\dagger V_i (U \otimes U)]^\dagger, \forall \rho \in \mathcal{M}_{N^2}.$$

Applications

Clearly, $\sum_{i=1}^{\ell}[(U\otimes U)^\dagger V_i(U\otimes U)]^\dagger[(U\otimes U)^\dagger V_i(U\otimes U)]=I$, so $\phi:\mathcal{M}_{N^2}\to\mathcal{M}_{N^2}$ is a quantum operation and for $i=1,2,\ldots,k$, we have

$$\begin{aligned}\phi(\rho_i\otimes\Sigma) &= (U\otimes U)^\dagger\phi'(\rho_i'\otimes\Sigma')(U\otimes U)\\ &= (U\otimes U)^\dagger(\rho_i'\otimes\rho_i')(U\otimes U)\\ &= (U^\dagger\rho_i'U)\otimes(U^\dagger\rho_i'U)\\ &= \rho_i\otimes\rho_i.\end{aligned}$$

Thank you !