DUALITY QUANTUM COMPUTERS

Stan Gudder
Department of Mathematics
University of Denver
Denver, Colorado 80208
stan.gudder@nsm.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 and point out a paradoxical situation that occurs when mixed states are considered. It is shown that a duality quantum computer can measure itself without needing a separate measurement apparatus to determine its final state.

1 Introduction

In a recent paper, Gui Lu Long proposed a new type of quantum computer called a duality quantum computer [4]. 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.

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, 2, 3, 5]. 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 [4]. In particular, we discuss the nonunitarity of certain circuits in a duality quantum computer. We also point out a paradoxical situation that occurs when mixed states are considered for a duality quantum computer. Finally, we show that a duality quantum computer can measure itself without needing a separate measurement apparatus to determine its final state. 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 Divider and Combiner Operators

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 $\|p\| = (\sum p_i^2)^{1/2}$ 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**

Lemma 2.1. *The operator D_p is a linear isometry.*

Proof. It is clear that D_p is linear and D_p is an isometry because

$$\langle D_p\psi, D_p\phi\rangle = \frac{1}{\|p\|^2}\langle \oplus(p_i\psi), \oplus(p_i\phi)\rangle = \frac{1}{\|p\|^2}\sum p_i^2\langle\psi,\phi\rangle = \langle\psi,\phi\rangle \qquad \square$$

We conclude from Lemma 2.1 that D_p is a unitary operator from H onto its range $\mathcal{R}(D_p)$. Of course, $\dim \mathcal{R}(D_j) = \dim H$. In particular, if $\dim H = m < \infty$ and $\{\phi_1, \dots, \phi_m\}$ is an orthonormal basis for H then an orthonormal basis for $\mathcal{R}(D_p)$ is

$$\left\{ \frac{1}{\|p\|}(p_1\phi_1, \dots, p_n\phi_1), \cdots, \frac{1}{\|p\|}(p_1\phi_m, \dots, p_n\phi_m) \right\}$$

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

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

Again, C is a linear operator and we have that

$$\begin{aligned}\langle C(\psi_1 \oplus \cdots \oplus \psi_n), C(\phi_1 \oplus \cdots \oplus \phi_n)\rangle &= \left\langle \sum \psi_i, \sum \phi_j \right\rangle \\ &= \sum_{i,j} \langle \psi_i, \phi_j\rangle\end{aligned}$$

It follows that C is not an isometry. However, if we define C_p to be the restriction of $\|p\|C$ to $\mathcal{R}(D_p)$ then we have the following result.

Lemma 2.2. *The operator C_p is a linear isometry and $C_p = D_p^*$.*

Proof. To show that C_p is an isometry, we have that

$$\langle C_p(p_1\psi \oplus \cdots \oplus p_n\psi),\ C_p(p_1\phi \oplus \cdots \oplus p_n\phi)\rangle$$
$$= \|p\|^2\langle \psi, \phi\rangle = \langle p_1\psi \oplus \cdots \oplus p_n\psi, p_1\phi \oplus \cdots \oplus p_n\phi\rangle$$

To show that $C_p = D_p^*$ we have that

$$C_pD_p\psi = C_p\left[\frac{1}{\|p\|} \oplus (p_i\psi)\right] = \sum p_i\psi = \psi$$

Hence, $C_pD_p = I_H$ where I_H is the identity operator on H. □

We call C_p the **combiner operator**. Suppose we apply D_p and then a unitary operator U_i on each of the paths, $i = 1, \ldots, n$ 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. We now give another way to describe generalized quantum gates. Define the operator $\oplus_{i=1}^n U_i \colon H^{\oplus^n} \to H^{\oplus^n}$ by

$$\oplus U_i(\phi_1 \oplus \cdots \oplus \phi_n) = U_1\phi_1 \oplus \cdots \oplus U_n\phi_n$$

It is easy to check that $\oplus U_i$ is unitary and

$$\sum p_iU_i = \|p\|C(\oplus U_i)D_p$$

Denoting the set of generalized quantum gates on H by $\mathcal{G}(H)$, it is easy to show that $\mathcal{G}(H)$ is a convex set. Of course, any unitary operator on H is in $\mathcal{G}(H)$ and in particular $I_H \in \mathcal{G}(H)$. We would now like to show that I_H is an extreme point of $\mathcal{G}(H)$. That is, $\sum p_iU_i = I_H$ if and only if $U_i = I_H$ for all i. It is not hard to show that this latter result holds when $\dim H < \infty$ and the U_i mutually commute. Indeed, in this case the U_i are simultaneously diagonalizable with matrix representations

$$U_i = \operatorname{diag}(\lambda_{i1}, \ldots, \lambda_{im})$$

and since $\sum p_i U_i = I_H$ we have that $\sum_{i=1}^n p_i \lambda_{ij} = 1$, $j = 1, \ldots, m$. Hence, $\sum p_i \mathrm{Re}(\lambda_{ij}) = 1$ and it follows that $\mathrm{Re}(\lambda_{ij}) = 1$ for all i, j. Since $|\lambda_{ij}| = 1$ we have that $\lambda_{ij} = 1$ for all i, j so that $U_i = I_H$ for all i. We now give a more delicate argument to prove this result in general.

