Int J Theor Phys (2008) 47: 2268–2278
DOI 10.1007/s10773-008-9659-4

Note on Generalized Quantum Gates and Quantum Operations

Yue-Qing Wang · Hong-Ke Du · Yan-Ni Dou

Received: 10 November 2007 / Accepted: 15 January 2008 / Published online: 25 January 2008

Abstract Recently, Gudder proved that the set of all generalized quantum gates coincides the set of all contractions in a finite-dimensional Hilbert space (S. Gudder, Int. J. Theor. Phys. 47:268–279, 2008). In this note, we proved that the set of all generalized quantum gates is a proper subset of the set of all contractions on an infinite dimensional separable Hilbert space $\mathcal{H}$. Meanwhile, we proved that the quantum operation deduced by an isometry is an extreme point of the set of all quantum operations on $\mathcal{H}$.

Keywords Generalized quantum gate · Duality quantum computer · Extreme point of quantum operations

1 Introduction

In more recent papers, Gudder (see [3, 4]) has established mathematical theory of the duality computer which proposed by Long in [6]. The mathematical theory of duality quantum computers attracts much more attention of a number of mathematicians (see [1–7]).

Let $\mathcal{H}$ and $\mathcal{K}$ be separable complex Hilbert spaces and let $\mathcal{B}(\mathcal{H},\mathcal{K})$ denote the all of bounded linear operators from $\mathcal{H}$ into $\mathcal{K}$. If $\mathcal{H}=\mathcal{K}$, it is abbreviated by $\mathcal{B}(\mathcal{H})(=\mathcal{B}(\mathcal{H},\mathcal{H}))$. An operator $A\in\mathcal{B}(\mathcal{H},\mathcal{K})$ is said to be a contraction if $\|A\|\leq 1$. The set of all contractions in $\mathcal{B}(\mathcal{H},\mathcal{K})$ is denoted by $\mathcal{B}(\mathcal{H},\mathcal{K})_1$. An operator $A\in\mathcal{B}(\mathcal{H})$ is said to be a positive operator if $(Ax,x)\geq 0$ for $x\in\mathcal{H}$. An operator $P\in\mathcal{B}(\mathcal{H})$ is said to be an orthogonal projection if $P=P^*=P^2$, where P^* denotes the adjoint of P. An operator $A\in\mathcal{B}(\mathcal{H})$ is said to be a semi-Fredholm if the range $\mathcal{R}(A)$ of A is closed and at least one of $\dim\mathcal{N}(A)$ and $\dim\mathcal{N}(A^*)$ is finite. In this case, the Fredholm index of A is defined by $\operatorname{ind}A=\dim\mathcal{N}(A)-\dim\mathcal{N}(A^*)$,

This subject is supported by NSF of China (10571113).

Y.-Q. Wang (✉) · H.-K. Du · Y.-N. Dou
College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, People's Republic of China
e-mail: wongyq@163.com

H.-K. Du
e-mail: hkdu@snnu.edu.cn

where $\dim \mathcal{N}(K)$ denotes the dimension of the null-space $\mathcal{N}(K)$ of an operators $K \in \mathcal{B}(\mathcal{H})$. An operator E is said to be a partial isometry if E as an operator from $\mathcal{R}(E^*)$ onto $\mathcal{R}(E)$ is a unitary.

The notation of generalized quantum gates was provided by Gudder in [3]. $\sum_{i=1}^n p_i U_i$ is called a generalized quantum gate if $U_i \in \mathcal{B}(\mathcal{H})$, $1 \leq i \leq n$, are unitary and $p = (p_1, \ldots, p_n)$ is a probability distribution. That is, $p_i > 0$, $1 \leq i \leq n$, and $\sum_{i=1}^n p_i = 1$. The set of all generalized quantum gates on $\mathcal{H}$ is denoted by $\mathcal{G}(\mathcal{H})$. It is clear that $\mathcal{G}(\mathcal{H})$ is a convex subset of $\mathcal{B}(\mathcal{H})$.

In [2], Gudder essentially proved:

Theorem G (See [4]) *If* $\dim \mathcal{H} < \infty$, *then* $\mathcal{G}(\mathcal{H}) = \mathcal{B}(\mathcal{H})_1$.

