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 $p(m) = \text{tr}(\mathcal{E}_m(\rho))$.

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

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

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,

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

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

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

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 $\text{tr}_{AD}\left(U(\rho_{AB} \otimes |00\rangle\langle 00|_{CD})U^\dagger\right)$. 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).

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

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

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

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 $\sum_k E_k^\dagger E_k = I$.

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

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

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

Rewriting (5) we have

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

Hence, we have shown that $\sum_k E_k^\dagger E_k \equiv \sum_{ad} E^\dagger_{ad} E_{ad} = I_{AB}$ where $E_{ad} = \big(\langle a| \otimes I_{BC} \otimes \langle d|\big)U\big(I_{AB} \otimes |0\rangle_C \otimes |0\rangle_D\big)$. 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. $U^\dagger U = I$.

$$U^\dagger U = \big(P_0\otimes I + P_1\otimes X\big)^\dagger\big(P_0\otimes I + P_1\otimes X\big) = \big(P_0\otimes I + P_1\otimes X^\dagger\big)\big(P_0\otimes I + P_1\otimes X\big) = \big(P_0\otimes I + P_1\otimes X\big)\big(P_0\otimes I + P_1\otimes X\big)$$
$$= \big(P_0\otimes I\big)\big(P_0\otimes I\big) + \big(P_0\otimes I\big)\big(P_1\otimes X\big) + \big(P_1\otimes X\big)\big(P_0\otimes I\big) + \big(P_1\otimes X\big)\big(P_1\otimes X\big)$$
$$\Rightarrow U^\dagger U = \big(P_0^2\otimes I^2\big) + P_0P_1\otimes IX + P_1P_0\otimes XI + P_1^2\otimes X^2 = P_0\otimes I + P_1\otimes I = \underbrace{\big(P_0 + P_1\big)}_{=I}\otimes I = I\otimes I = I$$

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

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

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

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

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.

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

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

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

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

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

$$\mathcal{E}_m(\rho) = \sum_k \langle e_k| \Big(M_m U\big(\rho \otimes \sum_j q_j |j\rangle\langle j|\big)U^\dagger M_m^\dagger\Big) |e_k\rangle = \sum_{kj} q_j \langle e_k| \Big(M_m U\big(\rho \otimes |j\rangle\langle j|\big)U^\dagger M_m^\dagger\Big) |e_k\rangle$$

$$\Rightarrow \mathcal{E}_m(\rho) \underbrace{=}_{\substack{\text{Using}\\ \text{(8.9) and (8.10)}\\ \text{in NC}}} \sum_{kj} \underbrace{\sqrt{q_j}\langle e_k|M_m U|j\rangle}_{=E_{kj}} \rho \underbrace{\sqrt{q_j}\langle j|U^\dagger M_m^\dagger|e_k\rangle}_{=E_{kj}^\dagger}$$

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.

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

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

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

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

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

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

$$\rho\otimes|e_0\rangle\langle e_0| = \sum_i p_i|\psi_i\rangle\langle\psi_i|\otimes|e_0\rangle\langle e_0| = \sum_i p_i|\psi_i e_0\rangle\langle\psi_i e_0|$$

$$\Rightarrow U\big(\rho\otimes|e_0\rangle\langle e_0|\big)U^\dagger = U\Big(\sum_i p_i|\psi_i e_0\rangle\langle\psi_i e_0|\Big)U^\dagger = \sum_i p_i U|\psi_i\rangle|e_0\rangle\langle\psi_i|\langle e_0|U^\dagger$$

$$\stackrel{\text{def of U}}{=} \sum_i p_i\sum_{mk}E_{mk}|\psi_i\rangle|m,k\rangle\sum_{mk}\langle\psi_i|E^\dagger_{mk}\langle m,k| = \sum_i p_i\sum_{mjk}E_{mj}|\psi_i\rangle|m,j\rangle\langle\psi_i|E^\dagger_{mk}\langle m,k|$$

$$\Rightarrow P_m U\big(\rho\otimes|e_0\rangle\langle e_0|\big)U^\dagger P_m = \sum_i p_i P_m\Big(\sum_{mjk}E_{mj}|\psi_i\rangle|m,j\rangle\langle\psi_i|E^\dagger_{mk}\langle m,k|\Big)P_m$$

$$= P_m\Big(\sum_{mjk}\sum_i p_i E_{mj}|\psi_i\rangle|m,j\rangle\langle\psi_i|E^\dagger_{mk}\langle m,k|\Big)P_m = P_m\Big(\sum_{mjk}\sum_i p_i E_{mj}|\psi_i\rangle\langle\psi_i|E^\dagger_{mk}\otimes|m,j\rangle\langle m,k|\Big)P_m$$

$$= P_m\Big(\sum_{mjk}E_{mj}\Big(\sum_i p_i|\psi_i\rangle\langle\psi_i|\Big)E^\dagger_{mk}\otimes|m,j\rangle\langle m,k|\Big)P_m = P_m\Big(\sum_{mjk}E_{mj}\rho E^\dagger_{mk}\otimes|m,j\rangle\langle m,k|\Big)P_m$$

$$= \sum_k|m,k\rangle\langle m,k|\Big(\sum_{mjk}E_{mj}\rho E^\dagger_{mk}\otimes|m,j\rangle\langle m,k|\Big)\sum_k|m,k\rangle\langle m,k|$$

$$= \sum_{mjkln}E_{mj}\rho E^\dagger_{mk}\otimes|m,l\rangle\underbrace{\langle m,l|m,j\rangle}_{=\delta_{lj}}\underbrace{\langle m,k|m,n\rangle}_{=\delta_{kn}}\langle m,n| = \sum_{mlk}E_{ml}\rho E^\dagger_{mk}\otimes|m,l\rangle\langle m,k|$$

$$\Rightarrow \mathrm{tr}_E\Big(P_m U\big(\rho\otimes|e_0\rangle\langle e_0|\big)U^\dagger P_m\Big) = \sum_k\langle m,k|\Big(\sum_{mlk}E_{ml}\rho E^\dagger_{mk}\otimes|m,l\rangle\langle m,k|\Big)|m,k\rangle$$

$$= \sum_{mlkk'}E_{ml}\rho E^\dagger_{mk}\otimes\underbrace{\langle m,k'|m,l\rangle}_{=\delta_{k'l}}\underbrace{\langle m,k|m,k'\rangle}_{=\delta_{kk'}} = \sum_{mk}E_{mk}\rho E^\dagger_{mk}$$

