DUALITY QUANTUM COMPUTERS and QUANTUM OPERATIONS

Stan Gudder
Department of Mathematics
University of Denver
Denver, Colorado 80208
sgudder@math.du.edu

Abstract

We present a mathematical theory for a new type of quantum computer called a duality quantum computer that has recently been proposed. We discuss the nonunitarity of certain circuits of a duality quantum computer. It is shown that a duality quantum computer can measure itself without needing a separate measurement apparatus to determine its final state. We then discuss the relevance of this work to quantum operations and their convexity theory. This discussion is based upon isomorphism theorems for completely positive maps.

1 Introduction

In a recent paper, Gui Lu Long proposed a new type of quantum computer called a duality quantum computer [7]. According to Long, a duality quantum computer is much more powerful than an ordinary quantum computer. In fact, a duality quantum computer can solve an unstructured database search problem in logarithmic time and can solve NP-complete problems in polynomial time. Moreover, Long has presented proof-in-principle designs for two possible duality quantum computers. This indicates that if a general purpose quantum computer can be constructed, then a duality quantum computer can probably also be constructed. A. Y. Shiekh has made a similar proposal [10].

Simply stated, a quantum computer is a series of quantum gates, represented by unitary operators $U_1, \ldots, U_n$ on a Hilbert space, that can be used to perform a computation [1, 3, 6, 9]. An initial state ψ_0 is input into the quantum computer and then evolves into the output state $\psi = U_n \cdots U_1 \psi_0$. To gain information about the computation, we make a measurement on the state ψ. If the measurement has m possible outcomes, then we obtain one of these outcomes with a probability depending on the state ψ. This resulting outcome gives information about ψ.

A duality quantum computer exploits the duality property that quantum systems can behave like both waves and particles. If a quantum system evolves undisturbed then it acts like a wave and when it is observed or measured it acts like a particle. Now a quantum wave ψ can be decomposed into parts using slits or beam splitters, for example. The wave parts or subwaves can move along separate paths and then be combined at which point they interfere. The subwaves are identical to ψ except they are at different locations along different paths. Because of these different locations, this does not violate the no cloning theorem which says that an unknown quantum state cannot be cloned exactly.

A duality quantum computer is a quantum computer that admits two new operations, a divider operator and a combiner operator. The divider operator decomposes the initial wave function into subwaves that are attenuated copies of the initial wave evolving along different paths. Each of the paths can contain quantum gates represented by unitary operators. After the subwaves pass through the quantum gates they are collected together by the combiner operator to form a final state. Finally, a measurement is performed on the final state to gain information about the computation. These multiple paths cause additional parallelism in a duality quantum computer and accounts for their superiority over ordinary quantum computers.

This article provides mathematical details of some of the work in [7]. In particular, we discuss the nonunitarity of certain circuits in a duality quantum computer. We show that a duality quantum computer can measure itself without needing a separate measurement apparatus to determine its final state. We then discuss the relevance of this work to quantum operations and their convexity theory. This discussion is based upon isomorphism theorems for completely positive maps [2, 9]. In this paper the states of a quantum system will refer only to the internal wave functions and the position part of the wave functions will not be displayed. In this way, the subwaves after a divider operation is applied will be copies of the initial wave function except

for an attenuation factor.

2 Generalized Quantum Gates

Let H be a complex Hilbert space and let $p = (p_1, \dots, p_n)$ be a probability distribution. That is, $p_i > 0$, $i = 1, \dots, n$, and $\sum p_i = 1$. We use the notation $\|p\| = \left(\sum p_i^2\right)^{1/2}$ and write $H^{\oplus^n}$ for $\oplus_{i=1}^n H_i$ where $H_i = H$, $i = 1, \dots, n$. The **divider operator** $D_p \colon H \to H^{\oplus^n}$ is defined by

$$D_p\psi = \frac{1}{\|p\|} \oplus_{i=1}^n (p_i\psi)$$

Thus, D_p maps ψ into attenuated copies of ψ. We think of each copy of H in $H^{\oplus^n}$ as a **path**. It is easy to check that D_p is a unitary operator from H onto its range $\mathcal{R}(D_p)$.

We next define the operator $C \colon H^{\oplus^n} \to H$ by

$$C(\psi_1 \oplus \cdots \oplus \psi_n) = \sum_{i=1}^n \psi_i$$

Although C is linear, it is not isometric. However, if we define C_p to be the restriction of $\|p\|C$ to $\mathcal{R}(D_p)$ then it is easy to show that C_p is unitary and $C_p = D_p^*$. We call C_p the **combiner operator**. Suppose we apply D_p and then a unitary operator U_i on each of the paths, $i = 1, \dots, n$ and finally apply C_p to obtain

$$\psi \to D_p\psi = \frac{1}{\|p\|} \oplus (p_i\psi) \to \frac{1}{\|p\|} \oplus (p_iU_i\psi) \to \left(\sum p_iU_i\right)\psi$$

We call $\sum p_iU_i$ a **generalized quantum gate**. Unlike an ordinary quantum computer, a duality quantum computer admits generalized quantum gates.

Denoting the set of generalized quantum gates on H by $\mathcal{G}(H)$, it is not hard to show that $\mathcal{G}(H)$ is a convex set and it is proved in [5] that the extreme points of $\mathcal{G}(H)$ are precisely the unitary operators on H. We conclude that except for a degenerate probability distribution, no generalized quantum gate is unitary; that is, no proper generalized quantum gate is a quantum gate. Stated in another way, except for the case of a single path, no duality quantum computer can be described by an ordinary quantum computer.

In a sense, a duality quantum computer is a mixture of ordinary quantum computers.