In Sect. 2 of this note, we shall show that $\mathcal{G}(\mathcal{H}) \neq \mathcal{B}(\mathcal{H})_1$ if $\dim \mathcal{H} = \infty$. Precisely, we shall prove:

Theorem 1.1 *If $A \in \mathcal{B}(\mathcal{H})_1$ is a finite-rank perturbation of a semi-Fredholm partial isometry with $indA \neq 0$, then A is not a generalized quantum gate.*

Denote $\mathcal{A} = (A_1, \ldots, A_n)$, where A_i, $1 \leq i \leq n$, are arbitrary operators in $\mathcal{B}(\mathcal{H})$ satisfying $\sum_{i=1}^n A_i^* A_i = I$. A quantum operation deduced by $\mathcal{A}$ is a bounded linear operator $\mathcal{E}_{\mathcal{A}}$ defined on $\mathcal{B}(\mathcal{H})$ by

$$\mathcal{E}_{\mathcal{A}}(X) = \sum_{i=1}^n A_i X A_i^*, \qquad X \in \mathcal{B}(\mathcal{H}).$$

The set of all quantum operations on $\mathcal{H}$ is denoted by $\mathcal{Q}(\mathcal{H})$. If the A_i $1 \leq i \leq n$, are positive operators satisfying $\sum_{i=1}^n A_i^2 = I$, then $\mathcal{E}_{\mathcal{A}}$ is called a positive quantum operation, the set of all positive quantum operations is denoted by $\mathcal{Q}_{\text{pos}}(\mathcal{H})$. If P_i, $1 \leq i \leq n$, are orthogonal projections satisfying $\sum_{i=1}^n P_i = I$, then $\mathcal{E}_{\mathcal{P}}$ is called a projective quantum operation, the set of all projective quantum operations is denoted by $\mathcal{Q}_{\text{pro}}(\mathcal{H})$. If U_i, $1 \leq i \leq n$, are unitary operators in $\mathcal{B}(\mathcal{H})$ and $\sum_{i=1}^n p_i = 1$ with $p_i > 0$, the quantum operation $\mathcal{E}_{\mathcal{U}}(X) = \sum_{i=1}^n p_i U_i X U_i^*$ is said to be a unitary quantum operation.

As Gudder [4] said that it is easy to check that $\mathcal{Q}(\mathcal{H})$, $\mathcal{Q}_{\text{u}}(\mathcal{H})$, $\mathcal{Q}_{\text{pos}}(\mathcal{H})$ are convex sets, while $\mathcal{Q}_{\text{pro}}(\mathcal{H})$ is not convex. In [4], Gudder established the extreme points of $\mathcal{Q}(\mathcal{H})$, $\mathcal{Q}_{\text{u}}(\mathcal{H})$ and $\mathcal{Q}_{\text{pos}}(\mathcal{H})$ under a finite-dimensional Hilbert space. In [4], Gudder concluded that $\mathcal{Q}_{\text{pro}}(\mathcal{H}) \subseteq \text{Ext}\mathcal{Q}_{\text{pos}}(\mathcal{H})$ if $\dim \mathcal{H} < \infty$, where $\text{Ext}K$ denotes the set of all extreme points of a convex set K. In [2], we extend this result on the setting with $\dim \mathcal{H} = \infty$ and showed that a projective quantum operation is not an extreme point of $\mathcal{Q}(\mathcal{H})$.

In Sect. 3, we shall show that a quantum operation deduced by an isometry is an extreme point of $\mathcal{Q}(\mathcal{H})$. That is,

Theorem 1.2 *Denote $\mathcal{E}_{\mathcal{V}}(X) = VXV^*$ if $V \in \mathcal{B}(\mathcal{H})$ is an isometry. Then $\mathcal{E}_{\mathcal{V}} \in Ext[\mathcal{Q}(\mathcal{H})]$.*

2 Proof of Theorem 1.1

In this section, we begin with some lemmas.

Lemma 2.1 *Let $p = (p_1, \ldots, p_n)$ be a probability distribution and let A_i, $1 \leq i \leq n$, be contractions. If $I = \sum_{i=1} p_i A_i$, then $A_i = I$ for $1 \leq i \leq n$.*

Proof For a unit vector $x \in \mathcal{H}$, we have that

$$\left|1 = (x, x) = \sum_{i=1}^{n} p_i (A_i x, x)\right|.$$

Observing that $|(A_i x, x)| \leq 1$ and the assumption of that $p = (p_1, \dots, p_n)$ be a probability distribution, then $(A_i x, x) = 1$ for a unit vector $x \in \mathcal{H}$. This concludes that $A_i = I$, $1 \leq i \leq n$. □

Lemma 2.2 *Let A be a contraction and let A as an operator from $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ into $\mathcal{H} = \mathcal{K}_1 \oplus \mathcal{H}_2$ have the operator matrix*

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}.$$

If A_{11} is a unitary from $\mathcal{H}_1$ onto $\mathcal{K}_1$, then $A_{12} = 0$ and $A_{21} = 0$.