Hence, we have obtained $\mathrm{tr}_E\Big(P_m U\big(\rho\otimes|e_0\rangle\langle e_0|\big)U^\dagger P_m\Big) = \sum_{mk}E_{mk}\rho E^\dagger_{mk}$. 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) $\mathrm{tr}_E\Big(P_m U\big(\rho\otimes|e_0\rangle\langle e_0|\big)U^\dagger P_m\Big) = \sum_{mk}E_{mk}\rho E^\dagger_{mk} = \mathcal{E}_m(\rho)$.
(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 $W_{jk} \equiv \mathrm{tr}(E_j^\dagger E_k)$. 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 $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ 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 $W_{jk} = \mathrm{tr}(E_j^\dagger E_k)$, 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 $W_{jk} = W_{kj}^*$.

$$W_{jk} = \mathrm{tr}\left(E_j^\dagger E_k\right) = \sum_{n=0}^{d-1} \langle n| E_j^\dagger E_k |n\rangle$$
$$\Rightarrow W_{kj} = \mathrm{tr}\left(E_k^\dagger E_j\right) = \sum_{n=0}^{d-1} \langle n| E_k^\dagger E_j |n\rangle$$
$$\Rightarrow W_{kj}^* = \sum_{n=0}^{d-1} \left(\langle n| E_k^\dagger E_j |n\rangle\right)^\dagger = \sum_{n=0}^{d-1} \langle n| E_j^\dagger E_k |n\rangle = W_{jk}$$

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

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

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, $W_{jk} = \mathrm{tr}\left(E_j^\dagger E_k\right) = \sum_{n=0}^{d-1} \langle n| E_j^\dagger E_k |n\rangle$. Substituting this in (11) we have

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

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

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

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).

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

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

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

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 $\sum_k E_k \rho E_k^\dagger$ for the operation $\mathcal{E}$ has at most d^2 operation elements E_k.

8.11: Suppose $\mathcal{E}$ is a quantum operation mapping a d-dimensional input space to a d'-dimensional output space. Show that $\mathcal{E}$ can be described using a set of at most dd' operation elements $\{E_k\}$.

The operation $\mathcal{E}$ maps an input space of dimension d to an output space of dimension d'. We show that the operator sum representation $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ consists of at most dd' operation elements. Let Q_i be the input space and $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ be a set of orthonormal basis for Q_i. Let Q_o be the output space and $\{|0\rangle, |1\rangle, \cdots, |d'-1\rangle\}$ be a set of orthonormal basis for Q_o. Then the set of linear operators L_E mapping the space Q_i to the space Q_o is a Hilbert space containing (operation) elements $E_k : Q_i \to Q_o$. The outer product representation of the operation element E_k is

$$E_k = \sum_{m=0}^{d'-1} \sum_{n=0}^{d-1} \langle m| E_k |n\rangle |m\rangle \langle n| \tag{12}$$

From (12) we see that there are dd' elements $|m\rangle\langle n|$ that span the space of L_E. Also, we see that $\sum_{m=0}^{d'-1} \sum_{n=0}^{d-1} \langle m| E_k |n\rangle |m\rangle \langle n| = 0$ if and only if $\langle m| E_k |n\rangle = 0$. Hence the elements $|m\rangle\langle n|$ are mutually linearly independent. Therefore, we see that space L_E of linear operators $E_k : Q_i \to Q_o$ is of dimension dd'. This implies that there are at most dd' independent E_k's.
From here we can use the same argument as in 8.10. We define the matrix $W_{jk} \equiv \mathrm{tr}\left(E_j^\dagger E_k\right)$ and we can show (using similar arguments as before) that W is Hermitian and of rank at most dd'. Thus there is a unitary matrix u such that $uWu^\dagger$ is diagonal with at most dd' non-zero diagonal elements.

And then we can use u to define a new set of at most dd' non-zero operation elements F_k for $\mathscr{E}$.

8.12: Why can we assume that O has determinant 1 in the decomposition (8.93) ?

The assumption that O has determinant 1 follows from the fact that for an orthogonal matrix $O^TO = I$ where I is the identity matrix.
Then $1 = \det(I) = \det(O^TO) = \det(O^T)\det(O) = \det(O)\det(O) = \left(\det(O)\right)^2$. This shows that $\det(O) = \pm 1$.

8.13: Show that unitary transformations correspond to rotations of the Bloch sphere.

We assume a Bloch sphere representing a single qubit. Rotations can be accomplished using the special unitary transformations in 2-dimensions, $SU(2)$. It is the group of 2×2 matrices with determinant 1. Let U be such a matrix and hence $U^\dagger U = UU^\dagger = I$ and $\det(U) = 1$. Applying U to ρ we have the evolution of the density matrix, $\rho \xrightarrow{U} U\rho U^\dagger$. The Bloch sphere representation of the density matrix is $\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma})$ where $\vec{\sigma}$ is the Pauli vector. Then the evolution of the density matrices is represented by the transformation $\frac{1}{2}(I+\vec{r}\cdot\vec{\sigma}) \xrightarrow{U} \frac{1}{2}(UIU^\dagger + U\vec{r}\cdot\vec{\sigma}U^\dagger) = \frac{1}{2}(I + U\vec{r}\cdot\vec{\sigma}U^\dagger)$. And $\vec{r'}\cdot\vec{\sigma} = U\vec{r}\cdot\vec{\sigma}U^\dagger$ is a rotation since U is unitary with determinant 1 and $\mathrm{tr}(\vec{r'}\cdot\vec{\sigma}) = \mathrm{tr}(U\vec{r}\cdot\vec{\sigma}U^\dagger) = \mathrm{tr}(\vec{r}\cdot\vec{\sigma}U^\dagger U) = \mathrm{tr}(\vec{r}\cdot\vec{\sigma}I) = \mathrm{tr}(\vec{r}\cdot\vec{\sigma}) = 0$. As an example consider the matrix $R = e^{-i\frac{\theta}{2}\sigma_3}$ where σ_3 is a Pauli matrix. Note that we can write this as $R = e^{-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}}$ where $\vec{n} \equiv (0,0,1)$ is a real unit vector and $\vec{\sigma}$ is the Pauli vector. From (2.231) we have the following relation

$$f(\alpha\vec{n}\cdot\vec{\sigma}) = \frac{f(\alpha)+f(-\alpha)}{2}I + \frac{f(\alpha)-f(-\alpha)}{2}\vec{n}\cdot\vec{\sigma}$$

