Quantum Computation and Quantum Information

-Michael A. Nielsen and Isaac L. Chuang

Chapter 8. Quantum Noise and Quantum Operations

Solutions

8.1: (Unitary evolution as a quantum operation) Pure states evolve under unitary transforms as $|\psi\rangle \to U|\psi\rangle$. Show that, equivalently, we may write $\rho \to \mathcal{E}(\rho) \equiv U\rho U^\dagger$, for $\rho = |\psi\rangle\langle\psi|$.

Pure states evolve under unitary transforms as $|\psi\rangle \to U|\psi\rangle$. Suppose the initial state is $|\psi\rangle$ and the evolved state is $|\zeta\rangle = U|\psi\rangle$. Then, in terms of density we can write the evolved state as $\rho_{\text{ev}} = |\zeta\rangle\langle\zeta| = U|\psi\rangle\langle\psi|U^\dagger = U\rho U^\dagger \equiv \mathcal{E}(\rho)$. Hence, $\rho \to \mathcal{E}(\rho)$.

8.2: (Measurement as a quantum operation) Recall from section 2.2.3 (on page 84) that a quantum measurement with outcomes labeled as m is described by a set of measurement operators M_m such that $\sum_m M_m^\dagger M_m = I$. Let the state of the system immediately before the measurement be ρ. Show that for $\mathcal{E}_m(\rho) \equiv M_m \rho M_m^\dagger$, the state of the system immediately after the measurement is $\frac{\mathcal{E}_m(\rho)}{\text{tr}(\mathcal{E}_m(\rho))}$. Also show that the probability of obtaining this measurement result is $p(m) = \text{tr}\big(\mathcal{E}_m(\rho)\big)$.

First we show that given the state ρ before measurement, the probability of getting the outcome labeled m is $p(m) = \text{tr}(\mathcal{E}_m(\rho)) \equiv \text{tr}(M_m \rho M_m^\dagger)$.
Suppose the quantum system is initially in one of a number of states $|\psi_i\rangle$ with respective probabilities p_i. Then $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.
Using the law of total probability and linearity of trace, the probability of obtaining outcome m given the initial state $|\psi_i\rangle$ (for any index i) is

$$p(m) = \sum_i p(m \mid i) p_i = \sum_i p_i \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \sum_i p_i \text{tr}\big(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\big)$$
$$= \text{tr}\Big(\sum_i p_i M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\Big) = \text{tr}\Big(M_m^\dagger M_m \underbrace{\sum_i p_i |\psi_i\rangle\langle\psi_i|}_{=\rho}\Big) = \text{tr}\big(M_m^\dagger M_m \rho\big) = \text{tr}\big(M_m \rho M_m^\dagger\big) \equiv \text{tr}\big(\mathcal{E}_m(\rho)\big)$$

where $\text{tr}\big(M_m^\dagger M_m \rho\big) = \text{tr}\big(M_m \rho M_m^\dagger\big)$ by the cyclic property of trace. Hence, we have shown that $p(m) = \text{tr}\big(\mathcal{E}_m(\rho)\big)$. Next, we show that the state of the system immediately after the measurement is $\frac{\mathcal{E}_m(\rho)}{\text{tr}(\mathcal{E}_m(\rho))}$.
If the initial state of the quantum system was $|\psi_i\rangle$ (for any i) then the state after obtaining the outcome m is

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}}$$

Hence, we have an ensemble of states $|\psi_i^m\rangle$ with probabilities $p(i \mid m)$. Hence, the corresponding density operator ρ_m after the measurement is

$$\rho_m = \sum_i p(i \mid m) |\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i \mid m) \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}$$

By elementary probability theory we have $p(i \mid m) = p(m,i)/p(m) = p(m \mid i) p_i / p(m)$. We know $p(m \mid i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle$ and $p(m) = \text{tr}\big(\mathcal{E}_m(\rho)\big)$.

Hence,

$$\rho_m = \sum_i p(i \mid m) \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle} = \sum_i \frac{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle p_i}{\text{tr}\big(\mathcal{E}_m(\rho)\big)} \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle} = \sum_i p_i \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\text{tr}\big(\mathcal{E}_m(\rho)\big)}$$
$$\Rightarrow \rho_m = \frac{M_m \left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right) M_m^\dagger}{\text{tr}\big(\mathcal{E}_m(\rho)\big)} = \frac{M_m \rho M_m^\dagger}{\text{tr}\big(\mathcal{E}_m(\rho)\big)} \equiv \frac{\mathcal{E}_m(\rho)}{\text{tr}\big(\mathcal{E}_m(\rho)\big)}$$

Hence, the state of the system immediately after measurement is $\frac{\mathcal{E}_m(\rho)}{\text{tr}\left(\mathcal{E}_m(\rho)\right)}$.

8.3: Our derivation of the operator-sum representation implicitly assumed that the input and output spaces for the operation were the same. Suppose a composite system AB initially in an unknown quantum state ρ is brought into contact with a composite system CD initially in some standard state $|0\rangle$, and the two systems interact according to a unitary interaction U. After the interaction we discard systems A and D, leaving a state ρ' of system BC. Show that the map $\mathcal{E}(\rho) = \rho'$ satisfies $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ for some set of linear operators E_k from the state space of system AB to the state space of system BC, and such that $\sum_k E_k^\dagger E_k = I$.

Note: In Nielsen & Chuang (NC) the partial trace involved in the formalism of the operator-sum representation is a little confusing. NC starts with $|e_k\rangle$ as the orthonormal basis of the state space of the environment and $\rho_{\text{env}} = |e_0\rangle\langle e_0|$ as the initial state of the environment and justifies that there's no loss of generality in assuming that the system starts in a pure state. Suppose ρ is a state in the principal system under consideration. Then the operation $\mathcal{E}$ on the state is represented as

$$\mathcal{E}(\rho) = \sum_k \langle e_k| U \left(\rho \otimes |e_0\rangle\langle e_0|\right) U^\dagger |e_k\rangle = \sum_k E_k \rho E_k^\dagger \tag{1}$$

where $E_k \equiv \langle e_k|U|e_0\rangle$ is an operator on the state space of the principal system. I think it adds a little more clarity in writing E_k as $E_k \equiv \langle I \otimes e_k|U|I \otimes e_0\rangle$, where I is an identity in the state space of the principal system. This is because U is an operator in the product space of the principal system and the environment (indeed, it operates on $\rho \otimes |e_0\rangle\langle e_0|$), whereas $|e_k\rangle$ is an orthonormal basis in the state space of the environment.
Next, we justify below the use of $E_k \equiv \langle I \otimes e_k|U|I \otimes e_0\rangle$.
We expand $\rho \otimes |e_0\rangle\langle e_0|$ into product and re-arrange the terms as shown below. I_{env} is an identity in the state space of the environment. Also, we make use of the property of tensor product: $(A \otimes B)(C \otimes D) = AC \otimes BD$.

