Part III, Lent 2018
Quantum Information Theory

Example Sheet 2

Exercise 1

1. Prove that if A is positive semi-definite, then A is Hermitian.

2. The action of a flip operator $\mathbb{F} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, where $\mathcal{H}_A, \mathcal{H}_B \simeq \mathbf{C}^d$, is defined through the following equation:

$$\mathbb{F}|i\rangle \otimes |j\rangle = |j\rangle \otimes |i\rangle,$$

where $\{|i\rangle\}_{i=1}^d$ denotes an orthonormal basis of $\mathbf{C}^d$. Write an explicit expression for $\mathbb{F}$ in terms of the basis vectors $|i\rangle$. What are the eigenvalues of $\mathbb{F}$ and what are their multiplicities? Express $\mathbb{F}$ in terms of the MES

$$|\Omega\rangle := \frac{1}{\sqrt{d}}|i\rangle \otimes |i\rangle.$$

Hint: Think of what mathematical operation you would use to relate one to the other.

Use the relation that you obtain to rewrite equations (1.4) and (1.5) of Lemma 1 of Notes 7 (on the course webpage) using the flip operator instead of the MES.

Solution

1. If $A \geq 0$, then $\langle v, Av\rangle \geq 0$ for all $|v\rangle \in \mathcal{H}$. In particular, $\langle v|Av\rangle \in \mathbb{R}$. Then

$$\langle v|Av\rangle = \overline{\langle v|Av\rangle} = \langle Av|v\rangle = \langle v|A^*v\rangle\,.$$

That is,

$$\langle v|(A - A^*)v\rangle = 0, \qquad \forall\, |v\rangle \in \mathcal{H}. \tag{1}$$

Next, we can see that the operator $B := A - A^*$ is *normal*, i.e. it commutes with it's adjoint. Since $B^* = A^* - A = -B$, we have

$$BB^* = B(-B) = -B^2$$

and

$$B^*B = (-B)B = -B^2.$$

Thus, $[B, B^*] = 0$ and thus B is normal. Therefore, B is diagonal in some basis $|i\rangle$. Since $\langle i|\, B\, |i\rangle$ is the ith entry on the diagonal when B is written in the basis $|i\rangle$, by letting $|v\rangle$ range over $|i\rangle$ in (1), we see that all of the diagonal entries of B are zero. Since all the other entries of B are zero in this basis too, B is thus the zero matrix. Therefore, $A = A^*$.

2. Since $\mathbb{F}\,|i\rangle \otimes |j\rangle = |j\rangle \otimes |i\rangle$, we see that we can write

$$\mathbb{F} = \sum_{i,j} (|j\rangle \otimes |i\rangle)(\langle i| \otimes \langle j|) = \sum_{i,j} |ji\rangle\, \langle ij|\,. \tag{2}$$

Indeed, this must be a matrix representation of $\mathbb{F}$ as it agrees with $\mathbb{F}$ on the basis $\{|i\rangle \otimes |j\rangle\}$. We can see that $\mathbb{F}$ is self-adjoint:

$$\langle ij, \mathbb{F}ij\rangle = \langle ij, ji\rangle = \delta_{ij} = \langle ji, ij\rangle = \langle \mathbb{F}ij, ij\rangle = \langle ij, \mathbb{F}^*ij\rangle\,. \tag{3}$$

That is, $\langle ij, (\mathbb{F} - \mathbb{F}^*)ij\rangle = 0$ for all i, j. Since $\{|i\rangle \otimes |j\rangle\}_{i,j}$ is a basis of $\mathbf{C}^d \otimes \mathbf{C}^d$, we have $\langle v, (\mathbb{F} - \mathbb{F}^*)v\rangle = 0$ for every $|v\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d$. Just as before, we find we must have $\mathbb{F} = \mathbb{F}^*$.

We can see that $\mathbb{F}^2 = \mathbb{1}$ since

$$\mathbb{F}^2\,|i\rangle \otimes |j\rangle = \mathbb{F}\,|j\rangle \otimes |i\rangle = |i\rangle \otimes |j\rangle\,. \tag{4}$$

Since the eigenvalues of $\mathbb{F}^2$ are the squares of the eigenvalues of $\mathbb{F}$, we must have that every eigenvalue of $\mathbb{F}$ is ± 1. Moreover, they must not all be 1 since $\mathbb{F} \neq \mathbb{1}$.