Proof If A is a contraction, then A^*A is also a contraction. In this case,

$$\begin{aligned} A^*A &= \begin{pmatrix} A_{11}^* & A_{21}^* \\ A_{12}^* & A_{22}^* \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \\ &= \begin{pmatrix} A_{11}^*A_{11} + A_{21}^*A_{21} & A_{11}^*A_{12} + A_{21}^*A_{22} \\ A_{12}^*A_{11} + A_{22}^*A_{21} & A_{12}^*A_{12} + A_{22}^*A_{22} \end{pmatrix}. \end{aligned}$$

By the assumption of that A_{11} is a unitary from $\mathcal{H}_1$ onto $\mathcal{K}_1$, we have $A_{11}^*A_{11} + A_{21}^*A_{21} = I_{\mathcal{H}_1} + A_{21}^*A_{21}$. Moreover, observing that A^*A is a contraction implies that $A_{11}^*A_{11} + A_{21}^*A_{21}$ is also a contraction, thus $A_{21} = 0$.

Similarly, consider AA^*, we have

$$\begin{aligned} AA^* &= \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} A_{11}^* & A_{21}^* \\ A_{12}^* & A_{22}^* \end{pmatrix} \\ &= \begin{pmatrix} A_{11}A_{11}^* + A_{12}A_{12}^* & A_{11}A_{21}^* + A_{12}A_{22}^* \\ A_{21}A_{11}^* + A_{22}A_{12}^* & A_{21}A_{21}^* + A_{22}A_{22}^* \end{pmatrix}. \end{aligned}$$

Here $A_{11}A_{11}^* + A_{12}A_{12}^* = I_{\mathcal{K}_1} + A_{12}A_{12}^*$. So $A_{12} = 0$. □

Proof of Theorem 1.1 If A is a finite-rank perturbation of a semi-Fredholm partial isometry with that index is not zero, then A has a representation as follows

$$A = E + B,$$

where E is a semi-Fredholm partial isometry with $\mathrm{ind} A \neq 0$ and B is a finite-rank operator. Then E and B as operators from $\mathcal{H} = \mathcal{R}(E^*) \oplus \mathcal{R}(E^*)^\perp$ into $\mathcal{H} = \mathcal{R}(E) \oplus \mathcal{R}(E)^\perp$ have the operator matrices

$$E = \begin{pmatrix} E_0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} B^{11} & B^{12} \\ B^{21} & B^{22} \end{pmatrix}, \tag{1}$$

where E_0 is a unitary from $\mathcal{R}(E^*)$ onto $\mathcal{R}(E)$, $\dim \mathcal{R}(E^*)^\perp \neq \dim \mathcal{R}(E)^\perp$ and B^{ij} are finite-rank, $1 \leq i, j \leq 2$. Moreover, using Lemma 2.2, E and B as operators from $\mathcal{H} =$

$(\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*)) \oplus \mathcal{R}((B^{11})^*) \oplus \mathcal{R}(E^*)^{\perp}$ into $\mathcal{H} = E(\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*)) \oplus (\mathcal{R}(E) \ominus (E(\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*))) \oplus \mathcal{R}(E)^{\perp}$ have the operator matrices

$$E = \begin{pmatrix} E_0^1 & 0 & 0 \\ 0 & E_0^2 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & B_{12}^{11} & B_{13}^{12} \\ 0 & B_{22}^{11} & B_{23}^{12} \\ B_{31}^{21} & B_{32}^{21} & B^{22} \end{pmatrix}, \tag{2}$$

where E_0^1 is a unitary from $\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*)$ onto $E(\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*))$, E_0^2 is a unitary from $\mathcal{R}((B^{11})^*)$ onto $\mathcal{R}(E) \ominus (E(\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*))$, $\dim \mathcal{R}((B^{11})^*) = \dim(\mathcal{R}(E) \ominus (E(\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*))) < \infty$ and

$$E_0 = \begin{pmatrix} E_0^1 & 0 \\ 0 & E_0^2 \end{pmatrix}, \qquad B^{11} = \begin{pmatrix} 0 & B_{12}^{11} \\ 0 & B_{22}^{11} \end{pmatrix}, \qquad B^{12} = \begin{pmatrix} B_{13}^{12} \\ B_{23}^{12} \end{pmatrix}, \qquad B^{21} = \begin{pmatrix} B_{31}^{21} & B_{32}^{21} \end{pmatrix}.$$