$$\begin{aligned}
\rho \otimes |e_0\rangle\langle e_0| &= (\rho I) \otimes (I_{\text{env}}|e_0\rangle\langle e_0|I_{\text{env}}) = (\rho \otimes I_{\text{env}}|e_0\rangle)(I \otimes \langle e_0|I_{\text{env}}) = (\rho \otimes I_{\text{env}})(I \otimes |e_0\rangle)(I \otimes \langle e_0|)(I \otimes I_{\text{env}}) \\
&= (\rho \otimes I_{\text{env}})(I \otimes |e_0\rangle)(I \otimes \langle e_0|) = (\underbrace{\rho I}_{=I\rho} \otimes \underbrace{I_{\text{env}}|e_0\rangle}_{=|e_0\rangle})(I \otimes \langle e_0|) = (I\rho \otimes |e_0\rangle)(I \otimes \langle e_0|) = (I \otimes |e_0\rangle)\rho(I \otimes \langle e_0|) \\
&\Rightarrow \rho \otimes |e_0\rangle\langle e_0| \equiv (I \otimes |e_0\rangle)\rho(I \otimes \langle e_0|) \qquad (\star)
\end{aligned}$$

Next, we substitute this result and rewrite (1) as

$$\mathcal{E}(\rho) = \sum_k (I \otimes \langle e_k|)U[(I \otimes |e_0\rangle)\rho(I \otimes \langle e_0|)]U^\dagger(I \otimes |e_k\rangle) = \sum_k \underbrace{(I \otimes \langle e_k|)U(I \otimes |e_0\rangle)}_{\equiv E_k}\rho\underbrace{(I \otimes \langle e_0|)U^\dagger(I \otimes |e_k\rangle)}_{\equiv E_k^\dagger} = \sum_k E_k \rho E_k^\dagger$$

where $E_k \equiv (I \otimes \langle e_k|)U(I \otimes |e_0\rangle)$. We can drop the identity I and write $E_k \equiv \langle e_k|U|e_0\rangle$. This is because, by the principle of implicit measurement, $\langle e_k| \cdot |e_0\rangle$ only affects the state of the environment and doesn't change the state of the principal system. And this is more clearly expressed in $(I \otimes \langle e_k|)U(I \otimes |e_0\rangle)$

The solution to the given problem is as follows.
Suppose $|a\rangle$, $|b\rangle$, $|c\rangle$, $|d\rangle$ are the orthonormal bases of the state space of systems A, B, C, D respectively. The composite system AB is in the unknown state ρ_{AB} and the composite system CD is in the standard state $|0\rangle_{CD}$ which is equivalent to $|0\rangle\langle 0|_{CD} \equiv |0\rangle|0\rangle\langle 0|\langle 0|_{CD} \equiv |0\rangle\langle 0|_C \otimes |0\rangle\langle 0|_D$. Next, the system AB interacts with the system CD according to a unitary interaction U. The interaction can be denoted as $U(\rho_{AB} \otimes |00\rangle\langle 00|_{CD})U^\dagger$. We then discard systems A and D by carrying out the partial trace $\text{tr}_{AD}\Big(U(\rho_{AB} \otimes |00\rangle\langle 00|_{CD})U^\dagger\Big)$. This can be rewritten as the quantum operation $\mathcal{E}(\rho_{AB})$ that leaves a state ρ'_{BC} in the state space of BC. We show that the operation $\mathcal{E}(\cdot)$ satisfies $\mathcal{E}(\rho_{AB}) = \sum_k E_k \rho_{AB} E_k^\dagger$.

$$\mathcal{E}(\rho_{AB}) = \sum_{ad} \left(\langle a| \otimes \underbrace{I_B \otimes I_C}_{=I_{BC}} \otimes \langle d|\right) U(\rho_{AB} \otimes |00\rangle\langle 00|_{CD})U^\dagger\left(|a\rangle \otimes \underbrace{I_B \otimes I_C}_{=I_{BC}} \otimes |d\rangle\right) \tag{2}$$

Next, we note that $\rho_{AB} \otimes |00\rangle\langle 00|_{CD} \equiv (I_{AB} \otimes |00\rangle_{CD})\rho_{AB}(I_{AB} \otimes \langle 00|_{CD})$ using $(\star)$ in the note above.

Therefore, we can rewrite (2) as shown in (3).

$$\mathscr{E}(\rho_{AB}) = \sum_{ad} \underbrace{\left(\langle a| \otimes I_{BC} \otimes \langle d|\right) U \left(I_{AB} \otimes |00\rangle_{CD}\right)}_{=E_{ad}} \rho_{AB} \underbrace{\left(I_{AB} \otimes \langle 00|_{CD}\right) U^\dagger \left(|a\rangle \otimes I_{BC} \otimes |d\rangle\right)}_{=E^\dagger_{ad}} \tag{3}$$

We can re-index $(a,d) \equiv k$ and write the linear operator E_{ad} as

$$E_k \equiv E_{ad} = \left(\langle a| \otimes I_{BC} \otimes \langle d|\right) U \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) \tag{4}$$

Thus, we can write $\mathscr{E}(\rho_{AB}) = \sum_k E_k \rho_{AB} E_k^\dagger$. The operator E_k maps states in the system AB to those in the system BC. Next, we show that $\sum_k E_k^\dagger E_k = I$.

$$\sum_k E_k^\dagger E_k \equiv \sum_{ad} E^\dagger_{ad} E_{ad} = \sum_{ad} \left(I_{AB} \otimes \langle 0|_C \otimes \langle 0|_D\right) U^\dagger \underbrace{\left(|a\rangle \otimes I_{BC} \otimes |d\rangle\right)\left(\langle a| \otimes I_{BC} \otimes \langle d|\right)}_{=|a\rangle\langle a| \otimes I_{BC} \otimes |d\rangle\langle d| \quad (\star\star)} U \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) \tag{5}$$