An example of a generalized quantum gate occurs in the following vector selection algorithm. Let $\psi_1,\dots,\psi_N$ be an orthonormal basis for H and suppose we want to select a marked but unknown vector ψ_k from among them. A quantum computer possess an oracle (black box) that recognizes ψ_k and the oracle is given by the unitary operator U where $U\psi_i=-(-1)^{\delta_{i,k}}\psi_i$. Let p be the probability distribution $p=(1/2,1/2)$ and let $\psi=(N)^{-1/2}\sum\psi_i$ be the input state for a duality quantum computer. Form the generalized quantum gate given by

$$\|p\|\,C(I\oplus U)D_p=\frac{1}{2}I_H+\frac{1}{2}U$$

Since $\frac{1}{2}(I_H+U)\psi_i=\delta_{i,k}\psi_i$ we have that $\frac{1}{2}(I_H+U)=P_k$ where P_k is the projection onto the one-dimensional subspace generated by ψ_k. Moreover, $\frac{1}{2}(I+U)\psi=(N)^{-1/2}\psi_k$ so the duality quantum computer selects the marked vector ψ_k using a single query to the oracle. This is the mechanism behind Long's logarithmic time database search algorithm [7].

We have seen that $\mathcal{G}(H)$ is a convex set whose extreme points are the unitary operators on H. Let $\mathcal{B}(H)$ be the set of bounded linear operators on H and let $\mathbb{R}^+\mathcal{G}(H)$ be the positive cone generated by $\mathcal{G}(H)$. That is,

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

It is shown in [5] that if $\dim H<\infty$, then a duality quantum computer can simulate any operator on H; that is $\mathcal{B}(H)=\mathbb{R}^+\mathcal{G}(H)$.

Suppose we have a duality quantum computer represented by the generalized quantum gate $\sum p_iU_i$. If the input state is represented by a unit vector ψ, then presumably the output state is represented by the unit vector

$$\sum p_iU_i\psi\Big/\left\|\sum p_iU_i\psi\right\|$$

Notice that it was necessary to renormalize the vector $\sum p_iU_i\psi$ because $\sum p_iU_i$ is not unitary in general. Instead of a pure state, suppose we input a mixed state represented by a density operator ρ. In accordance with the formalism of quantum mechanics, the divider operator D_p will transform ρ to the state $D_p\rho D_p^*=D_p\rho C_p$. Since

$$\begin{aligned}D_p\rho C_p\left[\oplus(p_i\phi)\right]&=\|p\|\,D_p\rho\left(\sum p_i\phi\right)=\|p\|\,D_p\rho\phi\\&=\oplus(p_i\rho\phi)=(\oplus p_i\rho)\phi\end{aligned}$$

we conclude that $D_p \rho D_p^* = \oplus p_i \rho$. If we now apply the quantum gates $\oplus U_i$ along the various paths we obtain $\oplus p_i U_i \rho U_i^*$. Finally, applying the operator C gives $\sum p_i U_i \rho U_i^*$.

The map $\mathcal{E}(\rho) = \sum p_i U_i \rho U_i^*$ is called a **quantum operation** in the literature [1, 3, 6, 9]. One advantage of this approach is that $\mathcal{E}(\rho)$ is again a state so we do not have to renormalize. Indeed, clearly $\mathcal{E}(\rho)$ is positive and we have that

$$\begin{aligned} \mathrm{tr}\left[\mathcal{E}(\rho)\right] &= \mathrm{tr}\left(\sum p_i U_i \rho U_i^*\right) = \sum p_i \mathrm{tr}\left(U_i \rho U_i^*\right) \\ &= \sum p_i \mathrm{tr}(\rho) = 1 \end{aligned}$$

Quantum operations of the form $\mathcal{E}$ are also frequently used to describe noisy quantum channels and error correcting quantum codes. For further discussions concerning the quantum operation $\mathcal{E}$ we refer the reader to [5, 8].

We now show that projective measurements can be directly incorporated into a duality quantum computer. To be precise, we show that a projective quantum measurement can be performed using a generalized quantum gate.

A general quantum operation has the form $\mathcal{E}(\rho) = \sum A_i \rho A_i^*$ where A_i are arbitrary operators on H satisfying $\sum A_i^* A_i = I_H$. If the A_i are projection operators P_i satisfying $\sum P_i = I_H$, then $\mathcal{E}$ is called a **projective measurement**. Notice that a generalized quantum gate also gives a quantum operation because we can write

$$\mathcal{E}(\rho) = \sum p_i U_i \rho U_i^* = \sum \sqrt{p_i}\, U_i \rho \sqrt{p_i}\, U_i^*$$

where

$$\sum \left(\sqrt{p_i}\, U_i\right)^* \left(\sqrt{p_i}\, U_i\right) = \sum p_i U_i^* U_i = \sum p_i I_H = I_H$$

Theorem 2.1. [5] *Let* $\dim H < \infty$ *and let* $\mathcal{E}(\rho) = \sum P_i \rho P_i$ *be a projective measurement. Then there exists a generalized quantum gate* $\sum p_i U_i$ *such that* $\mathcal{E}(\rho) = \sum p_i U_i \rho U_i^*$.

Proof. We shall employ the unitary freedom theorem [2, 9] which states that two quantum operations $\mathcal{E}(\rho) = \sum A_i \rho A_i^*$ and $\mathcal{F}(\rho) = \sum B_i \rho B_i^*$ coincide if and only if there exists a unitary matrix $[u_{jk}]$ such that $E_j = \sum_k u_{jk} F_k$ for all i, j. Letting $i = \sqrt{-1}$, the discrete Fourier transform is given by the unitary

$n \times n$ matrix $\left[n^{-1/2} e^{2\pi ijk/n}\right]$. Define the unitary operators U_j, $j = 1, \ldots, n$, by

$$U_j = \sum_{k=1}^{n} e^{2\pi ijk/n} P_k$$

We can then write

$$\frac{1}{\sqrt{n}} U_j = \sum_{k=1}^{n} \frac{1}{\sqrt{n}} e^{2\pi ijk/n} P_k$$

Applying the unitary freedom theorem, we conclude that

$$\mathcal{E}(\rho) = \sum P_i \rho P_i = \sum \left(\frac{1}{\sqrt{n}}\, U_i\right) \rho \left(\frac{1}{\sqrt{n}}\, U_i\right)^* = \sum \frac{1}{n} U_i \rho U_i^* \qquad \square$$

3 Matrix Endomorphisms

In preparation for a study of quantum operations this section considers the more general concept of matrix endomorphisms. Our discussion is similar to the work of Choi [2]. In this and the next section we shall employ Dirac notation which denotes the inner product by $\langle \phi \mid \psi \rangle$ and the outer product by $|\phi\rangle\langle\psi|$.