Since $A = E + B \in \mathcal{B}(\mathcal{H})_1$,

$$A = \begin{pmatrix} E_0^1 & B_{12}^{11} & B_{13}^{12} \\ 0 & E_0^2 + B_{22}^{11} & B_{23}^{12} \\ B_{31}^{21} & B_{32}^{21} & B^{22} \end{pmatrix},$$

and E_0^1 is unitary, by Lemma 2.2 we have

$$B_{12}^{11} = 0, \qquad B_{13}^{12} = 0, \qquad B_{31}^{21} = 0.$$

Thus

$$A = E + B = \begin{pmatrix} E_0^1 & 0 & 0 \\ 0 & E_0^2 + B_{22}^{11} & B_{23}^{12} \\ 0 & B_{32}^{21} & B^{22} \end{pmatrix}.$$

Denote $\mathcal{H}_1 = (\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*))$, $\mathcal{H}_2 = \mathcal{R}((B^{11})^*) \oplus \mathcal{R}(E^*)^{\perp}$, $\mathcal{K}_1 = E(\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*))$, $\mathcal{K}_2 = (\mathcal{R}(E) \ominus (E(\mathcal{R}(E^*) \ominus \mathcal{R}((B^{11})^*))) \oplus \mathcal{R}(E)^{\perp}$ and

$$B_0 = \begin{pmatrix} E_0^2 + B_{22}^{11} & B_{23}^{12} \\ B_{32}^{21} & B^{22} \end{pmatrix}.$$

Then B_0 as an operator from $\mathcal{H}_2$ into $\mathcal{K}_2$ is finite-rank and $\dim \mathcal{H}_2 \neq \dim \mathcal{K}_2$. Therefore, A as an operator from $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ into $\mathcal{H} = \mathcal{K}_1 \oplus \mathcal{K}_2$ has the operator matrix

$$A = \begin{pmatrix} E_0^1 & 0 \\ 0 & B_0 \end{pmatrix}.$$

Next, we shall show that A is not a generalized quantum gate.

By the contrary, assume that A is a generalized quantum gate. Then there exist a probability distribution $p = (p_1, \ldots, p_n)$ and unitaries U_i, $1 \leq i \leq n$, such that $A = \sum_{i=1}^n p_i U_i$. Suppose that U_i, $1 \leq i \leq n$, as operators from $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ into $\mathcal{H} = \mathcal{K}_1 \oplus \mathcal{K}_2$ have the operator matrices

$$U_i = \begin{pmatrix} U_{11}^i & U_{12}^i \\ U_{21}^i & U_{22}^i \end{pmatrix}.$$

Then

$$\begin{pmatrix} E_0^1 & 0 \\ 0 & B_0 \end{pmatrix} = \sum_{i=1}^{n} p_i \begin{pmatrix} U_{11}^i & U_{12}^i \\ U_{21}^i & U_{22}^i \end{pmatrix}. \tag{3}$$

Denote $E_0^* = E_0^{1*} \oplus 0$. E_0^* is an operator from $\mathcal{H} = \mathcal{K}_1 \oplus \mathcal{K}_2$ into $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$. Multiplying (3) on the left by $\left(\begin{smallmatrix} E_0^{1*} & 0 \\ 0 & 0 \end{smallmatrix}\right)$, we obtain that

$$\begin{pmatrix} I_{\mathcal{H}_1} & 0 \\ 0 & \end{pmatrix} = \sum_{i=1}^{n} p_i \begin{pmatrix} E_0^{1*} U_{11}^i & E_0^{1*} U_{12}^i \\ 0 & 0 \end{pmatrix}.$$

Hence,

$$I_{\mathcal{H}_1} = \sum_{i=1}^{n} p_i E_0^{1*} U_{11}^i.$$

By Lemma 2.1, $E_0^* U_{11}^i = I_{\mathcal{H}_1}$, hence $U_{11}^i = E_0^1$, $1 \le i \le n$. Moreover, by Lemma 2.2, $U_{12}^i = 0$ and $U_{21}^i = 0$, $1 \le i \le n$, since U_i, $1 \le i \le n$, are unitaries. Thus U_i, $1 \le i \le n$, as operators from $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ into $\mathcal{H} = \mathcal{K}_1 \oplus \mathcal{K}_2$ have operator matrices

$$U_i = \begin{pmatrix} E_0 & 0 \\ 0 & U_{22}^i \end{pmatrix}, \quad 1 \le i \le n,$$

respectively. But, $\dim \mathcal{H}_2 \ne \dim \mathcal{K}_2$ implies that U_{22}^i, $1 \le i \le n$, are not unitary. Thus U_i, $1 \le i \le n$, are not unitary. It is a contradiction. □

Corollary 2.3 *A non-unitary isometry is not a generalized quantum gate.*

As a consequence, it is immediate.

Corollary 2.4 *If* $\dim \mathcal{H} = \infty$, *then* $\mathcal{G}(\mathcal{H}) \ne \mathcal{B}(\mathcal{H})_1$.