We show $(\star\star)$. We use the tensor product property $(A \otimes B)(C \otimes D) = AC \otimes BD$.

$$\left(|a\rangle \otimes I_{BC} \otimes |d\rangle\right)\left(\langle a| \otimes I_{BC} \otimes \langle d|\right) = \left(|a\rangle \otimes I_{BC}\right)\left(\langle a| \otimes I_{BC}\right) \otimes |d\rangle\langle d| = |a\rangle\langle a| \otimes I_{BC} \otimes |d\rangle\langle d|$$

Rewriting (5) we have

$$\begin{aligned}
\sum_k E_k^\dagger E_k \equiv \sum_{ad} E^\dagger_{ad} E_{ad} &= \sum_{ad} \left(I_{AB} \otimes \langle 0|_C \otimes \langle 0|_D\right) U^\dagger \left(|a\rangle\langle a| \otimes I_{BC} \otimes |d\rangle\langle d|\right) U \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) \\
&= \left(I_{AB} \otimes \langle 0|_C \otimes \langle 0|_D\right) U^\dagger \sum_{ad} \Big(|a\rangle\langle a| \otimes I_{BC} \otimes |d\rangle\langle d|\Big) U \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) \\
&= \left(I_{AB} \otimes \langle 0|_C \otimes \langle 0|_D\right) U^\dagger \sum_{ad} \Big(|a\rangle\langle a| \otimes \big(\sum_{bc} |bc\rangle\langle bc|\big) \otimes |d\rangle\langle d|\Big) U \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) \quad \left(\text{Using } I_{BC} = \sum_{bc} |bc\rangle\langle bc|\right) \\
&= \left(I_{AB} \otimes \langle 0|_C \otimes \langle 0|_D\right) U^\dagger \sum_{abcd} \big(\underbrace{|a\rangle\langle a| \otimes |bc\rangle\langle bc| \otimes |d\rangle\langle d|}_{=|abcd\rangle\langle abcd|}\big) U \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) \\
&= \left(I_{AB} \otimes \langle 0|_C \otimes \langle 0|_D\right) U^\dagger \underbrace{\sum_{abcd} |abcd\rangle\langle abcd|}_{=I_{ABCD}} U \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) \\
&= \left(I_{AB} \otimes \langle 0|_C \otimes \langle 0|_D\right) \underbrace{U^\dagger I_{ABCD} U}_{\substack{=U^\dagger U \\ =I_{ABCD}}} \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) = \left(I_{AB} \otimes \langle 0|_C \otimes \langle 0|_D\right)\left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right) \\
&= \left(I_{AB} \otimes \langle 00|_{CD}\right)\left(I_{AB} \otimes |00\rangle_{CD}\right) = I_{AB} I_{AB} \otimes \langle 00|00\rangle_{CD} = I_{AB}
\end{aligned}$$

Hence, we have shown that $\sum_k E_k^\dagger E_k \equiv \sum_{ad} E^\dagger_{ad} E_{ad} = I_{AB}$ where $E_{ad} = \left(\langle a| \otimes I_{BC} \otimes \langle d|\right) U \left(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\right)$. We can drop the identities and rewrite $E_{ad} = \langle a| \langle d| U |0\rangle_C |0\rangle_D$.

> **8.4: (Measurement)** Suppose we have a single qubit principal system, interacting with a single qubit environment through the transform $U = P_0 \otimes I + P_1 \otimes X$, where X is the usual Pauli matrix (acting on the environment), and $P_0 \equiv |0\rangle\langle 0|$, $P_1 \equiv |1\rangle\langle 1|$ are projectors (acting on the system). Give the quantum operation for this process, in the operator-sum representation, assuming the environment starts in the state $|0\rangle$.

Suppose the system is in an unknown state ρ. The environment starts in the pure state $|0\rangle\langle 0|$. The Pauli matrix X has the property $X^2 = I$. Also, $P_0 P_1 = |0\rangle\langle 0|1\rangle\langle 1| = 0 = P_1 P_0$. We show that the transform $U = P_0 \otimes I + P_1 \otimes X$ is unitary, i.e. $U^\dagger U = I$.

$$U^\dagger U = \left(P_0 \otimes I + P_1 \otimes X\right)^\dagger \left(P_0 \otimes I + P_1 \otimes X\right) = \left(P_0 \otimes I + P_1 \otimes X^\dagger\right)\left(P_0 \otimes I + P_1 \otimes X\right) = \left(P_0 \otimes I + P_1 \otimes X\right)\left(P_0 \otimes I + P_1 \otimes X\right)$$
$$= \left(P_0 \otimes I\right)\left(P_0 \otimes I\right) + \left(P_0 \otimes I\right)\left(P_1 \otimes X\right) + \left(P_1 \otimes X\right)\left(P_0 \otimes I\right) + \left(P_1 \otimes X\right)\left(P_1 \otimes X\right)$$
$$\Rightarrow U^\dagger U = \left(P_0^2 \otimes I^2\right) + P_0 P_1 \otimes IX + P_1 P_0 \otimes XI + P_1^2 \otimes X^2 = P_0 \otimes I + P_1 \otimes I = \underbrace{\left(P_0 + P_1\right)}_{=I} \otimes I = I \otimes I = I$$

Next, we express the quantum operation for the process in the operator-sum representation. We perform the following partial trace with respect to the environment. From equations (8.9) and (8.10) in Nielsen and Chuang we have

$$\mathscr{E}(\rho) = \mathrm{tr}_{\mathrm{env}}\left(U\left(\rho \otimes |0\rangle\langle 0|\right)U^\dagger\right) = \sum_{k=0}^{1} \langle k|U\left(\rho \otimes |0\rangle\langle 0|\right)U^\dagger|k\rangle = \sum_{k=0}^{1} \underbrace{\langle k|U|0\rangle}_{=E_k} \rho \underbrace{\langle 0|U^\dagger|k\rangle}_{=E_k^\dagger}$$

As shown in the solution to problem 8.3 we can write $E_k = \langle k|U|0\rangle \equiv \left(I \otimes \langle k|\right)U\left(I \otimes |0\rangle\right)$.