In the sequel we shall only consider a finite-dimensional Hilbert space H with $\dim H = n$. We can identify the set of bounded operators $\mathcal{B}(H)$ with the set of $n \times n$ complex matrices $\mathcal{M}_n$. We denote the standard basis for $H = \mathbb{C}^n$ for $|i\rangle$, $i = 1, \ldots, n$. The set of endomorphisms (linear transformations) from $\mathcal{M}_n$ into $\mathcal{M}_n$ is denoted by $\mathrm{End}(\mathcal{M}_n)$. The set $\mathrm{End}(\mathcal{M}_n)$ is a complex linear space in the usual way. The matrix units $E_{ij} = |i\rangle\langle j|$ form a basis for $\mathcal{M}_n$ and for $\mathcal{E}, \mathcal{F} \in \mathrm{End}(\mathcal{M}_n)$ we define the inner product

$$\langle \mathcal{E} \mid \mathcal{F} \rangle = \sum_{i,j} \mathrm{tr}\left(\mathcal{E}(E_{ij})^* \mathcal{F}(E_{ij})\right)$$

For $i, j, k, \ell = 1, \ldots, n$, we define $S_{ijk\ell} \in \mathcal{M}_{n^2}$ by $|i\rangle|j\rangle\langle k|\langle \ell|$. It is well known that $\{S_{ijk\ell}\}$ forms an orthonormal basis for $\mathcal{M}_{n^2}$ under the Hilbert-Schmidt inner product

$$\langle A \mid B \rangle = \mathrm{tr}(A^* B)$$

For $i, j, k, \ell = 1, \ldots, n$ we define $\mathcal{T}_{ijk\ell} \in \mathrm{End}(\mathcal{M}_n)$ by

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

It is easy to show that $\{\mathcal{T}_{ijk\ell}\}$ forms an orthonormal basis for $\mathrm{End}(\mathcal{M}_n)$. Define the map $^\vee\colon \mathcal{M}_{n^2} \to \mathrm{End}(\mathcal{M}_n)$ by $S^\vee_{ijk\ell} = \mathcal{T}_{ijk\ell}$ and extend by linearity. Then $^\vee$ becomes a unitary transformation from $\mathcal{M}_{n^2}$ onto $\mathrm{End}(\mathcal{M}_n)$. We denote the inverse of $^\vee$ by $^\wedge\colon \mathrm{End}(\mathcal{M}_n) \to \mathcal{M}_{n^2}$. A straightforward calculation shows that

$$E^\vee = \sum_{i,j,k,\ell} \langle j|\langle i|E|\ell\rangle|k\rangle \mathcal{T}_{ijk\ell}$$

and we then obtain the following result.

Lemma 3.1. *For $\mathcal{E} \in \mathrm{End}(\mathcal{M}_n)$ we have that*

$$\widehat{\mathcal{E}} = \sum_{i,j,k,\ell} \langle i|\mathcal{E}(E_{kj})|\ell\rangle S_{ijk\ell}$$

Proof. Since

$$\begin{aligned}
\mathcal{E} &= \sum \langle \mathcal{T}_{ijk\ell} \mid \mathcal{E}\rangle \mathcal{T}_{ijk\ell} = \sum_{i,j,k,\ell} \sum_{r,s} \mathrm{tr}\left[\mathcal{T}_{ijk\ell}(E_{rs})^* \mathcal{E}(E_{rs})\right] \mathcal{T}_{ijk\ell} \\
&= \sum_{i,j,k,\ell} \sum_{r,s} \mathrm{tr}\left[\left(|i\rangle\langle k|\,|r\rangle\langle s|\,|j\rangle\langle \ell|\right)^* \mathcal{E}(E_{rs})\right] \mathcal{T}_{ijk\ell} \\
&= \sum_{i,j,k,\ell} \sum_{r,s} \delta_{kr}\delta_{sj} \mathrm{tr}\left[|\ell\rangle\langle i|\mathcal{E}(E_{rs})\right] \mathcal{T}_{ijk\ell} \\
&= \sum \mathrm{tr}\left[|\ell\rangle\langle i|\mathcal{E}(E_{kj})\right] \mathcal{T}_{ijk\ell} = \sum \langle i|\mathcal{E}(E_{kj}|\ell\rangle \mathcal{T}_{ijk\ell}
\end{aligned}$$

taking $^\wedge$ of both sides gives the result □

The reason that the unitary transformation $^\wedge\colon \mathrm{End}(\mathcal{M}_n) \to \mathcal{M}_{n^2}$ is useful follows from the next result.

Theorem 3.2. *If $\mathcal{E} \in \mathrm{End}(\mathcal{M}_n)$ has the form $\mathcal{E}(A) = EAF$ for fixed $E, F \in \mathcal{M}_n$, then $\widehat{\mathcal{E}} = E \otimes F$*

Proof. Applying Lemma 3.1 we obtain

$$\begin{aligned}\widehat{\mathcal{E}} &= \sum \langle i|\mathcal{E}(E_{kj})|\ell\rangle S_{ijk\ell} = \sum \langle i|EE_{kj}F|\ell\rangle S_{ijk\ell} \\ &= \sum \langle i|E|k\rangle\langle j|F|\ell\rangle|i\rangle|j\rangle\langle k|\langle\ell| \\ &= \sum_{j,k,\ell} \langle j|F|\ell\rangle E|k\rangle|j\rangle\langle k|\langle\ell| \\ &= \sum_{j,\ell} \langle j|F|\ell\rangle E \otimes |j\rangle\langle\ell| = E \otimes \sum_{j,\ell} \langle j|F|\ell\rangle|j\rangle\langle\ell| \\ &= E \otimes F\end{aligned}$$

□

Some further applications of this work can be found in [4].