Theorem 2.3. *The identity I_H is an extreme point of $\mathcal{G}(H)$.*

Proof. Suppose that $\sum p_i U_i = I_H$. Letting $\psi \in H$ with $\|\psi\| = 1$ we have that $\sum p_i U_i \psi = \psi$. By Schwarz's inequality we obtain

$$\begin{aligned} 1 = \|\psi\|^2 &= \sum_{i,j} p_i p_j \langle U_i \psi, U_j \psi \rangle \leq \sum_{i,j} p_i p_j \left| \langle U_i \psi, U_j \psi \rangle \right| \\ &\leq \sum_{i,j} p_i p_j = \sum_i p_i \sum_j p_j = 1 \end{aligned}$$

Hence,

$$\sum_{i,j} p_i p_j \left| \langle U_i \psi, U_j \psi \rangle \right| = 1$$

Since $|\langle U_i \psi, U_j \psi \rangle| \leq 1$ we have that $|\langle U_i \psi, U_j \psi \rangle| = 1$ for all i, j. But then

$$|\langle U_i \psi, U_j \psi \rangle| = \|U_i \psi\| \, \|U_j \psi\|$$

so we have equality in Schwarz's inequality for all i, j. Hence, $U_i \psi = \alpha U_j \psi$ with $|\alpha| = 1$. Thus, there exist $\alpha_i \in \mathbb{C}$ with $|\alpha_i| = 1$ such that $U_i \psi = \alpha_i U_1 \psi$ for all i. We conclude that

$$\psi = \sum p_i U_i \psi = \left(\sum p_i \alpha_i \right) U_1 \psi$$

Therefore, for any unit vector ψ there exists an $\alpha_\psi \in \mathbb{C}$ with $|\alpha_\psi| = 1$ such that $U_1 \psi = \alpha_\psi \psi$; that is, every nonzero vector is an eigenvector of U_1. The only unitary operators with this property are αI_H, $|\alpha| = 1$. Hence, $U_1 = \alpha_1 I_H$ with $|\alpha_1| = 1$ and similarly $U_i = \alpha_i I$ with $|\alpha_i| = 1$, $i = 1, \ldots, n$. Therefore, $I_H = \sum p_i \alpha_i I_H$ so that $\sum p_i \alpha_i = 1$. But then $\sum p_i \mathrm{Re}(\alpha_i) = 1$ so that $\mathrm{Re}(\alpha_i) = 1$, $i, \ldots, n$. Hence, $\alpha_i = 1$ and we conclude that $U_i = I_H$, $i = 1, \ldots, n$. □

Corollary 2.4. *The extreme points of $\mathcal{G}(H)$ are precisely the unitary operators H.*

Proof. Suppose $A \in \mathcal{G}(H)$ is an extreme point. Then $A = \sum p_i U_i$ which implies that $U_i = A$ for all i so A is unitary. Conversely, suppose U is unitary. To show that U is an extreme point of $\mathcal{G}(H)$ assume that $U = \sum p_i U_i$. Then

$$I_H = UU^* = \left(\sum p_i U_i\right)\left(\sum p_j U_j\right)^* = \sum_{i,j} p_i p_j U_i U_j^*$$

Applying Theorem 2.3 we conclude that $U_i U_j^* = I_H$ for all i, j. In particular, $U_i = U_1$ for all i. Hence,

$$U = \sum p_i U_1 = U_1 = U_i$$

for all i. □

We conclude from Corollary 2.4 that except for a degenerate probability distribution, no generalized quantum gate is unitary; that is, no 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 $\psi_1, \ldots, \psi_N$ 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 [4].

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,

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

The next result shows that if $\dim H < \infty$ then a duality quantum computer can simulate any operator on H.

Theorem 2.5. *If* $\dim H < \infty$, *then* $\mathcal{B}(H) = \mathbb{R}^+\mathcal{G}(H)$.