$$E_k = \left(I \otimes \langle k|\right)U\left(I \otimes |0\rangle\right) = \left(I \otimes \langle k|\right)\left(P_0 \otimes I + P_1 \otimes X\right)\left(I \otimes |0\rangle\right)$$
$$\Rightarrow E_k = \left(I \otimes \langle k|\right)\left(P_0 \otimes I\right)\left(I \otimes |0\rangle\right) + \left(I \otimes \langle k|\right)\left(P_1 \otimes X\right)\left(I \otimes |0\rangle\right) = \left(IP_0 \otimes \langle k|I\right)\left(I \otimes |0\rangle\right) + \left(IP_1 \otimes \langle k|X\right)\left(I \otimes |0\rangle\right)$$
$$\Rightarrow E_k = P_0 \otimes \langle k|I|0\rangle + P_1 \otimes \langle k|X|0\rangle$$

Since the environment is single qubit, $k = 0, 1$. Hence,

$$E_0 = P_0 \otimes \underbrace{\langle 0|I|0\rangle}_{=1} + P_1 \otimes \underbrace{\langle 0|X|0\rangle}_{=0} = P_0$$
$$E_1 = P_0 \otimes \underbrace{\langle 1|I|1\rangle}_{=0} + P_1 \otimes \underbrace{\langle 1|X|1\rangle}_{=1} = P_1$$

Therefore, $E_k = P_k \equiv |k\rangle\langle k|$ for $k = 0, 1$. Hence, the quantum operation in the operator-sum representation is

$$\mathscr{E}(\rho) = \sum_{k=0}^{1} E_k \rho E_k^\dagger = \sum_{k=0}^{1} P_k \rho P_k^\dagger = P_0 \rho P_0^\dagger + P_1 \rho P_1^\dagger$$

8.5: (Spin flips) Just as in the previous exercise, but now let $U = \frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X$. Give the quantum operation for this process in the operator-sum representation.

X, Y, Z are the Pauli matrices. Suppose the system is in the unknown state ρ. We know $X^2 = Y^2 = Z^2 = I$. Also, $XY = iZ$ and $YX = -iZ$.
First, we show that the transform U is unitary

$$U^\dagger U = \left(\frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X\right)^\dagger \left(\frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X\right) = \left(\frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X\right)\left(\frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X\right)$$
$$\Rightarrow U^\dagger U = \frac{X^2}{2} \otimes I + \frac{XY}{2} \otimes IX + \frac{YX}{2} \otimes XI + \frac{Y^2}{2} \otimes X^2 = \frac{I_s^2}{2} \otimes I + \frac{iZ}{2} \otimes X - \frac{iZ}{2} \otimes X + \frac{I_s^2}{2} \otimes X^2 = \frac{I_s^2}{2} \otimes I + \frac{I_s^2}{2} \otimes I = I$$

Note that I_s and I are the identity matrices in the state space of the system and the environment respectively. Hence, we have shown that $U = \frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X$ is unitary.
Just as in the previous exercise, we can find the expressions for E_k as shown below.

$$E_k = \left(I \otimes \langle k|\right)U\left(I \otimes |0\rangle\right) = \left(I \otimes \langle k|\right)\left(\frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X\right)\left(I \otimes |0\rangle\right)$$
$$= (I \otimes \langle k|)\left(\frac{X}{\sqrt{2}} \otimes I\right)(I \otimes |0\rangle) + (I \otimes \langle k|)\left(\frac{Y}{\sqrt{2}} \otimes X\right)(I \otimes |0\rangle) = \left(\frac{X}{\sqrt{2}} \otimes \langle k|I\right)(I \otimes |0\rangle) + \left(\frac{Y}{\sqrt{2}} \otimes \langle k|X\right)(I \otimes |0\rangle)$$

$$\Rightarrow E_k = \frac{X}{\sqrt{2}} \otimes \langle k| I |0\rangle + \frac{Y}{\sqrt{2}} \otimes \langle k| X |0\rangle \quad k = 0,1$$
$$\Rightarrow E_0 = \frac{X}{\sqrt{2}} \otimes \underbrace{\langle 0| I |0\rangle}_{=1} + \frac{Y}{\sqrt{2}} \otimes \underbrace{\langle 0| X |0\rangle}_{=0} = \frac{X}{\sqrt{2}}$$
$$E_1 = \frac{X}{\sqrt{2}} \otimes \underbrace{\langle 1| I |0\rangle}_{=0} + \frac{Y}{\sqrt{2}} \otimes \underbrace{\langle 1| X |0\rangle}_{=1} = \frac{Y}{\sqrt{2}}$$

Therefore, the operator-sum representation of the quantum operation is

$$\mathscr{E}(\rho) = \sum_{k=0}^{1} E_k \rho E_k^\dagger = \frac{X}{\sqrt{2}}\rho\frac{X^\dagger}{\sqrt{2}} + \frac{Y}{\sqrt{2}}\rho\frac{Y^\dagger}{\sqrt{2}} = \frac{X}{\sqrt{2}}\rho\frac{X}{\sqrt{2}} + \frac{Y}{\sqrt{2}}\rho\frac{Y}{\sqrt{2}}$$

8.6: (Composition of quantum operations) Suppose $\mathscr{E}$ and $\mathscr{F}$ are quantum operations on the same quantum system. Show that the composition $\mathscr{F} \circ \mathscr{E}$ is a quantum operation, in the sense that it has an operator-sum representation. State and prove an extension of this result to the case where $\mathscr{E}$ and $\mathscr{F}$ do not necessarily have the same input and output spaces.

First we show the result when $\mathscr{E}$ and $\mathscr{F}$ have the same input and output spaces. Suppose the principal system is in the unknown state ρ. The operation $\mathscr{E}$ on ρ results in the state ρ' in the same state space of the principal system. The operator-sum representation of the operation $\mathscr{E}(\cdot)$ is $\rho' = \mathscr{E}(\rho) = \sum_k E_k \rho E_k^\dagger$. Next, the operation $\mathscr{F}$ on the state ρ' results in the state ρ'' in the state space of the principal system. The operator-sum representation of the operation $\mathscr{F}(\cdot)$ is

$$\rho'' = \mathscr{F}(\rho') = \mathscr{F}\left(\mathscr{E}(\rho)\right) = \sum_l F_l \mathscr{E}(\rho) F_l^\dagger = \sum_l F_l \sum_k E_k \rho E_k^\dagger F_l^\dagger = \sum_{kl} F_l E_k \rho E_k^\dagger F_l^\dagger = \sum_{kl} F_l E_k \rho (F_l E_k)^\dagger$$

Hence, $\mathscr{F} \circ \mathscr{E}$ is a quantum operation, $\mathscr{F} \circ \mathscr{E}\left(\rho\right) = \sum_{kl} F_l E_k \rho (F_l E_k)^\dagger$. The operators $\{F_l E_k\}$ are the operation elements for the quantum operation $\mathscr{F} \circ \mathscr{E}$.