Although, in general, Theorem G does not hold in an infinite-dimensional setting, but we have a weaker fact.

Lemma 2.5 (See Proposition 3.2.23 in [8]) *If* $A \in \mathcal{B}(\mathcal{H})$ *with* $\|A\| < 1 - \frac{2}{n}$ *for some* $n > 2$, *there are unitary operators* $U_1, U_2, \ldots, U_n$ *such that*

$$A = \frac{1}{n}(U_1 + U_2 + \cdots + U_n). \tag{4}$$

Define the inner $\mathcal{B}(\mathcal{H})_1^\circ$ of $\mathcal{B}(\mathcal{H})_1$ by

$$\mathcal{B}(\mathcal{H})_1^\circ = \{A \in \mathcal{B}(\mathcal{H}) : \ \|A\| < 1\}.$$

From Lemma 2.5, we have:

Theorem 2.6 $\mathcal{B}(\mathcal{H})_1^\circ \subset \mathcal{G}(\mathcal{H})$.

Theorem 2.6 shows that, if $A \in \mathcal{B}(\mathcal{H})_1$ is not a generalized quantum gate, then A should be in the spherical surface of the unit ball $\mathcal{B}(\mathcal{H})_1$.

Let $\mathbb{R}^+\mathcal{G}(\mathcal{H})$ be the positive cone generalized by $\mathcal{G}(\mathcal{H})$. That is,

$$\mathbb{R}^+\mathcal{G}(H) = \{\alpha A : A \in \mathcal{G}(H),\ \alpha \geq 0\}.$$

In the recent paper [3, 4], Gudder proved that if $\dim \mathcal{H} < \infty$, then $\mathcal{B}(\mathcal{H}) = \mathbb{R}^+\mathcal{G}(\mathcal{H})$ (see Theorem 2.5 in [3]). We shall show that it holds also for $\dim \mathcal{H} = \infty$.

Theorem 2.7 $\mathcal{B}(\mathcal{H}) = \mathbb{R}^+\mathcal{G}(\mathcal{H})$.

Proof From Corollary 2.4, it is obvious. □

By Theorem 1.1, the following conjecture is natural.

Conjecture 2.8 *$\mathcal{B}(\mathcal{H})_1 \setminus \mathcal{G}(\mathcal{H})$ is the set of all finite-rank perturbations of semi-Fredholm partial isometries with that the index dose not equal to* 0.

3 Proof of Theorem 1.2

To complete the proof of Theorem 1.2, we need some lemmas.

Lemma 3.1 *Let $A \in \mathcal{B}(\mathcal{H})$. If, for each vector $x \in \mathcal{H}$, there exists a complex number λ_x such that $Ax = \lambda_x x$, then there exists a complex number λ such that $A = \lambda I$.*

Lemma 3.2 *If $X = \sum_{i=1}^n A_i X A_i^*$ for each operator $X \in \mathcal{B}(\mathcal{H})$, then $A_i = \lambda_i I$, where $\lambda_i \in \mathbb{C}$ and $1 \leq i \leq n$.*

Proof By Lemma 3.1, to this end, it is enough to show that for each vector $x \in \mathcal{H}$ and each i, $1 \leq i \leq n$, there exists a complex number λ_{ix} such that $A_i x = \lambda_{ix} x$.

Denote by P_x the orthogonal projection on the subspace spanning by a vector x. Then

$$P_x = \sum_{i=1}^n A_i P_x A_i^*.$$

In this case, P_x and A_i have the operator matrices

$$P_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad A_i = \begin{pmatrix} \lambda_{ix} & A_{12}^i \\ A_{21}^i & A_{22}^i \end{pmatrix}$$

with respect to the space decomposition $\mathcal{H} = \bigvee\{x\} \oplus (\bigvee\{x\})^\perp$, respectively, where λ_{ix} are complex numbers. Hence,

$$\begin{aligned}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &= \sum_{i=1}^n \begin{pmatrix} \lambda_{ix} & A_{12}^i \\ A_{21}^i & A_{22}^i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \overline{\lambda}_{ix} & A_{21}^{i*} \\ A_{12}^{i*} & A_{22}^{i*} \end{pmatrix} \\ &= \sum_{i=1}^n \begin{pmatrix} |\lambda_{ix}|^2 & \lambda_{ix} A_{21}^{i*} \\ \overline{\lambda}_{ix} A_{21}^i & A_{21}^i A_{21}^{i*} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^n |\lambda_{ix}|^2 & \sum_{i=1}^n \lambda_{ix} A_{21}^{i*} \\ \sum_{i=1}^n \overline{\lambda}_{ix} A_{21}^i & \sum_{i=1}^n A_{21}^i A_{21}^{i*} \end{pmatrix}.\end{aligned}$$