4 Quantum Operations

As a slight generalization of the discussion in Section 3, a **quantum operation** on H is an endomorphism $\mathcal{E} \in \mathrm{End}\,(\mathcal{B}(H))$ of the form

$$\mathcal{E}(A) = \sum_{i=1}^{N} E_i A E_I^*$$

where $E_i \in \mathcal{B}(H)$ satisfy $\sum E_i^* E_i = I_H$. The terms of the finite sequence $\{E_i\}$ are called **operational elements** of $\mathcal{E}$ and we write $\mathcal{E} \approx \{E_i\}$. If $\mathcal{E} \approx \{E_i\}$ and $\mathcal{E} \approx \{F_j\}$, we write $\{E_i\} \sim \{F_j\}$. Then $\sim$ is an equivalence relation. Moreover, by the unitary freedom theorem [2, 9], $\{E_i\} \sim \{F_j\}$ if and only if there exists a unitary matrix $[u_{ij}]$ such that $E_i = \sum_j u_{ij} F_j$ for all i. We say that a quantum operation $\mathcal{E}$ is **normal**, **positive**, or **projective** if $\mathcal{E} \approx \{E_i\}$ where E_i are normal, positive, or projection operators, respectively. If $E_i = \sqrt{p_i}\, U_i$ where U_i are unitary and $p_i \geq 0$, $\sum p_i = 1$ then $\mathcal{E}$ is a **unitary** quantum operation. Of course, unitary quantum operations correspond to generalized quantum gates and have the form

$$\mathcal{E}(A) = \sum p_i U_i A U_i^*$$

If the E_i mutually commute, then $\mathcal{E}$ is **commutative**.

If $\mathcal{E} \approx \{E_i\}$ is projective, then $\mathcal{E}$ corresponds to a projection-valued measure and we have $\sum E_i = I$. In this case $\mathcal{E}$ is commutative. If $\mathcal{E} \approx \{E_i\}$

is positive, then $\mathcal{E}$ corresponds to a positive operator-valued measure $\{E_i^2\}$ where $\sum E_i^2 = I_H$. Conversely, if $\{E_i\}$ is a positive operator-valued measure, then $\mathcal{E} \approx \left\{E_i^{1/2}\right\}$ is a positive quantum operation of considerable importance [9]. If $\{E_i\} \sim \{F_j\}$ then clearly, E_i mutually commute if and only if F_j mutually commute. In general, we can have $\{E_i\} \sim \{F_i\}$ where the E_i are normal, positive, projective or unitary, respectively and the F_j are not of these types, respectively. Thus, for example, when we say that $\mathcal{E}$ is normal we mean that there exists normal operators E_i such that $E \approx \{E_i\}$. It is then possible that $E \approx \{F_j\}$ where the F_j are not normal.

Lemma 4.1. *If $A_i \neq 0$ are positive and $B_i \neq 0$ are projections then $\{A_1, \ldots, A_n\} \sim \{B_1, \ldots, B_n\}$ if and only if $\{A_1, \ldots, A_n\}$ is a permutation of $\{B_1, \ldots B_n\}$*

Proof. By the unitary freedom theorem, $\{A_1, \ldots, A_n\} \sim \{B_1, \ldots B_n\}$ implies that $A_i = \sum u_{ij} B_j$ for some unitary matrix $[u_{ij}]$. Since A_i is positive, $u_{ij} \geq 0$ for all j. If $u_{ij} \neq 0$, then by unitarity $u_{ik} = 0$ for $k \neq j$. But then by unitarity, $u_{ij} = 1$. Hence, $[u_{ij}]$ is a permutation matrix and the result follows. □

Lemma 4.2. *If P_i are one-dimensional projections then $\{A_1, \ldots, A_n\} \sim \{P_1, \ldots, P_n\}$ if and only if A_i commute, are normal and $\operatorname{tr}(A_i^* A_k) = \delta_{ik}$.*

Proof. If $\{A_1, \ldots, A_n\} \sim \{P_1, \ldots, P_n\}$, then $A_i = \sum u_{ij} P_j$ for a unitary matrix $[u_{ij}]$. Hence, A_i commute and are normal. Moreover,

$$\begin{aligned}\operatorname{tr}(A_i^* A_k) &= \operatorname{tr}\left(\sum_j \overline{u}_{ij} P_j \sum_\ell u_{k\ell} P_\ell\right) = \operatorname{tr}\left(\sum_j \overline{u}_{ij} u_{kj} P_j\right) \\ &= \sum_j \overline{u}_{ij} u_{kj} = \delta_{ik}\end{aligned}$$

Conversely, suppose A_i commute, are normal and $\operatorname{tr}(A_i^* A_k) = \delta_{ik}$. Since the A_i are normal and commute, they are simultaneously diagonalizable so we can represent them by

$$A_i = \operatorname{diag}(a_{i_1}, \ldots, a_{i_n})$$

Now the vectors $a_i = (a_{i_1}, \ldots, a_{i_n})$ form an orthonormal basis because $\operatorname{tr}(A_i^* A_k) = \delta_{ik}$. Letting P_i be the one-dimensional projection onto the ith-coordinate, $i = 1, \ldots, n$, we have that $A_i = \sum a_{ij} P_j$. Since $[a_{ij}]$ forms a unitary matrix, it follows that $\{A_i, \ldots, A_n\} \sim \{P_1, \ldots, P_n\}$. □

Let $\mathcal{Q}(H)$ denote the set of quantum operations on H. We denote the sets of unitary, positive and projective quantum operations on H by $\mathcal{Q}_u(H)$, $\mathcal{Q}_{\text{pos}}(H)$, and $\mathcal{Q}_{\text{pro}}(H)$, respectively. It is easy to check that $\mathcal{Q}(H)$, $\mathcal{Q}_u(H)$ and $\mathcal{Q}_{\text{pos}}(H)$ are convex sets, while $\mathcal{Q}_{\text{pro}}(H)$ is not convex. It appears that characterizing the set of extreme points $\text{Ext}\,[\mathcal{Q}(H)]$ of $\mathcal{Q}(H)$ is very difficult. As we shall see, the situation is much simpler for $\mathcal{Q}_u(H)$ and we have some partial results and a conjecture for $\mathcal{Q}_{\text{pos}}(H)$. Theorem 2.1 shows that $\mathcal{Q}_{\text{pro}}(H) \subseteq \mathcal{Q}_u(H)$. We conjecture that $\mathcal{Q}_{\text{pos}}(H) \subseteq \mathcal{Q}_u(H)$. If this conjecture is true, it would show that a duality quantum computer can measure itself using a positive operator-valued measurement.