Using this relation for $R = e^{-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}}$ we get

$$R = e^{-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}} = \frac{e^{i\frac{\theta}{2}}+e^{-i\frac{\theta}{2}}}{2}I + \frac{e^{-i\frac{\theta}{2}}-e^{i\frac{\theta}{2}}}{2}\vec{n}\cdot\vec{\sigma} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\vec{n}\cdot\vec{\sigma} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\sigma_3$$

We can check that R is unitary, i.e. $R^\dagger R = RR^\dagger = I$.

$$R^\dagger R = \left(\cos\left(\frac{\theta}{2}\right)I + i\sin\left(\frac{\theta}{2}\right)\sigma_3\right)\left(\cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\sigma_3\right) = \cos^2\left(\frac{\theta}{2}\right)I + \sin^2\left(\frac{\theta}{2}\right)\underbrace{\sigma_3^2}_{=I} = I$$

Similarly, we can show $RR^\dagger = I$. Next, using this transformation on ρ we have

$$R\rho R^\dagger = \frac{1}{2}R(I+\vec{r}\cdot\vec{\sigma})R^\dagger = \frac{1}{2}(I + R\vec{r}\cdot\vec{\sigma}R^\dagger) = \frac{1}{2}(I + r_1R\sigma_1R^\dagger + r_2R\sigma_2R^\dagger + r_3R\sigma_3R^\dagger)$$
$$\text{Next, } r_kR\sigma_kR^\dagger = r_k\left(\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\sigma_3\right)\sigma_k\left(\cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}\sigma_3\right) \quad \text{for } 1\le k\le 3$$
$$= r_k\left(\cos^2\frac{\theta}{2}\sigma_k + i\sin\frac{\theta}{2}\cos\frac{\theta}{2}\sigma_k\sigma_3 - i\sin\frac{\theta}{2}\cos\frac{\theta}{2}\sigma_3\sigma_k + \sin^2\frac{\theta}{2}\sigma_3\sigma_k\sigma_3\right)$$
$$\therefore,\quad r_1R\sigma_1R^\dagger = r_1(\cos\theta\sigma_1 + \sin\theta\sigma_2),\quad r_2R\sigma_2R^\dagger = r_2(\cos\theta\sigma_2 - \sin\theta\sigma_1),\quad r_3R\sigma_3R^\dagger = r_3\sigma_3$$

Using the expressions for $r_kR\sigma_kR^\dagger$ for $1\le k\le 3$ we have

$$R\rho R^\dagger = \frac{1}{2}\Big(I + r_1(\cos\theta\sigma_1 + \sin\theta\sigma_2) + r_2(\cos\theta\sigma_2 - \sin\theta\sigma_1) + r_3\sigma_3\Big) =$$
$$\Rightarrow R\rho R^\dagger = \frac{1}{2}\Big(I + (r_1\cos\theta - r_2\sin\theta)\sigma_1 + (r_1\sin\theta + r_2\cos\theta)\sigma_2 + r_3\sigma_3\Big)$$

And so

$$\rho = \frac{1}{2}(I + r_1\sigma_1 + r_2\sigma_2 + r_3\sigma_3) \xrightarrow{R} R\rho R^\dagger = \frac{1}{2}\Big(I + (r_1\cos\theta - r_2\sin\theta)\sigma_1 + (r_1\sin\theta + r_2\cos\theta)\sigma_2 + r_3\sigma_3\Big) \tag{13}$$

Therefore, from (13) we observe the following maps

$$r_1 \longrightarrow r_1 \cos\theta - r_2 \sin\theta = r'_1$$
$$r_2 \longrightarrow r_1 \sin\theta + r_2 \cos\theta = r'_2$$
$$r_3 \longrightarrow r_3 = r'_3$$

Hence, we have a rotational transformation mapping (r_1, r_2, r_3) to (r'_1, r'_2, r'_3) as shown below

$$\begin{pmatrix} r'_1 \\ r'_2 \\ r'_3 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} \Rightarrow \vec{r}' = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \vec{r}$$

Hence, we can conclude that unitary transformations correspond to rotations of the Bloch sphere.

8.14: Show that det(S) need not be positive.

From (8.93) we have $M = OS$ where M is a 3×3 real matrix, O is orthogonal and S is a symmetric matrix. Taking the determinant of M gives $\det(M) = \det(OS) = \det(O)\det(S)$. In the solution to 8.12 we showed that $\det(O) = \pm 1$. Hence, $\det(M) = \pm\det(S)$ and hence $\det(S) = \pm\det(M)$. So, $\det(S)$ need not be positive.

8.15: Suppose a projective measurement is performed on a single qubit in the basis $|+\rangle, |-\rangle$, where $|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$. In the event that we are ignorant of the result of the measurement, the density matrix evolves according to the equation

$$\rho \longrightarrow \mathcal{E}(\rho) = |+\rangle\langle +|\rho|+\rangle\langle +| + |-\rangle\langle -|\rho|-\rangle\langle -|$$

Illustrate this transformation on the Bloch sphere.

We can write the measurement operators $|\pm\rangle\langle\pm|$ in terms of the Pauli matrices.
$|+\rangle\langle +| = \frac{1}{2}(I + \sigma_1)$, $|-\rangle\langle -| = \frac{1}{2}(I - \sigma_1)$. Then $\mathcal{E}(\rho) = \frac{1}{4}(I + \sigma_1)\rho(I + \sigma_1) + \frac{1}{4}(I - \sigma_1)\rho(I - \sigma_1) = \frac{1}{4}(2\rho + 2\sigma_1\rho\sigma_1) = \frac{1}{2}(\rho + \sigma_1\rho\sigma_1)$.

$$\mathcal{E}(\rho) = \frac{1}{2}(\rho + \sigma_1\rho\sigma_1) = \frac{1}{2}\Big(\frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}) + \frac{1}{2}\sigma_1(I + \vec{r}\cdot\vec{\sigma})\sigma_1\Big) = \frac{1}{2}\Big(\frac{1}{2}I + \frac{1}{2}\sum_{i=1}^{3} r_i\sigma_i + \frac{1}{2}(I + r_1\sigma_1 + r_2\underbrace{\sigma_1\sigma_2\sigma_1}_{=-\sigma_2} + r_3\underbrace{\sigma_1\sigma_3\sigma_1}_{=-\sigma_3})\Big)$$

$$\Rightarrow \mathcal{E}(\rho) = \frac{1}{2}\Big(\frac{1}{2}I + \frac{1}{2}\sum_{i=1}^{3} r_i\sigma_i + \frac{1}{2}I + \frac{1}{2}(r_1\sigma_1 - r_2\sigma_2 - r_3\sigma_3)\Big) = \frac{1}{2}(I + r_1\sigma_1)$$

Hence we have the following transformation

$$\rho = \frac{1}{2}(I + r_1\sigma_1 + r_2\sigma_2 + r_3\sigma_3) \xrightarrow{\mathcal{E}} \rho' = \frac{1}{2}(I + r_1\sigma_1)$$

We can illustrate this transformation on the Bloch sphere as

$$(r_1, r_2, r_3) \longrightarrow (r_1, 0, 0)$$

Hence, the Bloch vector is projected along the x axis and the y and z components of the Bloch vector are lost.