> **8.7:** Suppose that instead of doing a projective measurement on the combined principal system and environment we had performed a general measurement described by measurement operators $\{M_m\}$. Find operator-sum representations for the corresponding quantum operations $\mathcal{E}_m$ on the principal system, and show that the respective measurement probabilities are $\mathrm{tr}[\mathcal{E}_m(\rho)]$.

Suppose the principal system Q is in the unknown state ρ and the environment E is in the initial standard state σ. Then the joint state of the principal system and environment is $\rho_{QE} = \rho \otimes \sigma$. The systems interact according to some unitary interaction U. After the interaction a measurement M_m is performed on the joint system. We then perform a partial trace with respect to the environment to obtain the state of the principal system alone. Hence, the quantum operation $\mathcal{E}_m(\cdot)$ corresponding to the outcome m on the state ρ of the principal system is given as

$$\mathcal{E}_m(\rho) = \mathrm{tr}_{\mathrm{E}}\Big(M_m U\big(\rho_{QE}\big)U^\dagger M^\dagger\Big) = \mathrm{tr}_{\mathrm{E}}\Big(M_m U\big(\rho\otimes\sigma\big)U^\dagger M^\dagger\Big) = \sum_k \langle e_k|\Big(M_m U\big(\rho\otimes\sigma\big)U^\dagger M^\dagger\Big)|e_k\rangle$$

where $|e_k\rangle$ is the orthonormal basis of the environment.
Suppose the state σ of the environment has an ensemble decomposition $\sigma = \sum_j q_j |j\rangle\langle j|$. Hence, we have

$$\begin{aligned}\mathcal{E}_m(\rho) &= \sum_k \langle e_k|\Big(M_m U\big(\rho\otimes\sum_j q_j|j\rangle\langle j|\big)U^\dagger M_m^\dagger\Big)|e_k\rangle = \sum_{kj} q_j\langle e_k|\Big(M_m U\big(\rho\otimes|j\rangle\langle j|\big)U^\dagger M_m^\dagger\Big)|e_k\rangle \\ \Rightarrow \mathcal{E}_m(\rho) &\underbrace{=}_{\substack{\text{Using}\\ \text{(8.9) and (8.10)}\\ \text{in NC}}} \sum_{kj} \underbrace{\sqrt{q_j}\langle e_k|M_m U|j\rangle}_{=E_{kj}}\,\rho\,\underbrace{\sqrt{q_j}\langle j|U^\dagger M_m^\dagger|e_k\rangle}_{=E_{kj}^\dagger}\end{aligned}$$

Hence, we have an operator-sum representation for the quantum operation $\mathcal{E}_m(\cdot)$, given as $\mathcal{E}_m(\rho) = \sum_{kj} E_{kj}\rho E_{kj}^\dagger$ with $E_{kj} \equiv \sqrt{q_j}\langle e_k|M_m U|j\rangle$.
Next, we show that the respective measurement probabilities are $\mathrm{tr}[\mathcal{E}_m(\rho)]$. The evolution and measurement of the joint state ρ_{QE} of the combined system is shown below.

$$\rho_{QE} \xrightarrow[\text{Interaction}]{U} \rho'_{QE} \equiv U\big(\rho\otimes\sigma\big)U^\dagger \xrightarrow[\text{Measurement}]{M_m} M_m U\big(\rho\otimes\sigma\big)U^\dagger M_m^\dagger \xrightarrow[\text{wrt } E]{\text{Partial trace}} \mathrm{tr}_E\Big(M_m U\big(\rho\otimes\sigma\big)U^\dagger M_m^\dagger\Big)$$

Next, upon performing trace with respect to the principal system Q we obtain the probability $p(m)$ for the outcome m, i.e.

$$p(m) = \mathrm{tr}_Q\Big(\underbrace{\mathrm{tr}_E\Big(M_m U\big(\rho\otimes\sigma\big)U^\dagger M_m^\dagger\Big)}_{\equiv\mathcal{E}_m(\rho)}\Big) = \mathrm{tr}_Q\left(\mathcal{E}_m(\rho)\right)$$

> **8.8: (Non-trace-preserving quantum operations)** Explain how to construct a unitary operator for a system-environment model of a non-trace-preserving quantum operation, by introducing an extra operator, E_∞, into the set of operation elements E_k, chosen so that when summing over the complete set of k, including $k=\infty$, one obtains $\sum_k E_k^\dagger E_k = I$.

Suppose $\mathcal{E}(\cdot)$ is a non-trace-preserving quantum operation, with operator-sum representation generated by operation elements $\{E_k\}$ satisfying $\sum_k E_k^\dagger E_k < I$. We introduce an extra operator, E_∞, into the set $\{E_k\}$ such that the sum over the complete index set k (including $k=\infty$) satisfies $\sum_{1\le k\le\infty} E_k^\dagger E_k = I$. We want to find an appropriate unitary operator U for a system-environment model of a non-trace-preserving operation. Let $|e_k\rangle$ be an orthonormal basis set for the environment E, in one-to-one correspondence with the index k for the operators E_k.

Note: NC has given the derivation for trace-preserving operations. Some details have been glossed over in equation (8.38). The operator U (later shown to be unitary) is defined in (8.37) as having the following action on states of the form $|\psi\rangle|e_0\rangle$ (where $|e_0\rangle$ is a standard state of the environment),

$$U|\psi\rangle|e_0\rangle \equiv \sum_k E_k|\psi\rangle|e_k\rangle \tag{6}$$

From (6) it looks like the operator E_k acts on the state $|\psi\rangle|e_k\rangle$. However, it is important to note that E_k acts only on states of the principal system. Hence, (6) is more like

$$U|\psi\rangle|e_0\rangle \equiv \sum_k (E_k \otimes I)(|\psi\rangle \otimes |e_k\rangle)$$