Therefore, $\sum_{i=1}^{n} A_{21}^{i} A_{21}^{i*} = 0$. This implies that $A_{21}^{i} = 0$, $1 \le i \le n$. That is,

$$A_i = \begin{pmatrix} \lambda_{ix} & A_{12}^{i} \\ 0 & A_{22}^{i} \end{pmatrix}, \quad 1 \le i \le n.$$

So, we conclude $A_i x = \lambda_{ix} x$, $x \in \mathcal{H}$ and $1 \le i \le n$. □

Proof of Theorem 1.2 Let V be an isometry. By the contrary, assume that there exist two quantum operations $\mathcal{E}_{\mathcal{A}}(X) = \sum_{i=1}^{n} A_i X A_i^*$ and $\mathcal{E}_{\mathcal{B}}(X) = \sum_{j=1}^{m} B_j X B_j^*$ such that

$$VXV^* = \lambda \sum_{i=1}^{n} A_i X A_i^* + (1-\lambda) \sum_{j=1}^{m} B_j X B_j^*, \tag{5}$$

we shall prove that $\sum_{i=1}^{n} A_i X A_i^* = \sum_{j=1}^{m} B_j X B_j^* = VXV^*$.

Multiplying (5) on the left by V^* and on the right by V, we get

$$X = \lambda \sum_{i=1}^{n} V^* A_i X A_i^* V + (1-\lambda) \sum_{j=1}^{m} V^* B_j X B_j^* V.$$

By Lemma 3.2, there exist complex numbers $\{\lambda_i\}$ and $\{\mu_j\}$ such that $V^* A_i = \lambda_i I$ and $V^* B_j = \mu_j I$.

Next, we shall prove that $A_i = \lambda_i V$ and $B_j = \mu_j V$.

Since V is an isometry, V, A_i, $1 \le i \le n$, and B_j, $1 \le j \le m$, as operators from $\mathcal{H}$ into $\mathcal{H} = \mathcal{R}(V) \oplus \mathcal{R}(V)^{\perp}$ have the operator matrices

$$V = \begin{pmatrix} V_1 \\ 0 \end{pmatrix}, \qquad A_i = \begin{pmatrix} A_1^i \\ A_2^i \end{pmatrix}, \qquad B_j = \begin{pmatrix} B_1^j \\ B_2^j \end{pmatrix},$$

respectively, where V_1 is a unitary operator from $\mathcal{H}$ onto $\mathcal{R}(V)$. From $V^* A_i = \lambda_i I$ and $V_1^* B_j = \mu_j I$, we have

$$(V_1^*, 0) \begin{pmatrix} A_1^i \\ A_2^i \end{pmatrix} = V_1^* A_1^i = \lambda_i I$$

and

$$(V_1^*, 0) \begin{pmatrix} B_1^j \\ B_2^j \end{pmatrix} = V_1^* B_1^j = \mu_j I.$$

Hence, $A_1^i = \lambda_i V_1$, $1 \le i \le n$, and $B_1^j = \mu_j V_1$, $1 \le j \le m$. Therefore, to prove that $A_i = \lambda_i V$ and $B_j = \mu_j V$, it is enough to show that $A_2^i = 0$ and $B_2^j = 0$. Substituting I for X in (5), we get

$$VV^* = \lambda \sum_{i=1}^{n} A_i A_i^* + (1-\lambda) \sum_{j=1}^{m} B_j B_j^*.$$

So

$$\begin{pmatrix} V_1V_1^* & 0 \\ 0 & 0 \end{pmatrix}$$
$$= \lambda \sum_{i=1}^{n} \begin{pmatrix} A_1^i A_1^{i*} & A_1^i A_2^{i*} \\ A_2^i A_1^{i*} & A_2^i A_2^{i*} \end{pmatrix} + (1-\lambda) \sum_{j=1}^{m} \begin{pmatrix} B_1^j B_1^{j*} & B_1^j B_2^{j*} \\ B_2^j B_1^{j*} & B_2^j B_2^{j*} \end{pmatrix}$$
$$= \begin{pmatrix} \lambda \sum_{i=1}^n A_1^i A_1^{i*} + (1-\lambda) \sum_{j=1}^m B_1^j B_1^{j*} & \lambda \sum_{i=1}^n A_1^i A_2^{i*} + (1-\lambda) \sum_{j=1}^m B_1^j B_2^{j*} \\ \lambda \sum_{i=1}^n A_2^i A_1^{i*} + (1-\lambda) \sum_{j=1}^m B_2^j B_1^{j*} & \lambda \sum_{i=1}^n A_2^i A_2^{i*} + (1-\lambda) \sum_{j=1}^m B_2^j B_2^{j*} \end{pmatrix}.$$

Comparing the two sides of equation above,

$$\lambda \sum_{i=1}^{n} A_2^i A_2^{i*} + (1-\lambda) \sum_{j=1}^{m} B_2^j B_2^{j*} = 0.$$

This shows that $A_2^i = 0$, $1 \le i \le n$, and $B_2^j = 0$, $1 \le j \le m$. Therefore, $A_i = \lambda_i V$ and $B_j = \mu_j V$.