The eigenspace associated to $+1$ is the so-called "symmetric subspace": the subspace of vectors of $\mathbf{C}^d \otimes \mathbf{C}^d$ which is invariant under swapping, while the eigenspace associated to -1 is the "anti-symmetric subspace".

Define

$$P_{\text{sym}} = \frac{1}{2}(\mathbb{1} + F), \qquad P_{\text{asym}} = \frac{1}{2}(\mathbb{1} - F). \tag{5}$$

$$P_{\text{sym}}^2 = \frac{1}{4}(\mathbb{1} + 2\mathbb{F} + \mathbb{F}^2) = \frac{1}{4}(2\mathbb{1} + 2\mathbb{F}) = P_{\text{sym}}. \tag{6}$$

Since $\mathbb{1}$ and $\mathbb{F}$ are self-adjoint, so is P_{sym}. Thus, P_{sym} is an orthogonal projection, and thus positive semi-definite. Similarly, we see that

$$P_{\text{asym}}^2 = \frac{1}{4}(\mathbb{1}^2 + F^2 - 2F) = \frac{1}{2}(\mathbb{1} - F) = P_{\text{asym}} \tag{7}$$

and hence P_{asym} is an orthogonal projection. Moreover,

$$\mathbb{F} = P_{\text{sym}} - P_{\text{asym}}. \tag{8}$$

We have written $\mathbb{F}$ as a sum of its eigenvalues times orthogonal projections, and thus have found the spectral decomposition of $\mathbb{F}$. The multiplicity of $+1$ is thus the dimension of the subspace associated to P_{sym}, which is

$$\dim \operatorname{span}\{|v\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d : P_{\text{sym}} |v\rangle = |v\rangle\} = \operatorname{rank} P_{\text{sym}} = \operatorname{tr} P_{\text{sym}} \tag{9}$$

using that P_{sym} is a orthogonal projection, so its rank is its trace. The trace we may easily compute:

$$\begin{aligned}
\operatorname{tr} P_{\text{sym}} &= \frac{d^2}{2} + \frac{1}{2}\operatorname{tr}[\mathbb{F}] \\
&= \frac{d^2}{2} + \frac{1}{2}\sum_{ij} \langle ij|\mathbb{F}ij\rangle \\
&= \frac{d^2}{2} + \frac{1}{2}\sum_{ij} \langle ij|ji\rangle \\
&= \frac{d^2}{2} + \frac{1}{2}\sum_{ij} \delta_{ij} \\
&= \frac{d^2}{2} + \frac{1}{2}d = \frac{d^2+1}{2}.
\end{aligned}$$

The multiplicity of -1 is therefore $d^2 - \frac{d^2+1}{2} = \frac{d^2-1}{2}$, since the total number of eigenvalues is d^2 (since $\mathbb{F}$ is an operator on a d^2-dimensional vector space, $\mathbf{C}^d \otimes \mathbf{C}^d$).

To relate $\mathbb{F}$ to $|\Omega\rangle$ we note that

$$\Omega := |\Omega\rangle\langle\Omega| = \frac{1}{d}\sum_{ij} |i\rangle\langle j| \otimes |i\rangle\langle j|. \tag{10}$$

Thus, if we take the transpose over the second system in the basis $|i\rangle$ as the operator T, we have

$$(\mathrm{id} \otimes T)\Omega = \frac{1}{d}\sum_{ij} |i\rangle\langle j| \otimes |j\rangle\langle i| = \frac{1}{d}\mathbb{F}. \tag{11}$$

Thus,

$$\mathbb{F} = d(\mathrm{id} \otimes T)\Omega. \tag{12}$$

Lastly, we wish to rewrite

$$\langle\Omega|A \otimes B|\Omega\rangle = \frac{1}{d}\operatorname{tr}[A^T B] \tag{1.4}$$

and

$$A \otimes I\,|\Omega\rangle = (I \otimes A^T)\,|\Omega\rangle \tag{1.5}$$

using $\mathbb{F}$ instead of $|\Omega\rangle$.