Then for arbitrary states $|\psi\rangle$ and $|\phi\rangle$ of the principal system we have

$$\langle\psi|\langle e_0|U^\dagger U|\phi\rangle|e_0\rangle = \sum_j (\langle\psi|\otimes\langle e_j|)\underbrace{(E_j\otimes I)^\dagger}_{=E^\dagger\otimes I}\sum_k (E_k\otimes I)(|\phi\rangle\otimes|e_k\rangle) = \sum_j (\langle\psi|E_j^\dagger\otimes\langle e_j|)\sum_k (E_k|\phi\rangle\otimes|e_k\rangle)$$
$$= \sum_{jk}(\langle\psi|E_j^\dagger\otimes\langle e_j|)(E_k|\phi\rangle\otimes|e_k\rangle) = \sum_{jk}(\langle\psi|E_j^\dagger E_k|\phi\rangle)\otimes\underbrace{\langle e_j|e_k\rangle}_{=\delta_{jk}} = \sum_k \langle\psi|E_k^\dagger E_k|\phi\rangle = \langle\psi|(\underbrace{\sum_k E_k^\dagger E_k}_{\substack{=I\\ \because\text{ Trace-}\\ \text{Preserving}}})|\phi\rangle = \langle\psi|\phi\rangle$$

Thus the operator U can be extended to a unitary operator acting on the entire state space of the joint system.

Continuing with the solution to the problem, we define the operator U as

$$U|\psi\rangle|e_0\rangle \equiv \sum_{1\le k<\infty} E_k|\psi\rangle|e_k\rangle + E_\infty|\psi\rangle|e_\infty\rangle \tag{7}$$

where E_∞ is an extra operator along with the set $\{E_k\}$ such that $\sum_k E_k^\dagger E_k + E_\infty^\dagger E_\infty = I$. Then for arbitrary states $|\psi\rangle$ and $|\phi\rangle$ in the state space of the principal systems we have

$$\langle\psi|\langle e_0|U\dagger U|\phi\rangle|e_0\rangle = \sum_{jk}\langle\psi|E_j^\dagger\langle e_j|E_k|\psi\rangle|e_k\rangle + (\sum_k\langle\psi|E_k^\dagger\langle e_k|)E_\infty|\psi\rangle|e_\infty\rangle + \langle\psi|E_\infty^\dagger\langle e_\infty|(\sum_k E_k|\psi\rangle|e_k\rangle)+$$
$$\langle\psi|E_\infty^\dagger\langle e_\infty|E_\infty|\psi\rangle|e_\infty\rangle$$
$$= \sum_k\langle\psi|E_k^\dagger E_k|\phi\rangle + \langle\psi|E_\infty^\dagger\langle e_\infty|E_\infty|\psi\rangle|e_\infty\rangle = \langle\psi|(\sum_k E_k^\dagger E_k + E_\infty^\dagger E_\infty)|\phi\rangle = \langle\psi|I|\phi\rangle = \langle\psi|\phi\rangle$$

Hence, U as defined in (7) can be extended to a unitary operator in the entire state space of the joint system.

> **8.9: (Measurement Model)** If we are given a set of quantum operations $\{\mathcal{E}_m\}$ such that $\sum_m \mathcal{E}_m$ is trace-preserving, then it is possible to construct a *measurement model* giving rise to this set of quantum operations. For each m, let E_{mk} be a set of operations for $\mathcal{E}_m$. Introduce an environmental system, E, with an orthonormal basis $|m,k\rangle$ in one-to -one correspondence with the set of indices for the operation elements. Analogously to the earlier construction, define an operator U such that $U|\psi\rangle|e_0\rangle = \sum_{mk} E_{mk}|\psi\rangle|m,k\rangle$. Next define projectors $P_m \equiv \sum_m |m,k\rangle\langle m,k|$ on the environmental system, E. Show that performing U on $\rho\otimes|e_0\rangle\langle e_0|$, then measuring P_m gives m with probability $\mathrm{tr}(\mathcal{E}_m(\rho))$, and the corresponding post-measurement state of the principal system is $\mathcal{E}_m(\rho)/\mathrm{tr}(\mathcal{E}_m(\rho))$.

The set $\{E_{mk}\}$ is the set of operators for $\mathcal{E}_m$. $|m,k\rangle$ is an orthonormal basis for the environmental system E in one-to-one correspondence with E_{mk}. We note that E_{mk} acts on state $|\psi\rangle$. Hence, $E_{mk}|\psi\rangle|m,k\rangle \equiv E_{mk}|\psi\rangle\otimes|m,k\rangle$ (as shown in the note included in the solution to the previous problem). Now, we show that the operator U acting on states of the form $|\psi\rangle|e_0\rangle$ can be extended to a unitary operator acting on the entire state space of the joint system. We have $U|\psi\rangle|e_0\rangle \equiv \sum_{mk} E_{mk}|\psi\rangle|m,k\rangle$. For arbitrary states $|\psi\rangle$ and $|\phi\rangle$ we have

$$\langle\psi|\langle e_0|U^\dagger U|\phi\rangle|e_0\rangle = \sum_{mk}\langle\psi|E^\dagger_{mk}\langle m,k|\sum_{mk}E_{mk}|\phi\rangle|m,k\rangle = \sum_{mjk}\langle\psi|E^\dagger_{mj}\langle m,j|E_{mk}|\phi\rangle|m,k\rangle$$
$$= \sum_{mjk}\langle\psi|E^\dagger_{mj}E_{mk}|\phi\rangle\otimes\underbrace{\langle m,j|m,k\rangle}_{=\delta_{jk}} = \sum_{mk}\langle\psi|E^\dagger_{mk}E_{mk}|\phi\rangle = \langle\psi|\sum_{mk}E^\dagger_{mk}E_{mk}|\phi\rangle \quad (\circledast)$$

Next, we see that in $(\circledast)$ we can have $\sum_{mk}E^\dagger_{mk}E_{mk} \le I$ (non-trace-preserving) or $\sum_{mk}E^\dagger_{mk}E_{mk} = I$ (trace-preserving). If the latter holds then $\langle\psi|\sum_{mk}E^\dagger_{mk}E_{mk}|\phi\rangle = \langle\psi|\phi\rangle$. However, if the former holds then as shown in the previous problem we can introduce an extra operator E_∞ in the definition of U, chosen such that we have $\sum_{mk}E^\dagger_{mk}E_{mk} = I$ where the sum runs through different k including $k=\infty$.
Hence, we have shown that $\langle\psi|\langle e_0|U^\dagger U|\phi\rangle|e_0\rangle = \langle\psi|\phi\rangle$. Thus, U can be extended to a unitary operator acting on the entire state space of the joint principal-environment system.