The conjecture $\mathcal{Q}_{\text{pos}}(H) \subseteq \mathcal{Q}_u(H)$ would follow if we could show that the extreme points of $\mathcal{Q}_{\text{pos}}(H)$ are precisely the elements of $\mathcal{Q}_{\text{pro}}(H)$. Indeed, since $\dim H < \infty$ it would follow that every $\mathcal{E} \in \mathcal{Q}_{\text{pos}}(H)$ is a convex combination of elements of $\mathcal{Q}_{\text{pro}}(H)$. Since $\mathcal{Q}_{\text{pro}}(H) \subseteq \mathcal{Q}_u(H)$, it would then follow that $\mathcal{Q}_{\text{pos}}(H) \subseteq \mathcal{Q}_u(H)$. For any $\mathcal{E} \in \mathcal{Q}_{\text{pos}}(H)$ we have that $\mathcal{E} \approx \{E_i\}$ where E_i are positive operators on H. Since $\sum E_i^2 = I_n$ we have that $0 \leq E_i \leq I_H$ for all i. Now operators E that satisfy $0 \leq E \leq I_H$ are called **effects**. We denote the convex set of effects on H by $\mathcal{E}(H)$ and the set of projection operators on H by $\mathcal{P}(H)$. The next result is well known and is an indication that the conjecture

$$\mathcal{Q}_{\text{pro}}(H) = \text{Ext}\,[\mathcal{Q}_{\text{pos}}(H)]$$

might be true.

Theorem 4.3. $\mathcal{P}(H) = \text{Ext}\,[\mathcal{E}(H)]$.

Proof. Suppose $P \in \mathcal{P}(H)$ and $P = \lambda E + (1-\lambda)F$ where $E, F \in \mathcal{E}(H)$ and $0 < \lambda < 1$. If $P\phi = \phi$ with $\|\phi\| = 1$ we have that

$$1 = \langle P\phi, \phi\rangle = \lambda\langle E\phi, \phi\rangle + (1-\lambda)\langle F\phi, \phi\rangle$$

This implies that $E\phi = F\phi = \phi$. If $P\psi = 0$ with $\|\psi\| = 1$, then

$$0 = \langle P\psi, \psi\rangle = \langle E\psi, \psi\rangle + (1-\lambda)\langle F\psi, \psi\rangle$$

This implies that $E\psi = F\psi = 0$. Hence, $E = F = P$ and we conclude that $\mathcal{P}(H) \subseteq \text{Ext}\,[\mathcal{E}(H)]$. To prove the opposite inclusion, for $E \in \mathcal{E}(H)$ we have that $E^2 \leq E \leq 2E$ so that $2E - E^2 \geq 0$. Also

$$0 \leq (I - E)^2 = I - 2E + E^2$$

so that $2E - E^2 \leq I$. Hence, $E_1 = 2E - E^2 \in \mathcal{E}(H)$. Letting $E_2 = E^2 \in \mathcal{E}(H)$ we have that $E = \frac{1}{2}E_1 + \frac{1}{2}E_2$. If $E \notin \mathcal{P}(H)$, then $E \neq E^2$ and hence $E_2 \neq E$ and $E_1 \neq E$. Therefore, $E \notin \text{Ext}\,[\mathcal{E}(H)]$ and it follows that $\mathcal{P}(H) = \text{Ext}\,[\mathcal{E}(H)]$. □

Although the next result is not surprising, its proof is not completely trivial.

Theorem 4.4. *The elements of* $\text{Ext}\,[\mathcal{Q}_u(H)]$ *are precisely those of the form* $\mathcal{E}(A) = UAU^*$ *where* U *is unitary.*

Proof. Suppose $\mathcal{E} \in \text{Ext}\,[\mathcal{Q}_u(H)]$. Since $\mathcal{E} \in \mathcal{Q}_u(H)$ we have that $\mathcal{E}(H) = \sum p_i U_i A U_i^*$ and since $\mathcal{E}$ is extremal it follows that $U_i A U_i^* = U_1 A U_1^*$ for all i. Therefore, $\mathcal{E}(A) = U_1 A U_1^*$. Conversely, suppose that $UAU^* = \sum p_i U_i A U_i^*$. Letting $A = P_\psi$ we have that $P_{U\psi} = \sum p_i P_{U_i\psi}$. Applying Theorem 4.3 we conclude that $P_{U_i\psi} = P_{U\psi}$ for all i. In particular, $P_{U_1\psi} = P_{U\psi}$. Hence, there exists an $\alpha_\psi \in \mathbb{C}$ with $|\alpha_\psi| = 1$ such that $U_1\psi = \alpha_\psi U\psi$. Now let ϕ be a vector satisfying $\|\phi\| = 1$ and $\phi \perp \psi$. Then as before there exists an $\alpha_\phi \in \mathbb{C}$ with $|\alpha_\phi| = 1$ such that $U_1\phi = \alpha_\phi U\phi$. Letting $\gamma = (\phi + \psi)/\sqrt{2}$ we have that

$$U_1\left(\frac{\psi+\phi}{\sqrt{2}}\right) = \alpha_\gamma U\left(\frac{\psi+\phi}{\sqrt{2}}\right)$$

Hence,

$$\alpha_\psi U\psi + \alpha_\phi U\phi = U_1(\psi+\phi) = \alpha_\gamma U(\psi+\phi) = \alpha_\gamma U\psi + \alpha_\gamma U\phi$$

It follows that $\alpha_\psi = \alpha_\phi = \alpha_\gamma$. Therefore, there exists an $\alpha_1 \in \mathbb{C}$ with $|\alpha_1| = 1$ such that $U_1 = \alpha_1 U$. Similarly, there exist $\alpha_i \in \mathbb{C}$ with $|\alpha_i| = 1$ such that $U_i = \alpha_i U$ for every i. We conclude that $U_i A U_i^* = UAU^*$ for every i. □

The next theorem is a partial result toward proving that $\mathcal{Q}_{\text{pro}}(H) = \text{Ext}\,[\mathcal{Q}_{\text{pos}}(H)]$.