Hence, $\sum_i^n |\lambda_i|^2 I = \sum_{i=1}^n \overline{\lambda}_i V^* \lambda_i V = \sum_{i=1}^n A_i^* A_i = I$ and $\sum_i^n |\mu_i|^2 I = \sum_{i=1}^n \overline{\mu}_i V^* \mu_i V = \sum_{j=1}^m B_j^* B_j = I$. So, $\sum_i^n |\lambda_i|^2 = \sum_j^m |\mu_j|^2 = 1$. Moreover, we conclude that

$$\sum_{i=1}^{n} A_i X A_i^* = \left(\sum_{i}^{n} |\lambda_i|^2 \right) V X V^* = V X V^*$$

and

$$\sum_{j=1}^{m} B_j X B_j^* = \left(\sum_{j=1}^{m} |\mu_j|^2 \right) V X V^* = V X V^*. \qquad \square$$

Corollary 3.3 *A quantum operation deduced by a unitary is an extreme point of* $\mathcal{Q}(\mathcal{H})$.

As the end of this paper, by a similar idea above, we get a slight extension of the Lemma 4.2 in [4]. But the proof is different from that of [4].

Theorem 3.4 *Let* $\mathcal{A} = (A_1, \ldots, A_m)$ *and* $\mathcal{P} = (P_1, \ldots, P_n)$, *where* A_j, $P_i \in \mathcal{B}(\mathcal{H})$, $\sum_{j=1}^m A_j^* A_j = I$, $\sum_{i=1}^n P_i^* P_i = I$ *and* P_i, $1 \le i \le n$, *are orthogonal projections. If* $\mathcal{E}_{\mathcal{P}} = \mathcal{E}_{\mathcal{A}}$, *then there exists an* $m \times n$ *complex matrix* $M = (\lambda_{ji})_{m \times n}$ *with* $M^* M = I_{n \times n}$ *and*

$$A_j = \sum_{i=1}^{n} \lambda_{ji} P_i,$$

where $I_{n \times n}$ *denotes the* $n \times n$ *identity matrix.*

Proof If $\mathcal{E}_{\mathcal{P}} = \mathcal{E}_{\mathcal{A}}$, then

$$\sum_{i=1}^{n} P_i X P_i = \sum_{j=1}^{m} A_j X A_j^*, \quad \text{for } X \in \mathcal{B}(\mathcal{H}). \tag{6}$$

Next, we shall divide the proof in three steps.

Step 1. Substituting P_i for X in (6), we get

$$P_i = \sum_{j=1}^{m} A_j P_i A_j^*. \tag{7}$$

Now, P_i and A_j, $1 \le i \le n$, $1 \le j \le m$, have the operator matrices

$$P_i = \begin{pmatrix} I_{\mathcal{R}(P_i)} & 0 \\ 0 & 0 \end{pmatrix}, \qquad A_j = \begin{pmatrix} A_{11}^j & A_{12}^j \\ A_{21}^j & A_{22}^j \end{pmatrix} \tag{8}$$

with respect to the space decomposition $\mathcal{H} = \mathcal{R}(P_i) \oplus \mathcal{N}(P_i)$, respectively, where I_M denotes the identity on a closed subspace M. Substituting (8) in (7), we get

$$\begin{pmatrix} I_{\mathcal{R}(P_i)} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^m A_{11}^j A_{11}^{j*} & \sum_{j=1}^m A_{11}^j A_{21}^{j*} \\ \sum_{j=1}^m A_{21}^j A_{11}^{j*} & \sum_{j=1}^m A_{21}^j A_{21}^{j*} \end{pmatrix}. \tag{9}$$

Comparing two sides of (9), we obtain

$$\sum_{j=1}^{m} A_{21}^j A_{21}^{j*} = 0.$$

This shows that $A_{21}^j = 0$, $1 \le j \le m$.