First, we note

$$\langle\Omega|A \otimes B|\Omega\rangle = \operatorname{tr}[(A \otimes B)\,|\Omega\rangle\langle\Omega|] = \operatorname{tr}[(A \otimes B)\Omega]. \tag{13}$$

Then, since $\Omega = \frac{1}{d}(\mathrm{id} \otimes T)\mathbb{F}$ (since $T^2 = \mathrm{id}$), we have

$$\langle\Omega|A \otimes B|\Omega\rangle = \frac{1}{d}\operatorname{tr}[(A \otimes B)(\mathrm{id} \otimes T)\mathbb{F}]. \tag{14}$$

Therefore, (1.4) becomes

$$\frac{1}{d}\operatorname{tr}[(\mathrm{id} \otimes T)(\mathbb{F})(A \otimes B)] = \frac{1}{d}\operatorname{tr}[A^T B]. \tag{15}$$

Note $\mathrm{id} \otimes T$ is a superoperator acting on $\mathbb{F}$, the result of which is then multiplied by $(A \otimes B)$ in the trace.

For (1.5), we may consider the action of $A \otimes I$ on Ω. We have

$$(A \otimes I)\Omega = (A \otimes I) |\Omega\rangle \langle\Omega| = (I \otimes A^T) |\Omega\rangle \langle\Omega| = (I \otimes A^T)\Omega. \quad (16)$$

Therefore, using $\Omega = \frac{1}{d}(\mathrm{id} \otimes T)\mathbb{F}$, we have

$$(A \otimes I)(\mathrm{id} \otimes T)\mathbb{F} = (I \otimes A^T)(\mathrm{id} \otimes T)\mathbb{F} \quad (17)$$

Exercise 2 Show that any density operator of a qubit can be written as

$$\varrho = \tfrac{1}{2}\left(\mathbb{1} + \vec{s} \cdot \vec{\sigma}\right) = \tfrac{1}{2} \sum_{k=0}^{3} s_k \sigma_k, \quad (18)$$

where $\vec{s} = (s_1, s_2, s_3)$ is a real three–dimensional vector such that $||\vec{s}|| \leq 1$. In the above $\vec{\sigma} := (\sigma_1, \sigma_2, \sigma_3)$, with $\sigma_1, \sigma_2, \sigma_3$ being the three Pauli matrices $\sigma_x, \sigma_y, \sigma_z$. Moreover, σ_0 denotes the 2×2 identity matrix.

The vector $\vec{s}$ is usually referred to as the Bloch vector. The set of all Bloch vectors defines a sphere which is called the *Bloch sphere*. It provides a useful geometrical representation of the states of a qubit.

Show that $s_k = \mathrm{tr}\sigma_k\varrho$. Show that $||\vec{s}|| = 1$ for a pure state ρ. What is the Bloch representation of the completely mixed state $\rho = \mathbf{I}/2$? What do the North Pole and the South Pole of the Bloch sphere correspond to?

Solution

Any qubit density matrix can be written as

$$\rho = \begin{pmatrix} a & b - ic \\ b + ic & 1 - a \end{pmatrix} \quad (19)$$

where a, b, c are real numbers. This is simply because ρ is trace 1 and self-adjoint. For any vector $\vec{s} = (s_x, s_y, s_z)$, we can compute

$$\vec{s} \cdot \vec{\sigma} = \begin{pmatrix} s_z & s_x - is_y \\ s_x + is_y & -s_z \end{pmatrix} \quad (20)$$

Therefore,

$$\frac{I}{2} + \frac{1}{2}\vec{s} \cdot \vec{\sigma} = \begin{pmatrix} \frac{1}{2} + \frac{1}{2}s_z & \frac{1}{2}s_x - \frac{1}{2}is_y \\ \frac{1}{2}s_x + \frac{1}{2}is_y & \frac{1}{2} - \frac{1}{2}s_z \end{pmatrix} \quad (21)$$

Now, simply choose $s_z = 2a - 1$, $s_x = 2b$ and $s_y = 2c$. By checking each matrix entry, we find that $\rho = \frac{I}{2} + \frac{1}{2}\vec{s} \cdot \vec{\sigma}$. To check $\|\vec{s}\| \leq 1$, we need to use more properties of ρ. First,

$$\begin{aligned} \|\vec{s}\|^2 = s_x^2 + s_y^2 + s_z^2 &= (2a-1)^2 + 4b^2 + 4c^2 \\ &= 4a^2 + 1 - 4a + 4b^2 + 4c^2 \\ &= 1 - 4(a - r) \end{aligned}$$

for $r := a^2 + b^2 + c^2$. Therefore, $\|\vec{s}\| = \sqrt{1 - 4(a-r)}$.