Theorem 4.5. $\mathcal{Q}_{\text{pro}}(H) \subseteq \text{Ext}\,[\mathcal{Q}_{\text{pos}}(H)]$

Proof. Let $\mathcal{E}, \mathcal{F} \in \mathcal{Q}_{\text{pro}}(H)$ and $\mathcal{G} \in \mathcal{Q}_{\text{pro}}(H)$ with $\mathcal{E} \approx \{E_i\}$, $\mathcal{F} \approx \{F_j\}$ and $\mathcal{G} \approx \{P_k\}$. We can assume that $E_i, F_j, P_k \neq 0$ for all i, j, k. We can also assume without loss of generality that $E_i \neq \alpha E_{i'}$ and $F_j \neq \beta F_{j'}$ for any

$i \neq i'$, $j \neq j'$. Let $0 < \lambda < 1$ and suppose that $\mathcal{G} = \lambda\mathcal{E} + (1-\lambda)\mathcal{F}$. We then have that

$$\sum P_i A P_i = \sum \sqrt{\lambda}\, E_i A \sqrt{\lambda}\, E_i + \sum \sqrt{1-\lambda}\, F_i A \sqrt{1-\lambda}\, F_i$$

By the unitary freedom theorem there exists a unitary matrix $[u_{ij}]$ such that

$$\left[\sqrt{\lambda}\, E_1 \cdots \sqrt{\lambda}\, E_n \sqrt{1-\lambda}\, F_1 \cdots \sqrt{1-\lambda}\, F_m\right]^T = [u_{ij}][P_1 \cdots P_r\, 0 \cdots 0]^T$$

Notice that $n + m \geq r$ because otherwise $0 = \sum_j u_{ij} P_j$ which is impossible. Since $\sqrt{\lambda}\, E_i, \sqrt{1-\lambda}\, F_i \geq 0$, $u_{ij} \geq 0$ for all i and for $j = 1, \ldots, r$. For $j, k = 1, \ldots, r$, $j \neq k$, we have that $\sum_i u_{ij} u_{ik} = 0$. Hence, if $u_{ij} \neq 0$ then $u_{ik} = 0$, $j \neq k$, $j, k = 1, \ldots, r$ for every i. We can reorder the E_i if necessary so that $\sqrt{\lambda}\, E_i = u_{ii} P_i$. It follows that $n \leq r$. Since

$$I_H = \sum_{i=1}^{n} E_i^2 = \frac{1}{\lambda} \sum_{i=1}^{n} u_{ii}^2 P_i$$

we have that $n = r$ and $u_{ii} = \sqrt{\lambda}$. Hence, $E_i = P_i$. Continuing, we can reorder the F_i if necessary so that

$$\sqrt{1-\lambda}\, F_i = u_{n+i,n+i} P_i$$

Again, $m \leq r$ and we have that

$$I_H = \sum_{i=1}^{m} F_i^2 = \frac{1}{1-\lambda} \sum_{i=1}^{m} u_{n+i,n+i}^2 P_i$$

Hence, $m = r$ and $u_{n+i,n+i} = \sqrt{1-\lambda}$. Hence, $F_i = P_i$. Therefore, $\mathcal{E} = \mathcal{F} = \mathcal{G}$ so $\mathcal{G} \in \operatorname{Ext}[\mathcal{Q}_{\text{pos}}(H)]$. □

Because of Theorem 4.5, in order to show that $\mathcal{Q}_{\text{pro}}(H) = \operatorname{Ext}[\mathcal{Q}_{\text{pos}}(H)]$ we only need to show that $\operatorname{Ext}[\mathcal{Q}_{\text{pos}}(H)] \subseteq \mathcal{Q}_{\text{pro}}(H)$. To prove this latter inclusion we believe that the next result will be useful. This result involves the map $^\wedge\colon \operatorname{End}(\mathcal{M}_n) \to \mathcal{M}_{n^2}$ discussed in Section 3. In our present usage we consider $^\wedge$ to be a map from $\mathcal{Q}(H)$ to $\mathcal{B}(H \otimes H)$.

Theorem 4.6. (a) *If $\mathcal{E} \in \mathcal{Q}(H)$ has the form $\mathcal{E}(A) = \sum E_i A E_i^*$, then $\widehat{\mathcal{E}} = \sum E_i \otimes E_i^*$.* (b) *The map $\widehat{\ }\colon \mathcal{Q}(H) \to \mathcal{B}(H \otimes H)$ given by $\widehat{\mathcal{E}} = \sum E_i \otimes E_i^*$ where $\mathcal{E} \approx \{E_i\}$ is well-defined, convex and injective.*

Proof. (a) This follows directly from Theorem 3.2. (b) The map $\widehat{\ }$ is well-defined because if $\mathcal{E} \approx \{E_i\} \sim \{F_i\}$, then $F_i = \sum u_{ij} E_j$ for a unitary matrix $[u_{ij}]$. But then

$$\begin{aligned}\sum_i F_i \otimes F_i^* &= \sum_i \sum_j u_{ij} E_j \otimes \sum_k \overline{u}_{ik} E_k^* = \sum_{j,k} \sum_i u_{ij} \overline{u}_{ik} E_j \otimes E_k^* \\ &= \sum_{j,k} \delta_{jk} E_j \otimes E_k^* = \sum_j E_j \otimes E_j^*\end{aligned}$$

The map $\widehat{\ }$ is injective because it is the restriction of the injective map $\widehat{\ }$ to $\mathcal{Q}(H)$. Since $\mathcal{Q}(H)$ is convex and $\widehat{\ }$ is linear on $\mathrm{End}\,(\mathcal{B}(H))$ we conclude that $\widehat{\ }\colon \mathcal{Q}(H) \to \mathcal{B}(H \otimes H)$ is convex. □

Corollary 4.7. *If $\sum E_i^* E_i = \sum F_i^* F_i = I_H$ and $\sum E_i \otimes E_i^* = \sum F_i \otimes F_i^*$ then $F_i = \sum_j u_{ij} E_j$ for a unitary matrix $[u_{ij}]$.*

We now present two partial results which show that $\mathrm{Ext}\,[\mathcal{Q}_{\mathrm{pos}}(H)] \subseteq \mathcal{Q}_{\mathrm{pro}}(H)$ holds in special cases.