Substituting $I - P_i$ for X in (6), we get

$$I - P_i = \sum_{j=1}^{m} A_j (I - P_i) A_j^*. \tag{10}$$

By a similar argument, then

$$\begin{pmatrix} 0 & 0 \\ 0 & I_{\mathcal{N}(P_i)} \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^m A_{12}^j A_{12}^{j*} & \sum_{j=1}^m A_{12}^j A_{22}^{j*} \\ \sum_{j=1}^m A_{22}^j A_{12}^{j*} & \sum_{j=1}^m A_{22}^j A_{22}^{j*} \end{pmatrix}. \tag{11}$$

Comparing two sides of (11), we obtain

$$\sum_{j=1}^{m} A_{12}^j A_{12}^{j*} = 0.$$

This shows that $A_{12}^j = 0$, $1 \le j \le m$.

Hence, $\mathcal{R}(P_i)$, $1 \le i \le n$, are reduced subspaces of A_j, $1 \le j \le m$. So, A_j, $1 \le j \le m$, have the operator matrices

$$A_j = \bigoplus_{i=1}^{n} A_{ii}^j, \quad 1 \le j \le m, \tag{12}$$

with respect to the space decomposition $\mathcal{H} = \bigoplus_{i=1}^n \mathcal{R}(P_i)$, respectively.

Step 2. By Step 1 and (6), we have

$$Y_i = \sum_{j=1}^{m} A_{ii}^{j} Y_i A_{ii}^{j*}, \quad \text{for } Y_i \in \mathcal{B}(\mathcal{R}(P_i)). \tag{13}$$

By Lemma 3.2, we conclude that

$$A_{ii}^{j} = \lambda_{ji} I_{\mathcal{R}(P_i)}, \quad 1 \le j \le m,\ 1 \le i \le n,\ \lambda_{ji} \in \mathbb{C}. \tag{14}$$

Substituting $I_{\mathcal{R}(P_i)}$ and $\lambda_{ji} I_{\mathcal{R}(P_i)}$ for Y_i and A_{ii}^{j} in (13), respectively, we obtain

$$1 = \sum_{j=1}^{m} |\lambda_{ji}|^2, \quad 1 \le i \le n.$$

Step 3. If X has the operator matrix

$$X = (X_{rs})_{n\times n}$$

with respect to the space decomposition $\mathcal{H} = \bigoplus_{i=1}^{n} \mathcal{R}(P_i)$, where $(X_{rs})_{n\times n}$ is an $n \times n$ operator matrix and $X_{rs} \in \mathcal{B}(\mathcal{R}(P_s), \mathcal{R}(P_r))$, then from (6) and Step 2 we get

$$\bigoplus_{i=1}^{n} X_{ii} = \sum_{j=1}^{m} (\lambda_{jr}\overline{\lambda}_{js} X_{rs})_{n\times n} = \left(\left(\sum_{j=1}^{m} \lambda_{jr}\overline{\lambda}_{js}\right) X_{rs}\right)_{n\times n}. \tag{15}$$

Comparing two sides of (15), since $X_{rs} \in \mathcal{B}(\mathcal{R}(P_s), \mathcal{R}(P_r))$ are arbitrary, we have

$$\sum_{j=1}^{m} \lambda_{ji}\overline{\lambda}_{ji} = 1, \quad 1 \le i \le n, \quad \text{and} \quad \sum_{j=1}^{m} \lambda_{jr}\overline{\lambda}_{js} = 0, \quad r \ne s,\ 1 \le r, s \le n. \tag{16}$$

Denote $M = (\lambda_{ji})_{m\times n}$. By (16),

$$M^* M = I_{n\times n}.$$ □

Corollary 3.5 *Under the assumption as in Theorem 3.4, additionally, $n = m$, then the matrix M is an $n \times n$ unitary.*

Remark

(1) In general, $m \ge n$ in Theorem 3.4.
(2) It is obvious that, in Theorem 3.4, A_j, $1 \le j \le m$, are mutually commutative normal operators.

References

1. Busch, P., Singh, J.: Lüders theorem for unsharp quantum measurements. Phys. Lett. A **249**, 10–12 (1998)
2. Du, H.K., Wang, Y.Q., Xu, J.L.: Applications of the generalized Lüders theorem. J. Math. Phys., in press
3. Gudder, S.: Mathematical theory of duality quantum computers. Quantum Inf. Process. **6**(1), 37–48 (2007)

4. Gudder, S.: Duality quantum computers and quantum operations. Int. J. Math. Phys. **47**(1), 268–279 (2008)
5. Long, G.L.: Mathematical theory of the duality computer in the density matrix formalism. Quantum Inf. Process. **6**, 49–54 (2007)
6. Long, G.L.: The general quantum interference principle and the duality computer. arxiv:quant-ph/0512120 (2005)
7. Nielsen, M., Chuang, J.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
8. Pedersen, G.K.: Analysis Now. Springer/World Publishing, Beijing (1990)