Now the probability of outcome m is

$$p(m) = \mathrm{tr}\Big(\mathrm{tr}_E\Big(P_m U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger P_m\Big)\Big) \tag{8}$$

Suppose the unknown state $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$. Then

$$\rho\otimes|e_0\rangle\langle e_0| = \sum_i p_i|\psi_i\rangle\langle\psi_i|\otimes|e_0\rangle\langle e_0| = \sum_i p_i|\psi_i e_0\rangle\langle\psi_i e_0|$$
$$\Rightarrow U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger = U\Big(\sum_i p_i|\psi_i e_0\rangle\langle\psi_i e_0|\Big)U^\dagger = \sum_i p_i U|\psi_i\rangle|e_0\rangle\langle\psi_i|\langle e_0|U^\dagger$$
$$\overset{\text{def of U}}{=}\sum_i p_i\sum_{mk}E_{mk}|\psi_i\rangle|m,k\rangle\sum_{mk}\langle\psi_i|E^\dagger_{mk}\langle m,k| = \sum_i p_i\sum_{mjk}E_{mj}|\psi_i\rangle|m,j\rangle\langle\psi_i|E^\dagger_{mk}\langle m,k|$$
$$\Rightarrow P_m U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger P_m = \sum_i p_i P_m\Big(\sum_{mjk}E_{mj}|\psi_i\rangle|m,j\rangle\langle\psi_i|E^\dagger_{mk}\langle m,k|\Big)P_m$$
$$= P_m\Big(\sum_{mjk}\sum_i p_i E_{mj}|\psi_i\rangle|m,j\rangle\langle\psi_i|E^\dagger_{mk}\langle m,k|\Big)P_m = P_m\Big(\sum_{mjk}\sum_i p_i E_{mj}|\psi_i\rangle\langle\psi_i|E^\dagger_{mk}\otimes|m,j\rangle\langle m,k|\Big)P_m$$
$$= P_m\Big(\sum_{mjk}E_{mj}\Big(\sum_i p_i|\psi_i\rangle\langle\psi_i|\Big)E^\dagger_{mk}\otimes|m,j\rangle\langle m,k|\Big)P_m = P_m\Big(\sum_{mjk}E_{mj}\rho E^\dagger_{mk}\otimes|m,j\rangle\langle m,k|\Big)P_m$$
$$= \sum_k|m,k\rangle\langle m,k|\Big(\sum_{mjk}E_{mj}\rho E^\dagger_{mk}\otimes|m,j\rangle\langle m,k|\Big)\sum_k|m,k\rangle\langle m,k|$$
$$= \sum_{mjkln}E_{mj}\rho E^\dagger_{mk}\otimes|m,l\rangle\underbrace{\langle m,l|m,j\rangle}_{=\delta_{lj}}\underbrace{\langle m,k|m,n\rangle}_{=\delta_{kn}}\langle m,n| = \sum_{mlk}E_{ml}\rho E^\dagger_{mk}\otimes|m,l\rangle\langle m,k|$$
$$\Rightarrow \mathrm{tr}_E\Big(P_m U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger P_m\Big) = \sum_k\langle m,k|\Big(\sum_{mlk}E_{ml}\rho E^\dagger_{mk}\otimes|m,l\rangle\langle m,k|\Big)|m,k\rangle$$
$$= \sum_{mlkk'}E_{ml}\rho E^\dagger_{mk}\otimes\underbrace{\langle m,k'|m,l\rangle}_{=\delta_{k'l}}\underbrace{\langle m,k|m,k'\rangle}_{=\delta_{kk'}} = \sum_{mk}E_{mk}\rho E^\dagger_{mk}$$

Hence, we have obtained $\mathrm{tr}_E\Big(P_m U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger P_m\Big) = \sum_{mk}E_{mk}\rho E^\dagger_{mk}$. This is the operator sum representation for the quantum operation $\mathcal{E}_m(\rho)$ corresponding to the outcome m. Hence, we can substitute this expression for $\mathrm{tr}_E(\cdots)$ in (8) and we obtain $p(m) = \mathrm{tr}\Big(\sum_{mk}E_{mk}\rho E^\dagger_{mk}\Big) = \mathrm{tr}\Big(\mathcal{E}_m(\rho)\Big)$.
Note: In section 8.2.4 (Axiomatic approach to quantum operations) we have the first axiomatic property of a quantum operation: $\mathrm{tr}(\mathcal{E}_m(\rho))$ is the probability of the measurement outcome described by $\mathcal{E}_m$ occurring.
We have shown the following two results.
(1) $\mathrm{tr}_E\Big(P_m U(\rho\otimes|e_0\rangle\langle e_0|)U^\dagger P_m\Big) = \sum_{mk}E_{mk}\rho E^\dagger_{mk} = \mathcal{E}_m(\rho)$.
(2) $p(m) = \mathrm{tr}\Big(\sum_{mk}E_{mk}\rho E^\dagger_{mk}\Big) = \mathrm{tr}\Big(\mathcal{E}_m(\rho)\Big)$.
Hence, the corresponding post-measurement state of the principal system is $\rho' = \frac{\mathcal{E}_m(\rho)}{\mathrm{tr}\big(\mathcal{E}_m(\rho)\big)}$.

8.10: Give a proof of Theorem 8.3 based on the freedom in the operator-sum representation, as follows. Let $\{E_j\}$ be a set of operation elements for $\mathcal{E}$. Define a matrix $W_{jk} \equiv \mathrm{tr}\big(E_j^\dagger E_k\big)$. Show that the matrix W is Hermitian and of rank at most d^2, and thus there is unitary matrix u such that $uWu^\dagger$ is diagonal with at most d^2 non-zero entries. Use u to define a new set of at most d^2 non-zero operation elements $\{F_j\}$ for $\mathcal{E}$.

Theorem 8.3 states: All quantum operations $\mathcal{E}$ on a system of Hilbert space dimension d can be generated by an operator-sum representation containing at most d^2 elements,

$$\mathcal{E}(\rho) = \sum_{k=1}^{M} E_k \rho E_k^\dagger \tag{9}$$

where $1 \le M \le d^2$. The proof of the theorem is as shown below.