Theorem 4.8. *If $\mathcal{E} \in \mathcal{Q}_{\mathrm{pos}}(H) \setminus \mathcal{Q}_{\mathrm{pro}}(H)$ and $\mathcal{E} \approx \{E_i\}$ where the E_i mutually commute, then $\mathcal{E} \notin \mathrm{Ext}\,[\mathcal{Q}_{\mathrm{pos}}(H)]$.*

Proof. We shall prove this result for the case $H = \mathbb{C}^3$, $\mathcal{B}(H) = \mathcal{M}_3$, and the higher dimensional cases are similar. Assume that $\mathcal{E} \approx \{E_1, E_2, E_3\}$. Since the E_i mutually commute we can assume that they are diagonal, $E_i = \mathrm{diag}(a_i, b_i, c_i)$, $i = 1, 2, 3$, where

$$a_1^2 + a_2^2 + a_3^2 = b_1^2 + b_2^2 + b_3^2 = c_1^2 + c_2^2 + c_3^2 = 1$$

Let $\underline{a}$ be the unit vector $\underline{a} = (a_1, a_2, a_3) \in \mathbb{C}^3$ and define $\underline{b}$, $\underline{c}$ similarly. We then have that

$$\begin{aligned}\sum_{i=1}^3 E_i \otimes E_i &= \sum_{i=1}^3 \mathrm{diag}\,(a_i \mathrm{diag}(a_i, b_i, c_i), b_i \mathrm{diag}(a_i, b_i, c_i), c_i \mathrm{diag}(a_i, b_i, c_i)) \\ &= \mathrm{diag}(1, \underline{a} \cdot \underline{b}\,, \underline{a} \cdot \underline{c}\,, \underline{a} \cdot \underline{b}\,, 1, \underline{b} \cdot \underline{c}\,, \underline{a} \cdot \underline{c}\,, \underline{b} \cdot \underline{c}\,, 1)\end{aligned}$$

Since E_1, E_2, E_3 are not all projections, at least one of the inner products $\underline{a}\cdot\underline{b}$, $\underline{a}\cdot\underline{c}$ or $\underline{b}\cdot\underline{c}$ is strictly between 0 and 1. Say, $\underline{a}\cdot\underline{b}=\alpha$ with $0<\alpha<1$. Then there exists an $\varepsilon>0$ such that

$$0<\alpha-\varepsilon<\alpha<\alpha+\varepsilon<1$$

We can now write

$$\begin{aligned}\sum_{i=1}^{3} E_i\otimes E_i = \frac{1}{2}\operatorname{diag}(1,\underline{a}\cdot\underline{b}+\varepsilon,\underline{a}\cdot\underline{c},\underline{a}\cdot\underline{b}+\varepsilon,1,\underline{b}\cdot\underline{c},\underline{a}\cdot\underline{c},\underline{b}\cdot\underline{c},1)\\ +\frac{1}{2}\operatorname{diag}(1,\underline{a}\cdot\underline{b}-\varepsilon,\underline{a}\cdot\underline{c},\underline{a}\cdot\underline{b}-\varepsilon,1,\underline{b}\cdot\underline{c},\underline{a}\cdot\underline{c},\underline{b}\cdot\underline{c},1)\end{aligned}$$

Now there exist unit vectors $\underline{a}'$, $\underline{b}'$ with nonnegative entries such that $\underline{a}'\cdot\underline{b}'=\underline{a}\cdot\underline{b}+\varepsilon$, $\underline{a}'\cdot\underline{c}=\underline{a}\cdot\underline{c}$, $\underline{b}'\cdot\underline{c}=\underline{b}\cdot\underline{c}$ and similarly there exist unit vectors $\underline{a}''$, $\underline{b}''$ with nonnegative entries such that $\underline{a}''\cdot\underline{b}''=\underline{a}\cdot\underline{b}-\varepsilon$, $\underline{a}''\cdot\underline{c}=\underline{a}\cdot\underline{c}$, $\underline{b}''\cdot\underline{c}=\underline{b}\cdot\underline{c}$. Then letting $\underline{c}'=\underline{c}''=\underline{c}$ and $F_i=\operatorname{diag}(a_i',b_i',c_i')$, $G_i=\operatorname{diag}(a_i'',b_i'',c_i'')$, $i=1,2,3$ we have that

$$\begin{aligned}\sum_{i=1}^{3} E_i\otimes E_i &= \frac{1}{2}\operatorname{diag}(1,\underline{a}'\cdot\underline{b}',\underline{a}'\cdot\underline{c}',\underline{a}'\cdot\underline{b}',1,\underline{b}'\cdot\underline{c}',\underline{a}'\cdot\underline{c}',\underline{b}'\cdot\underline{c}',1)\\ &\quad+\frac{1}{2}\operatorname{diag}(1,\underline{a}''\cdot\underline{b}'',\underline{a}''\cdot\underline{c}'',\underline{a}''\cdot\underline{b}'',1,\underline{b}''\cdot\underline{c}'',\underline{a}''\cdot\underline{c}'',\underline{b}''\cdot\underline{c}'',1)\\ &=\frac{1}{2}\sum_{i=1}^{3}F_i\otimes F_i+\frac{1}{2}\sum_{i=1}^{3}G_i\otimes G_i\end{aligned}$$