8.17: Verify (8.101) as follows. Define $\mathcal{E}(A) \equiv \frac{A+XAX+YAY+ZAZ}{4}$, show that $\mathcal{E}(I) = I$, $\mathcal{E}(X) = \mathcal{E}(Y) = \mathcal{E}(Z) = 0$. Now use the Bloch sphere representation for single qubit density matrices to verify (8.101).

We use the following property of the Pauli matrices

$$XY = -YX = iZ \quad YZ = -ZY = iX \quad ZX = -XZ = iY \tag{14}$$

Using the definition given in the problem

$$\begin{aligned}
\mathcal{E}(I) &= \frac{I+XIX+YIY+ZIZ}{4} = \frac{I+X^2+Y^2+Z^2}{4} = \frac{4I}{4} = I \\
\mathcal{E}(X) &= \frac{X+XXX+YXY+ZXZ}{4} = \frac{X+X-X-X}{4} = 0 \quad \text{Using (14)} \\
\mathcal{E}(Y) &= \frac{Y+XYX+YYY+ZYZ}{4} = \frac{Y-Y+Y-Y}{4} = 0 \quad \text{Using (14)} \\
\mathcal{E}(Z) &= \frac{Z+XZX+YZY+ZZZ}{4} = \frac{Z-Z-Z+Z}{4} = 0
\end{aligned}$$

Hence, using the definition $\mathcal{E}(\rho) = \frac{\rho+X\rho X+Y\rho Y+Z\rho Z}{4}$. We know $\rho = \frac{1}{2}(I+r_1X+r_2Y+r_3Z)$. Hence, $\mathcal{E}(\rho) = \mathcal{E}\left(\frac{1}{2}(I+r_1X+r_2Y+r_3Z)\right)$. By linearity of $\mathcal{E}(\cdot)$ we have $\mathcal{E}\left(\frac{1}{2}(I+r_1X+r_2Y+r_3Z)\right) = \frac{1}{2}\mathcal{E}(I)+r_1\frac{1}{2}\mathcal{E}(X)+r_2\frac{1}{2}\mathcal{E}(Y)+r_3\frac{1}{2}\mathcal{E}(Z) = \frac{1}{2}I = \frac{\rho+X\rho X+Y\rho Y+Z\rho Z}{4}$.

8.18: For $k \geq 1$ show that $\mathrm{tr}(\rho^k)$ is never increased by the action of the depolarizing channel.

We restrict ourselves to single qubit quantum systems. First, we obtain an expression for ρ^k, $k \in \mathbb{N}$. We know that $\rho = \frac{1}{2}(I+\vec{r}\cdot\vec{\sigma})$. For integer powers of ρ we observe the following

$$\begin{aligned}
\rho^2 &= \frac{1}{4}\big((1+|\vec{r}|^2)I + 2\vec{r}\cdot\vec{\sigma}\big) \\
\rho^3 &= \frac{1}{8}\big((1+3|\vec{r}|^2)I + (3+|\vec{r}|^2)\vec{r}\cdot\vec{\sigma}\big) \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\rho^k &= \frac{1}{2^k}\Big((1+(2^{k-1}-1)|\vec{r}|^2)I + (2^{k-1}-1+|\vec{r}|^2)\vec{r}\cdot\vec{\sigma}\Big) \\
\text{Hence, } \mathrm{tr}(\rho^k) &= \frac{1}{2^{k-1}}\Big(1+(2^{k-1}-1)|\vec{r}|^2\Big) \qquad (\dagger)
\end{aligned}$$

Next, the depolarizing channel is represented by the quantum operation $\rho' = \mathcal{E}(\rho) = p\frac{I}{2} + (1-p)\rho$. Hence, $\rho' = p\frac{1}{2}I + (1-p)\frac{1}{2}(I+\vec{r}\cdot\vec{\sigma}) = \frac{1}{2}(I+(1-p)\vec{r}\cdot\vec{\sigma})$. Therefore the depolarizing channel has the following transformation on the Bloch vector $\vec{r}$

$$(r_1, r_2, r_3) \longrightarrow ((1-p)r_1, (1-p)r_2, (1-p)r_3) \quad 0 \leq p \leq 1 \qquad (*)$$

Hence, the action of the depolarizing channel ($\rho \xrightarrow{\mathcal{E}} \rho'$) has the following effect on $\mathrm{tr}(\rho^k)$

$$\begin{aligned}
\mathrm{tr}(\rho'^k) &= \frac{1}{2^{k-1}}\Big(1+(2^{k-1}-1)\left|\vec{r'}\right|^2\Big) \qquad \text{(from } \dagger\text{)} \\
\Rightarrow \mathrm{tr}(\rho'^k) &= \frac{1}{2^{k-1}}\Big(1+(2^{k-1}-1)(1-p)^2|\vec{r}|^2\Big) \qquad \text{(from } *\text{)}
\end{aligned}$$

We notice that $(1-p)^2|\vec{r}|^2 \leq |\vec{r}|^2$. Hence, $\frac{1}{2^{k-1}}\Big(1+(2^{k-1}-1)(1-p)^2|\vec{r}|^2\Big) \leq \frac{1}{2^{k-1}}\Big(1+(2^{k-1}-1)|\vec{r}|^2\Big)$ for $k \geq 1$. And so, $\mathrm{tr}(\rho'^k) \leq \mathrm{tr}(\rho^k)$. Thus, for $k \geq 1$ the action of the depolarizing channel never increases $\mathrm{tr}(\rho^k)$.