We consider the set $\big\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\big\}$ as an orthonormal basis for the system Q of Hilbert space dimension d. The set L_Q of linear operators on the Hilbert space Q of dimension d is a Hilbert space (Exercise 2.39). Since Q has dimension d, L_Q has dimension d^2 (Exercise 2.39 (2)). Suppose $\{E_j\}_{j=1}^{M}$ is a set of operation elements for $\mathcal{E}$. The operation elements $\{E_j\}$ belong to the set L_Q. Since $\dim(L_Q) = d^2$, there can be at most d^2 mutually independent E_j's. Next, we define a matrix $W_{jk} = \mathrm{tr}\big(E_j^\dagger E_k\big)$, where $1 \le j,k \le M$. Note that W is an $M \times M$ matrix. We can show that the matrix W is Hermitian by showing $W_{jk} = W_{kj}^*$.

$$\begin{aligned}
W_{jk} &= \mathrm{tr}\big(E_j^\dagger E_k\big) = \sum_{n=0}^{d-1} \langle n| E_j^\dagger E_k |n\rangle \\
\Rightarrow W_{kj} &= \mathrm{tr}\big(E_k^\dagger E_j\big) = \sum_{n=0}^{d-1} \langle n| E_k^\dagger E_j |n\rangle \\
\Rightarrow W_{kj}^* &= \sum_{n=0}^{d-1} \Big(\langle n| E_k^\dagger E_j |n\rangle \Big)^\dagger = \sum_{n=0}^{d-1} \langle n| E_j^\dagger E_k |n\rangle = W_{jk}
\end{aligned}$$

Hence, W is Hermitian. Next, we show that $\mathrm{rank}(W) \le d^2$.
Since there is at most d^2 mutually independent E_j's we can write

$$E_j = \sum_{i=1}^{d^2} a_{ji} E_i \quad , \quad \text{for } j \ge d^2+1 \quad (\star\star)$$

Therefore, using $(\star\star)$ for $j \ge d^2+1$ and $\forall k$ we have

$$W_{jk} = \mathrm{tr}\big(E_j^\dagger E_k\big) = \sum_{n=0}^{d-1} \langle n| E_j^\dagger E_k |n\rangle = \sum_{n=0}^{d-1} \langle n| \sum_{i=1}^{d^2} a_{ji}^* E_i^\dagger E_k |n\rangle = \sum_{i=1}^{d^2} a_{ji}^* \underbrace{\sum_{n=0}^{d-1} \langle n| E_i^\dagger E_k |n\rangle}_{=\mathrm{tr}\left(E_i^\dagger E_k\right) = W_{ik}} = \sum_{i=1}^{d^2} a_{ji}^* W_{ik} \tag{10}$$

Note that (10) corresponds to expressing some row in the matrix W in terms of at most d^2 rows. Hence, we deduce that $\mathrm{rank}(W) \le d^2$.
Next, the matrix W has a singular value decomposition. Let u be a unitary matrix. Then $u^\dagger u = uu^\dagger = I$ and hence $u^\dagger$ is also unitary. There exists a diagonal matrix D containing the singular values of W such that $W = u^\dagger D u$. Then $uWu^\dagger = uu^\dagger D uu^\dagger = IDI = D$. Hence, $uWu^\dagger$ is diagonal and the diagonal elements are the singular values of the matrix W. We recall the fact that the number of non-zero singular values of a matrix equals the rank of the matrix. Hence, the diagonal matrix $uWu^\dagger$ has at most d^2 non-zero entries since $\mathrm{rank}(W) \le d^2$.
Now, each ilth entry of the matrix $uWu^\dagger$ can be represented as $\sum_{jk} u_{ij} W_{jk} u_{lk}^*$.

Since $uWu^\dagger$ is diagonal with at most d^2 non-zero diagonal elements, we must have

$$\sum_{jk} u_{ij} W_{jk} u^*_{lk} = \delta_{il}\lambda_i \quad , \quad 1 \le i \le d^2 \tag{11}$$

Also, $W_{jk} = \mathrm{tr}\big(E^\dagger_j E_k\big) = \sum_{n=0}^{d-1} \langle n| E^\dagger_j E_k |n\rangle$. Substituting this in (11) we have

$$\sum_{jk} u_{ij} W_{jk} u^*_{lk} = \sum_{n=0}^{d-1} \langle n| \Big(\sum_{jk} u_{ij} E^\dagger_j E_k u^*_{lk} \Big) |n\rangle = \delta_{il}\lambda_i$$

Next, define $F_l = \sum_k u^*_{lk} E_k$. $F'_l s$ are another set operation elements for the operation $\mathcal{E}$. We have

$$\sum_{n=0}^{d-1} \langle n| \Big(\underbrace{\sum_j u_{ij} E^\dagger_j}_{=F^\dagger_i} \underbrace{\sum_k u^*_{lk} E_k}_{=F_l} \Big) |n\rangle = \delta_{il}\lambda_i \Rightarrow \sum_{n=0}^{d-1} \langle n| F^\dagger_i F_l |n\rangle = \delta_{il}\lambda_i \quad \text{i.e.} \quad \sum_{n=0}^{d-1} \langle n| F^\dagger_i F_i |n\rangle = \lambda_i$$

Next, we show that there are at most d^2 non-zero F_l's (rather F_i's, please note the change in index below).

$$\lambda_i = \sum_{n=0}^{d-1} \langle n| F^\dagger_i F_i |n\rangle = \sum_{n=0}^{d-1} \langle n| F^\dagger_i I F_i |n\rangle = \sum_{n=0}^{d-1} \langle n| F^\dagger_i \sum_{n=0}^{d-1} |n\rangle \langle n| F_i |n\rangle = \sum_{n,m} \langle n| F^\dagger_i |m\rangle \langle m| F_i |n\rangle$$

We know there at most d^2 non-zero λ_i's. Hence, for $i \ge d^2 + 1$ we must have

$$0 = \sum_{n,m} \langle n| F^\dagger_i |m\rangle \langle m| F_i |n\rangle = \sum_{n,m} |\langle m| F_i |n\rangle|^2$$

Hence, $F_i = 0$ for $i \ge d^2 + 1$. Thus using the unitary u we obtained another set of (at most d^2 non-zero) operation elements $\{F_i\}$ for the same operation $\mathcal{E}$. So, we have shown that any operator-sum representation $\sum_k E_k \rho E^\dagger_k$ for the operation $\mathcal{E}$ has at most d^2 operation elements E_k.