It follows from this work that for $\sum_{i=1}^{n} E_i\otimes E_i$ in $\mathcal{M}_3\otimes\mathcal{M}_3$ where the E_i mutually commute, there exist commuting positive matrices F_1, F_2, F_3 such that

$$\sum_{i=1}^{n} E_i\otimes E_i=\sum_{i=1}^{3} F_i\otimes F_i$$

It follows from Theorem 4.6 that $\mathcal{E}\notin\operatorname{Ext}[\mathcal{Q}_{\text{pos}}(H)]$. □

Theorem 4.9. *If $\mathcal{E}\in\mathcal{Q}_{\text{pos}}(H)\setminus\mathcal{Q}_{\text{pro}}(H)$ and $\mathcal{E}\approx\{E_i\}$ where at least one of the E_i is invertible, then $\mathcal{E}\notin\operatorname{Ext}[\mathcal{Q}_{\text{pos}}(H)]$.*

Proof. We shall prove this result for the case $H = \mathbb{C}^2$, $\mathcal{B}(H) = \mathcal{M}_2$ and the higher dimensional cases are similar. We shall also assume that $\mathcal{E} \approx (E_1, E_2, E_3)$ where $E_1^2 + E_2^2 + E_3^2 = I_H$ and E_1 is invertible. Since E_1 is invertible there exists an $\varepsilon > 0$ such that $\sqrt{\varepsilon}\, I \leq E_1$. Now we can write

$$\sum_{i=1}^{3} E_i \otimes E_i = \frac{1}{2}\left[(1-\varepsilon)\sum_{i=1}^{3} E_i \otimes E_i + \varepsilon I_H \otimes I_H\right] + \frac{1}{2}\left[(1+\varepsilon)\sum_{i=1}^{3} E_i \otimes E_i - \varepsilon I_H \otimes I_H\right]$$

We have that

$$(1-\varepsilon)\sum_{i=1}^{n} E_i^2 + \varepsilon I_H = I_H$$

To treat the second term, we may assume that $E_1 = \operatorname{diag}(a, b)$, where $0 < a, b < 1$. Then

$$\begin{aligned}(1+\varepsilon)E_1 \otimes E_1 - \varepsilon I_H \otimes I_H \\ &= (1+\varepsilon)\operatorname{diag}(a^2, ab, ab, b^2) - \varepsilon \operatorname{diag}(1,1,1,1) \\ &= \operatorname{diag}\left((1+\varepsilon)a^2 - \varepsilon, (1+\varepsilon)ab - \varepsilon, (1+\varepsilon)ab - \varepsilon, (1+\varepsilon)b^2 - \varepsilon\right)\end{aligned}$$

Now $a^2, b^2 > \varepsilon$ so $(1+\varepsilon)a^2 - \varepsilon, (1+\varepsilon)b^2 - \varepsilon, (1+\varepsilon)ab - \varepsilon > 0$. Let

$$c = \sqrt{(1+\varepsilon)a^2 - \varepsilon}\,, \quad d = \sqrt{(1+\varepsilon)b^2 - \varepsilon}\,, \quad e = (1+\varepsilon)ab - \varepsilon$$

Since $2ab \leq b^2 + a^2$ we have that

$$e^2 = \left[(1+\varepsilon)ab - \varepsilon\right]^2 \leq \left[(1+\varepsilon)a^2 - \varepsilon\right]\left[(1+\varepsilon)b^2 - \varepsilon\right] = c^2 d^2$$

Now there exist vectors $(a_1, a_2), (b_1, b_2) \in \mathbb{C}^2$ such that $a_i, b_i \geq 0$, $i = 1, 2$, $a_1^2 + a_2^2 = c^2$, $b_1^2 + b_2^2 = d^2$ and $\langle (a_1, a_2), (b_1, b_2) \rangle = e$. Define $F, G \in \mathcal{M}_2$ by $F = \operatorname{diag}(a_1, b_1)$, $G = \operatorname{diag}(a_2, b_2)$. Then

$$\begin{aligned}(1+\varepsilon)E_1 \otimes E_1 - \varepsilon I_H \otimes I_H &= \operatorname{diag}(c^2, e, e, d^2) \\ &= \operatorname{diag}(a_1^2, a_1 b_1, a_1 b_1, b_1^2) + \operatorname{diag}(a_2^2, a_2 b_2, a_2 b_2, b_2^2) \\ &= F \otimes F + G \otimes G\end{aligned}$$

Therefore,

$$\begin{aligned}(1+\varepsilon)(E_1 \otimes E_1 + E_2 \otimes E_2 + E_3 \otimes E_3) - \varepsilon I_H \otimes I_H \\ = F \otimes F + G \otimes G + (1+\varepsilon)(E_2 \otimes E_2 + E_3 \otimes E_3)\end{aligned}$$

and

$$\begin{aligned}F^2 + G^2 + (1+\varepsilon)(E_2^2 + E_3^2) &= \mathrm{diag}(c^2, d^2) + (1+\varepsilon)(E_2^2 + E_3^2) \\ &= (1+\varepsilon)(E_1^2 + E_2^2 + E_3^2) - \varepsilon I_H \\ &= (1+\varepsilon)I_H - \varepsilon I_H = I_H\end{aligned}$$

Finally, if

$$(1-\varepsilon)\left(\sum_{i=1}^{n} E_i \otimes E_i\right) + \varepsilon I_H \otimes I_H = \sum_{i=1}^{3} E_i \otimes E_i$$

then $\sum E_i \otimes E_i = I_H$. It follows that $\mathcal{E} \notin \mathrm{Ext}\,[\mathcal{Q}_{\mathrm{pos}}(H)]$. □

References

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

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

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

[4] S. Gudder, Quantum mechanics on finite groups, *Found. Phys.* (to appear).

[5] S. Gudder, Duality quantum computers, *Quant. Info. Proc.* (to appear).

[6] M. Hirvensalo, *Quantum Computing*, Springer-Verlag, Berlin, 2001.

[7] G. L. Long, The general quantum interference principle and the duality computer, arxiv: quant-ph/0512120, 2005.

[8] G. L. Long, Mathematical theory of the duality computer in the density matrix formalism, arxiv: quant-ph/0605087, 2006.

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

[10] A. Y. Shiekh, The role of quantum interference in quantum computing, *Intern. J. Theor. Phys.* (to appear).