Proof. For $A \in \mathcal{B}(H)$ we must show that there exists an $\alpha \geq 0$ such that $A = \alpha \sum p_i U_i$ where U_i are unitary and $(p_1, \ldots, p_n)$ is a probability distribution. If $A = 0$, then letting $\alpha = 0$ we are finished, so suppose $A \neq 0$. Let $P \in \mathcal{B}(H)$ be a projection operator. Let $\psi_1, \ldots, \psi_M$ be an orthonormal basis for $\mathcal{R}(P)$ and extend to an orthonormal basis $\psi_1, \ldots, \psi_N$ for H. Define the unitary operator U on H by

$$U\psi_i = \begin{cases} \psi_i & \text{if} \quad i = 1, \ldots, M \\ -\psi_i & \text{if} \quad i = M+1, \ldots, N \end{cases}$$

Then $P = \frac{1}{2}I_H + \frac{1}{2}U \in \mathcal{G}(H)$. Now let $A \in \mathcal{B}(H)$ be self-adjoint with distinct eigenvalues $\lambda_i \neq 0$ and let $a = \sum |\lambda_i|$. Let P_i be the projection onto the eigenspace for λ_i. Then there exist unitary operators U_i such that $P_i = \frac{1}{2}I_H + \frac{1}{2}U_i$. Hence,

$$\begin{aligned} A &= \sum \lambda_i P_i = a \sum \frac{\lambda i}{a} P_i = a \sum \frac{|\lambda_i|}{a} (\mathrm{sgn}\lambda_i) P_i \\ &= a \sum \frac{|\lambda_i|}{a} \,\mathrm{sgn}\lambda_i \left(\frac{1}{2} I_H + \frac{1}{2} U_i \right) \\ &= a \left[\sum \frac{|\lambda_i|}{2a} (\mathrm{sgn}\lambda_i) I_H + \sum \frac{|\lambda_i|}{2a} (\mathrm{sgn}\lambda_i) U_i \right] \end{aligned}$$

Now $(\mathrm{sgn}\lambda_i)I_H$ and $(\mathrm{sgn}\lambda_i)U_i$ are unitary and $a^{-1}\sum |\lambda_i| = 1$. Hence, A has the required form and of course, so does iA $\left(i = \sqrt{-1}\,\right)$. Now suppose A is an arbitrary operator on H. Then $A = B + iC$ where B and C are self-adjoint. Now from before we have that $B = b\sum p_i U_i$ and $C = c\sum q_i V_i$ in the required form. Thus,

$$\begin{aligned} A = B + iC &= (b+c)\left(\frac{1}{b+c}\, B + \frac{1}{b+c}\, iC \right) \\ &= (b+c)\left[\frac{b}{b+c} \sum p_i U_i + \frac{c}{b+c} \sum q_i V_i \right] \end{aligned}$$

Since

$$\frac{b}{b+c} \sum p_i + \frac{c}{b+c} \sum q_i = 1$$

we are finished. □

Corollary 2.6. *If* $\dim H < \infty$*, then* $A \in \mathcal{B}(H)$ *is normal if and only if* $A = \alpha \sum p_i U_i$ *where* $\alpha \geq 0$*,* $p_i > 0$*,* $\sum p_i = 1$ *and* U_i *are unitary operators that mutually commute.*

3 Mixed States

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

$$\sum p_i U_i \psi \Big/ \left\| \sum p_i U_i \psi \right\|$$

Notice that it was necessary to renormalize the vector $\sum p_i U_i \psi$ because $\sum p_i U_i$ 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, 2, 3, 5]. 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

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

Unfortunately, even when ρ is pure, $\mathcal{E}(\rho)$ is pure only under very special circumstances as the next result shows. The one-dimensional projection onto the subspace spanned by a unit vector ψ is denoted by P_ψ. Of course, P_ψ is a density operator representing the pure state ψ.

Theorem 3.1. *The state $\mathcal{E}(\rho)$ is pure if and only if $\rho = P_\psi$ is pure and there exists a unit vector ϕ and $\alpha_i \in \mathbb{C}$, $|\alpha_i| = 1$ such that $U_i\psi = \alpha_i\phi$ for every i.*

Proof. If the condition holds then

$$\begin{aligned}\mathcal{E}(\rho) &= \sum p_i U_i \rho U_i^* = \sum p_i U_i P_\psi U_i^* = \sum p_i P_{U_i\psi} \\ &= \sum p_i P_\phi = P_\phi\end{aligned}$$

Hence, $\mathcal{E}(\rho)$ is pure. Conversely, suppose $\mathcal{E}(\rho)$ is pure so that $\mathcal{E}(\rho) = P_\phi$. Then

$$\begin{aligned}\sum p_i \langle U_i^*\phi, \rho U_i^*\phi\rangle &= \sum p_i \langle \phi, U_i\rho U_i^*\phi\rangle = \langle \phi, \mathcal{E}(\rho)\phi\rangle \\ &= \langle \phi, P_\phi\phi\rangle = 1\end{aligned}$$