8.21: (Amplitude damping of a harmonic oscillator) Suppose that our principal system, a harmonic oscillator, interacts with an environment, modeled as another harmonic oscillator, through the Hamiltonian

$$H = \chi\left(a^\dagger b + b^\dagger a\right)$$

where a and b are annihilation operators for the respective harmonic oscillators, as defined in Section 7.3.
(1) Using $U = \exp\left(-iH\Delta t\right)$, denoting the eigenstates of $b^\dagger b$ as $|k_b\rangle$, and selecting the vacuum state $|0_b\rangle$ as the initial state of the environment, show that the operation elements $\langle k_b|U|0_b\rangle$ are found to be

$$E_k = \sum_n \sqrt{\binom{n}{k}}\sqrt{(1-\gamma)^{n-k}\gamma^k}\,|n-k\rangle\langle n|$$

where $\gamma = 1-\cos^2\left(\chi\Delta t\right)$ is the probability of loosing a single quantum of energy, and states such as $|n\rangle$ are the eigenstates of $a^\dagger a$.
(2) Show that the operation elements E_k define a trace-preserving quantum operation.

(1) Let A and B denote the principal quantum system and the environment respectively. Both are modeled as Harmonic oscillators and they interact through the Hamiltonian $H = \chi\left(a^\dagger \otimes b + b^\dagger \otimes a\right)$.
Note: The tensor product is absent in the expression of the Hamiltonian H (in the question) that represents the interaction between the system and the environment. An operator such as H in this case is defined in the combined state space of system and environment and hence must include $\otimes$ in between $a\dagger$ ($b\dagger$) and b (a). Moreover, when the system and the environment are of different dimensions and the number of columns of $a^\dagger$ is not equal to the number of rows of b then $a^\dagger b$ has no meaning.
$a^\dagger$ and $b^\dagger$ are the creation operators for the respective oscillators, and a and b are the annihilation operators. The eigenstates of the Hamiltonian of the harmonic oscillator representing the quantum system has the following properties

$$a^\dagger a\,|n\rangle = n\,|n\rangle \tag{15}$$
$$a^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{16}$$
$$a\,|n\rangle = \sqrt{n}\,|n-1\rangle \tag{17}$$

First, we show that $|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$. From (16) we see that

$$\begin{gathered}
a^\dagger|0\rangle = \sqrt{1}\,|1\rangle \\
\Rightarrow a^\dagger\left(a^\dagger|0\rangle\right) = a^\dagger\left(\sqrt{1}\,|1\rangle\right) = \sqrt{1}a^\dagger|1\rangle = \sqrt{1}\sqrt{2}\,|2\rangle \\
\Rightarrow a^\dagger\left(a^\dagger\left(a^\dagger|0\rangle\right)\right) = a^\dagger\left(\sqrt{1}\sqrt{2}\,|2\rangle\right) = \sqrt{1}\sqrt{2}\sqrt{3}\,|3\rangle \\
\Rightarrow \left(a^\dagger\right)^3|0\rangle = \sqrt{3!}\,|3\rangle \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\Rightarrow a^\dagger\left(\cdots\cdots\left(a^\dagger\right)|0\rangle\right) = \sqrt{1\cdot 2\cdot 3\cdots\cdots n}\,|n\rangle \\
\Rightarrow \left(a^\dagger\right)^n|0\rangle = \sqrt{1\cdot 2\cdot 3\cdots\cdots n}\,|n\rangle = \sqrt{n!}\,|n\rangle \Rightarrow |n\rangle = \frac{\left(a^\dagger\right)^n}{\sqrt{n!}}|0\rangle \qquad (\ddagger)
\end{gathered}$$

We have similar result for the other system, i.e., $|k\rangle = \frac{(b^\dagger)^k}{\sqrt{k!}}$. Note that we have dropped the subscript b in $|k_b\rangle$ (as given in the question). Next, we try to obtain an expression for each element of the operator E_k (on system A) with respect to its basis states, i.e. $\left(E_k\right)_{mn}$. And we know that $E_k = \sum_{mn}\left(E_k\right)_{mn}|m\rangle\langle n|$.

Then, $\left(E_k\right)_{mn} = \langle m,k|U|n,0\rangle$.

$$\langle m,k|U|n,0\rangle = \langle m,k|U\frac{\left(a^\dagger\right)^n}{\sqrt{n!}}|0,0\rangle \qquad \left(\because, |n\rangle = \frac{\left(a^\dagger\right)^n}{\sqrt{n!}}|0\rangle\right)$$
$$\Rightarrow \langle m,k|U|n,0\rangle = \langle m,k|U\frac{\left(a^\dagger\right)^n}{\sqrt{n!}}U^\dagger U|0,0\rangle \qquad \left(\because, U^\dagger U = I\right)$$
$$= \langle m,k|\frac{\left(Ua^\dagger U^\dagger\right)^n}{\sqrt{n!}}U|0,0\rangle \qquad (*)$$

We need to show a couple of results concerning $(*)$. First, we show that $U\left(a^\dagger\right)^n U^\dagger = \left(Ua^\dagger U^\dagger\right)^n$. We use induction to establish the equality. First, it is easy to see that the statement is true for $n=1$, indeed $U\left(a^\dagger\right)^1 U^\dagger = \left(Ua^\dagger U^\dagger\right)^1$. Suppose it is true for $n = k-1$, i.e. $U\left(a^\dagger\right)^{k-1}U^\dagger = \left(Ua^\dagger U^\dagger\right)^{k-1}$. Then, we see that for $n=k$, we have $\left(Ua^\dagger U^\dagger\right)^k = \left(Ua^\dagger U^\dagger\right)^{k-1}\left(Ua^\dagger U^\dagger\right) = U\left(a^\dagger\right)^{k-1}\underbrace{U^\dagger U}_{=I}\left(a^\dagger\right)U^\dagger = U\left(a^\dagger\right)^{k-1}a^\dagger U^\dagger = U\left(a^\dagger\right)^k U^\dagger$. And so, we have shown that the result holds for any $n = 0,1,2,\ldots$.
Second, we need to show that $U|0,0\rangle = |0,0\rangle$. We use the power series expression for the matrix exponential $U = \exp\left(-i\chi\Delta t\left(a^\dagger b + ab^\dagger\right)\right)$.

$$U|0,0\rangle = \exp\left(-i\chi\Delta t\left(a^\dagger b + ab^\dagger\right)\right)|0,0\rangle = \sum_{n=0}^{\infty}\frac{\left(-i\chi\Delta t\right)^n\left(a^\dagger b + ab^\dagger\right)^n}{n!}|0,0\rangle$$
$$= I|0,0\rangle + \left(-i\chi\Delta t\right)\left(a^\dagger b + ab^\dagger\right)|0,0\rangle + \frac{\left(-i\chi\Delta t\right)^2\left(a^\dagger b + ab^\dagger\right)^2}{2!}|0,0\rangle + \cdots\cdots$$
$$\Rightarrow U|0,0\rangle = |0,0\rangle$$

The above holds because $\left(a^\dagger b + ab^\dagger\right)|0,0\rangle = a^\dagger b|0,0\rangle + ab^\dagger|0,0\rangle$. And $b|0\rangle$ is undefined and likewise $a|0\rangle$, since we have $a|n\rangle = \sqrt{n}|n-1\rangle$. So, the unitary operator U does not change $|0,0\rangle$.