It follows that $\langle U_i^*\phi, \rho U_i^*\phi\rangle = 1$ for every i. Hence, $\rho = P_\psi$ for some unit vector ψ and ρ is pure. Moreover,

$$\langle \phi, P_{U_i\psi}\phi\rangle = \langle \phi, U_i P_\psi U_i^*\phi\rangle = 1$$

for every i. We conclude that $P_{U_i\psi} = P_\phi$ so that $U_i\psi = \alpha_i\phi$ with $|\alpha_i| = 1$ for every i. □

It follows from Theorem 3.1 that this approach for mixed states is not a generalization of the previous approach where we had $\psi \mapsto (\sum p_i U_i)\,\psi$. In fact, we can show this directly as follows. If $\rho = P_\psi$ is a pure state then

$$\mathcal{E}(\rho) = \mathcal{E}(P_\psi) = \sum p_i U_i P_\psi U_i^* = \sum p_i P_{U_i\psi}$$

which is a lot different than $(\sum p_i U_i)\,\psi$. The two approaches are equivalent if and only if $\sum p_i P_{U_i\psi}$ is a one-dimensional projection for every unit vector ψ. But this holds if and only if all the U_i coincide up to multiplicative constants of modulus 1. But then

$$\mathcal{E}(\rho) = \sum P_i U_1 P_\psi U_1^* = \sum p_i P_{U_1\psi} = P_{U_1\psi}$$

which is an ordinary quantum computer.

This gives a definite puzzle of how to treat mixed states in a duality quantum computer. If we are to truly understand duality quantum computers, this paradox must be resolved. Notice that for ordinary quantum computers there is no such paradox. In this case there is only one path and pure

states are transformed by $\psi \mapsto U\psi$ while mixed states are transformed by $\rho \mapsto U\rho U^*$. Representing a pure state ψ by P_ψ we have

$$P_\psi \mapsto U P_\psi U^* = P_{U\psi}$$

which is equivalent to $U\psi$. Thus, the two approaches are equivalent for an ordinary quantum computer.

Moreover, in this second approach we seem to lose the greater power contained in the first approach. For example, in the vector selection algorithm we have that $U_1 = I_H$ and $U_2\psi_i = -(-1)^{\delta_{i,k}}\psi_i$ as before. Again, if the initial state is the uniform superposition ψ then

$$\mathcal{E}(P_\psi) = \frac{1}{2}\, P_{U_1\psi} + \frac{1}{2}\, P_{U_2\psi} = \frac{1}{2}\, P_\psi + \frac{1}{2}\, P_{U_2\psi}$$

If we now measure the basis $\psi_1, \ldots, \psi_N$ then we have N possible outcomes each with probability

$$\langle \mathcal{E}(P_\psi)\psi_k, \psi_i\rangle = \frac{1}{2}\, |\langle \psi, \psi_i\rangle|^2 + \frac{1}{2}\, |\langle U_2\psi, \psi_i\rangle|^2 = \frac{1}{2N} + \frac{1}{2N} = \frac{1}{N}$$

This gives no information at all. In general, the state $\mathcal{E}(\rho) = \sum p_i U_i \rho U_i^*$ is a mixture of states on each path so $\mathcal{E}(\rho)$ is a mixture of states each of which evolves according to an ordinary quantum computer. Thus, $\mathcal{E}(\rho)$ cannot give more information about the result of a computation than an ordinary quantum computer.

Long mentions that the decomposition into subwaves can be iterated so that any subwave can be further decomposed into sub-subwaves [4]. In this way, more complex duality quantum computers can be constructed. However, as we now show, these iterations do not give anything new that cannot already be accomplished with a single decomposition into subwaves. For example, after producing $\psi \mapsto \|p\|^{-1} \oplus p_i U_i \psi$ suppose we apply a divider operator to the first path to obtain

$$\left(\frac{1}{\|p\|\,\|q\|} p_1 \bigoplus_{j=1}^{m} q_j V_j U_1 \psi\right) \oplus \left(\frac{1}{\|p\|} \bigoplus_{i=2}^{n} p_i U_i \psi\right)$$

After applying the combiner operator we obtain

$$p_1 \sum_{j=1}^{m} q_j V_j U_1 \psi + \sum_{i=2}^{n} p_i U_i \psi$$

But this can be obtained using the single generalized quantum gate

$$\sum_{j=1}^{m} p_1 q_j V_j U_1 + \sum_{i=2}^{n} p_i U_i$$

4 Projective Measurements

This section shows 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 4.1. *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 [5] 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 $E_j = \sum_k u_{kj} F_k$ for all i, j. Letting $i = \sqrt{-1}$, the discrete Fourier transform is given by the unitary $n \times n$ matrix $\left[n^{-1/2} e^{2\pi i j k/n}\right]$. Define the unitary operators U_j, $j = 1, \ldots, n$, by

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

We can then write

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

Applying the unitary freedom theorem, we conclude that

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

References

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

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

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

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

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