So far we have shown $\left(E_k\right)_{mn} = \langle m,k|\frac{\left(Ua^\dagger U^\dagger\right)^n}{\sqrt{n!}}U|0,0\rangle$ which is equal to $\langle m,k|\frac{\left(Ua^\dagger U^\dagger\right)^n}{\sqrt{n!}}|0,0\rangle$. We have the term $\left(Ua^\dagger U^\dagger\right)^n$ in the expression for $\left(E_k\right)_{mn}$. We use the Baker-Campbell-Hausdorff formula to find out the transformations effected by the unitary matrix U upon $a^\dagger$. The Baker-Campbell-Hausdorff formula reads

$$e^{\lambda G}Ae^{-\lambda G} = \sum_{n=0}^{\infty}\frac{\lambda^n}{n!}C_n$$

where $C_0 = A$, $\quad C_1 = [G,C_0] = [G,A]$, $\quad C_2 = [G,C_1] = [G,[G,C_0]] = [G,[G,A]], \cdots\cdots$, $\quad C_n = [G,C_{n-1}]$.
We know $U = \exp\left(-i\chi\Delta t\left(a^\dagger b + ab^\dagger\right)\right)$. Let $\theta = \left(-i\chi\Delta t\right)$ and $G = a^\dagger b + ab^\dagger$. Then $U = e^{\theta G}$ and $U^\dagger = e^{-\theta G}$. And so we have (using the Baker-Campbell-Hausdorff formula)

$$Ua^\dagger U^\dagger = e^{\theta G}a^\dagger e^{-\theta G} = \sum_{n=0}^{\infty}\frac{\theta^n}{n!}C_n \tag{18}$$

Now we need to find the operators C_n. $C_0 = a^\dagger$. $C_1 = [G,a^\dagger] = \left(a^\dagger b + ab^\dagger\right)a^\dagger - a^\dagger\left(a^\dagger b + ab^\dagger\right) = b^\dagger$.
$C_2 = [G,C_1] = [G,b^\dagger] = \left(a^\dagger b + ab^\dagger\right)b^\dagger - b^\dagger\left(a^\dagger b + ab^\dagger\right) = a^\dagger$. In fact, we see that

$$C_{n\text{ even}} = a^\dagger, \quad C_{n\text{ odd}} = b^\dagger$$

Using these in (18) we get

$$Ua^\dagger U^\dagger = e^{\theta G}a^\dagger e^{-\theta G} = \sum_{n\text{ even}}\frac{\left(-i\chi\Delta t\right)^n}{n!}a^\dagger + \sum_{n\text{ odd}}\frac{\left(-i\chi\Delta t\right)^n}{n!}b^\dagger = \cos\left(\chi\Delta t\right)a^\dagger - i\sin\left(\chi\Delta t\right)b^\dagger \tag{19}$$

Hence, $\left(Ua^\dagger U^\dagger\right)^n = \left(\cos\left(\chi\Delta t\right)a^\dagger - i\sin\left(\chi\Delta t\right)b^\dagger\right)^n$. Notice that the operators $\cos\left(\chi\Delta t\right)a^\dagger$ and $-i\sin\left(\chi\Delta t\right)b^\dagger$ commute. Hence, we can use the formula for binomial expansion (involving numbers) for operators

and write $\left(Ua^{\dagger}U^{\dagger}\right)^n = \sum_{r=0}^{n}\binom{n}{r}\left(\cos\left(\chi\Delta t\right)a^{\dagger}\right)^{n-r}\left(-i\sin\left(\chi\Delta t\right)b^{\dagger}\right)^r = \sum_{r=0}^{n}\binom{n}{r}\cos^{n-r}\left(\chi\Delta t\right)\left(a^{\dagger}\right)^{n-r}\left(-i\right)^r\sin^r\left(\chi\Delta t\right)\left(b^{\dagger}\right)^r$.
Continuing with (∗) we have

$$\left(E_k\right)_{mn} = \langle m,k|U|n,0\rangle = \langle m,k|\frac{\left(Ua^{\dagger}U^{\dagger}\right)^n}{\sqrt{n!}}U|0,0\rangle = \langle m,k|\frac{1}{\sqrt{n!}}\sum_{r=0}^{n}\binom{n}{r}\cos^{n-r}\left(\chi\Delta t\right)\left(a^{\dagger}\right)^{n-r}\left(-i\right)^r\sin^r\left(\chi\Delta t\right)\left(b^{\dagger}\right)^r|0,0\rangle$$

With the substitution $\gamma = 1-\cos^2\left(\chi\Delta t\right)$ (the probability pf loosing a single quantum of energy) we get

$$\langle m,k|U|n,0\rangle = \langle m,k|\frac{1}{\sqrt{n!}}\sum_{r=0}^{n}\binom{n}{r}\sqrt{(1-\gamma)^{n-r}\gamma^r}\left(-i\right)^r\left(a^{\dagger}\right)^{n-r}\left(b^{\dagger}\right)^r|0,0\rangle$$

We know $E_k = \sum_{mn}(E_k)_{mn}|m\rangle\langle n|$. So, $E_k = \sum_{mn}\langle m,k|U|n,0\rangle|m\rangle\langle n|$.

$$E_k = \sum_{mn}\langle m,k|\frac{1}{\sqrt{n!}}\sum_{r=0}^{n}\binom{n}{r}\sqrt{(1-\gamma)^{n-r}\gamma^r}\left(-i\right)^r\left(a^{\dagger}\right)^{n-r}\left(b^{\dagger}\right)^r|0,0\rangle|m\rangle\langle n|$$

We have $\left(a^{\dagger}\right)^{n-r}\left(b^{\dagger}\right)^r|0,0\rangle$ in the above expression. Note that $\left(a^{\dagger}\right)^{n-r}$ and $\left(b^{\dagger}\right)^r$ operate on the first and second qubit respectively in $|0,0\rangle$ and using (‡) we get $\left(a^{\dagger}\right)^{n-r}\left(b^{\dagger}\right)^r|0,0\rangle = \sqrt{(n-r)!}\sqrt{r!}|n-r,r\rangle$. Using this result in the above expression for E_k results in the following

$$\begin{aligned}
E_k &= \sum_{mn}\langle m,k|\frac{1}{\sqrt{n!}}\sum_{r=0}^{n}\frac{n!}{(n-r)!r!}\sqrt{(1-\gamma)^{n-r}\gamma^r}\left(-i\right)^r\sqrt{(n-r)!}\sqrt{r!}|n-r,r\rangle|m\rangle\langle n| \\
&= \sum_{mn}\langle m,k|\frac{1}{\sqrt{n!}}\sum_{r=0}^{n}\frac{n!}{\sqrt{(n-r)!r!}}\sqrt{(1-\gamma)^{n-r}\gamma^r}\left(-i\right)^r|n-r,r\rangle|m\rangle\langle n| \\
&= \sum_{mn}\sum_{r=0}^{n}\sqrt{\frac{n!}{(n-r)!r!}}\sqrt{(1-\gamma)^{n-r}\gamma^r}\left(-i\right)^r\langle m,k|n-r,r\rangle|m\rangle\langle n|
\end{aligned}$$

Now we have $\langle m,k|n-r,r\rangle$ which is equal to $\delta_{m(n-r)}\delta_{kr}$, i.e. the expression is equal to 1 when $m = n-r$ and $k = r$, i.e. $m = n-k$. It is 0 otherwise. And hence, the expression for E_k becomes

$$E_k = \sum_{n=k}^{\infty}\sqrt{\frac{n!}{(n-k)!k!}}\sqrt{\left(1-\gamma\right)^{n-k}\gamma^k}|n-k\rangle\langle n| = \sum_{n=k}^{\infty}\sqrt{\binom{n}{k}}\sqrt{\left(1-\gamma\right)^{n-k}\gamma^k}|n-k\rangle\langle n| \tag{20}$$

So, we have obtained the required expression for E_k in (20). Next, if the principal system is a one-qubit system then we have the operation elements E_0 and E_1. We can plug in $k = 0,1$ in (20) to obtain the expressions

$$E_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|, \quad E_1 = \sqrt{\gamma}|0\rangle\langle 1| \tag{21}$$

In matrix notation they are

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

which are the expressions for operation elements for amplitude damping.

(2) We want to show that the operation elements $E_k = \sum_n\sqrt{\binom{n}{k}}\sqrt{\left(1-\gamma\right)^{n-k}\gamma^k}|n-k\rangle\langle n|$ define a trace preserving operation, i.e., $\sum_k E_k^{\dagger}E_k = I$.

$$\sum_k E_k^{\dagger}E_k = \sum_k\sum_n\sqrt{\binom{n}{k}}\sqrt{\left(1-\gamma\right)^{n-k}\gamma^k}|n\rangle\langle n-k|\sum_n\sqrt{\binom{n}{k}}\sqrt{\left(1-\gamma\right)^{n-k}\gamma^k}|n-k\rangle\langle n|$$

$$= \sum_k\sum_{nm}\sqrt{\binom{n}{k}\binom{m}{k}}\sqrt{\left(1-\gamma\right)^{n+m-2k}\gamma^{2k}}|n\rangle\underbrace{\langle n-k|m-k\rangle}_{=\delta_{nm}}\langle m| = \sum_k\sum_n\binom{n}{k}\left(1-\gamma\right)^{n-k}\gamma^k|n\rangle\langle n|$$

$$\Rightarrow \sum_k E_k^\dagger E_k = \sum_n \left(\sum_k \binom{n}{k} (1-\gamma)^{n-k} \gamma^k \right) |n\rangle\langle n| = \sum_n (1-\gamma+\gamma)^n |n\rangle\langle n| = \sum_n |n\rangle\langle n| = I$$

8.22: (Amplitude damping of single qubit density matrix) For the general single qubit state

$$\rho = \begin{pmatrix} a & b \\ b^* & c \end{pmatrix}$$

Show that amplitude damping leads to

$$\mathcal{E}_{AD}(\rho) = \begin{pmatrix} 1-(1-\gamma)(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{pmatrix}$$

The density matrix can be written as $\rho = a|0\rangle\langle 0| + b|0\rangle\langle 1| + b^*|1\rangle\langle 0| + c|1\rangle\langle 1|$. Then the amplitude damping using the operation elements $E_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|$ and $E_1 = \sqrt{\gamma}|0\rangle\langle 1|$ is represented as the quantum operation

$$\begin{aligned}
\mathcal{E}_{AD}(\rho) &= E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger \\
&= \left(|0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|\right)\left(a|0\rangle\langle 0| + b|0\rangle\langle 1| + b^*|1\rangle\langle 0| + c|1\rangle\langle 1|\right)\left(|0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|\right) \\
&\quad + \sqrt{\gamma}|0\rangle\langle 1|\left(a|0\rangle\langle 0| + b|0\rangle\langle 1| + b^*|1\rangle\langle 0| + c|1\rangle\langle 1|\right)\sqrt{\gamma}|0\rangle\langle 1| \\
&= \left(a + c\gamma\right)|0\rangle\langle 0| + b\sqrt{1-\gamma}|0\rangle\langle 1| + b^*\sqrt{1-\gamma}|1\rangle\langle 0| + c(1-\gamma)|1\rangle\langle 1|
\end{aligned}$$

Now, ρ being a density matrix satisfies $\mathrm{tr}(\rho) = a + c = 1$, i.e., $c = 1 - a$. So, the coefficient of $|0\rangle\langle 0|$ in the expression for $\mathcal{E}_{AD}(\rho)$ obtained above is $a + c\gamma = a + (1-a)\gamma = 1 - (1-\gamma)(1-a)$. Hence, we have

$$\mathcal{E}_{AD}(\rho) = \left(1-(1-\gamma)(1-a)\right)|0\rangle\langle 0| + b\sqrt{1-\gamma}|0\rangle\langle 1| + b^*\sqrt{1-\gamma}|1\rangle\langle 0| + c(1-\gamma)|1\rangle\langle 1|$$

And in matrix notation we obtain

$$\mathcal{E}_{AD}(\rho) = \begin{pmatrix} 1-(1-\gamma)(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{pmatrix}$$

8.23: (Amplitude damping of dual-rail qubits) Suppose that a single qubit is represented by using two qubits, as

$$|\psi\rangle = a|01\rangle + b|10\rangle$$

Show that $\mathcal{E}_{AD} \otimes \mathcal{E}_{AD}$ applied to this state gives a process which can be described by the operation elements

$$E_0^{\mathrm{dr}} = \sqrt{1-\gamma} I, \quad E_1^{\mathrm{dr}} = \sqrt{\gamma}\left(|00\rangle\langle 01| + |00\rangle\langle 10|\right)$$

that is, either nothing (E_0^{dr}) happens to the qubit, or the qubit is transformed (E_1^{dr}) into the state $|00\rangle$, which is orthogonal to $|\psi\rangle$. This is a simple error-detection code, and is also the basis of robustness of the 'dual-rail' qubit discussed in Section 7.4.

The third axiomatic property of the quantum operation $\mathcal{E}$ states that it is a completely positive map, which means $\mathcal{E}(\rho)$ is positive for some density operator ρ in the input system Q, also $\mathcal{E}(\hat{\rho})$ is positive for some density operator $\hat{\rho}$ in the state space of the combined system QR where R is introduced as an extra system.
We note that $\left(\mathcal{E}_{AD} \otimes \mathcal{E}_{AD}\right) = \left(\mathcal{E}_{AD} \otimes I\right)\left(I \otimes \mathcal{E}_{AD}\right)$. Next, $\mathcal{E}_{AD}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger$ where $E_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|$ and $E_1 = \sqrt{\gamma}|0\rangle\langle 1|$.

$$\mathscr{E}_{AD}(\rho) = \big(|0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|\big)\rho\big(|0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|\big) + \sqrt{\gamma}|0\rangle\langle 1|\rho\sqrt{\gamma}|1\rangle\langle 0|$$
$$\mathscr{E}_{AD}(|0\rangle\langle 0|) = |0\rangle\langle 0|, \quad \mathscr{E}_{AD}(|0\rangle\langle 1|) = \sqrt{1-\gamma}|0\rangle\langle 1|$$
$$\mathscr{E}_{AD}(|1\rangle\langle 0|) = \sqrt{1-\gamma}|1\rangle\langle 0|, \quad \mathscr{E}_{AD}(|1\rangle\langle 1|) = (1-\gamma)|1\rangle\langle 1| + \gamma|0\rangle\langle 0|$$

Using these results we have

$$\begin{aligned}
&\big(I\otimes\mathscr{E}_{AD}\big)\big(|\psi\rangle\langle\psi|\big) = \big(I\otimes\mathscr{E}_{AD}\big)\big(|a|^2|01\rangle\langle 10| + ab^*|01\rangle\langle 10| + ba^*|10\rangle\langle 01| + |b|^2|10\rangle\langle 10|\big)\\
&= \big(I\otimes\mathscr{E}_{AD}\big)\big(|a|^2|0\rangle\langle 0|\otimes|1\rangle\langle 1| + ab^*|0\rangle\langle 1|\otimes|1\rangle\langle 0| + ba^*|1\rangle\langle 0|\otimes|0\rangle\langle 1| + |b|^2|1\rangle\langle 1|\otimes|0\rangle\langle 0|\big)\\
&= |a|^2(1-\gamma)|0\rangle\langle 0|\otimes|1\rangle\langle 1| + |a|^2\gamma|0\rangle\langle 0|\otimes|0\rangle\langle 0| + ab^*\sqrt{1-\gamma}|0\rangle\langle 1|\otimes|1\rangle\langle 0| + ba^*\sqrt{1-\gamma}|1\rangle\langle 0|\otimes|0\rangle\langle 1| + |b|^2|1\rangle\langle 1|\otimes|0\rangle\langle 0|\\
&\Rightarrow \big(\mathscr{E}_{AD}\otimes I\big)\big(I\otimes\mathscr{E}_{AD}\big)\big(|\psi\rangle\langle\psi|\big) = \big(\mathscr{E}_{AD}\otimes\mathscr{E}_{AD}\big)\big(|\psi\rangle\langle\psi|\big) = |a|^2\big(1-\gamma\big)|01\rangle\langle 01| + |a|^2\gamma|00\rangle\langle 00| + ab^*\big(1-\gamma\big)|01\rangle\langle 10|\\
&+ba^*\big(1-\gamma\big)|10\rangle\langle 01| + |b|^2\big(1-\gamma\big)|10\rangle\langle 10| + |b|^2\gamma|00\rangle\langle 00|\\
&= \sqrt{1-\gamma}I\big[|a|^2|01\rangle\langle 10| + ab^*|01\rangle\langle 10| + ba^*|10\rangle\langle 01| + |b|^2|10\rangle\langle 10|\big]I\sqrt{1-\gamma} + \big[|a|^2 + |b|^2\big]\gamma|00\rangle\langle 00|\\
&\Rightarrow \big(\mathscr{E}_{AD}\otimes\mathscr{E}_{AD}\big)\big(|\psi\rangle\langle\psi|\big) = \sqrt{1-\gamma}I|\psi\rangle\langle\psi|I\sqrt{1-\gamma} + \big[|a|^2 + |b|^2\big]\gamma|00\rangle\langle 00|
\end{aligned}$$

We can check that the second term in the above expression for $\big(\mathscr{E}_{AD}\otimes\mathscr{E}_{AD}\big)\big(|\psi\rangle\langle\psi|\big)$ is the result of $E_1^{\mathrm{dr}}|\psi\rangle\langle\psi|E_1^{\mathrm{dr}\dagger}$.

$$\begin{aligned}
&\sqrt{\gamma}\big(|00\rangle\langle 01| + |00\rangle\langle 10|\big)\big(|a|^2|01\rangle\langle 10| + ab^*|01\rangle\langle 10| + ba^*|10\rangle\langle 01| + |b|^2|10\rangle\langle 10|\big)\sqrt{\gamma}\big(|01\rangle\langle 00| + |10\rangle\langle 00|\big)\\
&= \gamma\big(|a|^2\big)
\end{aligned}$$