Since ρ is a density matrix, its eigenvalues are non-negative. This implies a constraint on a, b, c. We solve the characteristic equation by setting the determinant of $\rho - \lambda I$ to zero:

$$\begin{aligned} 0 = \begin{vmatrix} a - \lambda & b - ic \\ b + ic & 1 - a - \lambda \end{vmatrix} &= (a - \lambda)(1 - a - \lambda) - (b^2 + c^2) \\ \lambda^2 - \lambda + a - (a^2 + b^2 + c^2) &= 0. \end{aligned}$$

Then

$$\lambda = \frac{1 \pm \sqrt{1 - 4(a-r)}}{2} \geq 0. \quad (22)$$

That is,

$$1 - \sqrt{1 - 4(a-r)} \geq 0 \iff \sqrt{1 - 4(a-r)} \leq 1. \quad (23)$$

That is, $\|\vec{s}\| \leq 1$. Moreover, $\|\vec{s}\| = 1$ if and only if one of the eigenvalues is zero, by (22). Thus, $\|\vec{s}\| = 1$ if and only if ρ is pure. By the same equation, we can see if the two eigenvalues are $\frac{1}{2}$, we must have $\|\vec{s}\| = \sqrt{1 - 4(a-r)} = 0$. That is, the Bloch vector for the completely mixed state is $\vec{s} = \vec{0}$.

The north pole is when $\vec{s} = (0, 0, 1)$. In that case, since $s_z = 2a - 1$, $s_x = 2b$ and $s_y = 2c$, we have $a = 1$, $b = c = 0$. That is, $\rho = |0\rangle \langle 0|$. For the south pole, $\vec{s} = (0, 0, -1)$. Then $a = b = c = 0$, so $\rho = |1\rangle \langle 1|$.

Next,

$$\mathrm{tr}[\sigma_k \rho] = \frac{1}{2}\mathrm{tr}[\sigma_k] + \frac{1}{2}\sum_{j \neq k} s_j \mathrm{tr}[\sigma_k \sigma_j] + \frac{1}{2}s_k \mathrm{tr}[\sigma_k^2]. \quad (24)$$

Note each Pauli matrix is traceless (besides the identity), so the first term is zero. For the second term, we can use the relation

$$\sigma_a \sigma_b = \delta_{ab} I + i \sum_c \varepsilon_{abc} \sigma_c \quad (25)$$

where ε_{abc} is either $+1, -1$, or zero, depending on a, b, c (this is the so-called Levi-Civita symbol). Taking the trace, $\mathrm{tr}[\sigma_a \sigma_b] = \delta_{ab}\mathrm{tr}[I] = 2\delta_{ab}$, since σ_c is traceless. Finally, for any Pauli matrix, $\sigma_k^2 = I$. So (24) becomes

$$\mathrm{tr}[\sigma_k \rho] = \frac{1}{2} \cdot 0 + \frac{1}{2} \sum_{j \neq k} s_j \cdot 0 + \frac{1}{2} s_k (2) = s_k. \tag{26}$$

Exercise 3 Given the density matrix

$$\rho = \begin{pmatrix} \frac{3}{5} & \frac{1}{4} - i\frac{1}{6} \\ \frac{1}{4} + i\frac{1}{6} & \frac{2}{5} \end{pmatrix}$$

what is the Bloch vector $\vec{s} = (s_x, s_y, s_z)$ for ρ? Is it a pure state or a mixed state? What is the probability that a measurement of the spin of the qubit along the Z-axis will yield a value $+1$?

Solution

We can write

$$\rho = \frac{1}{2} I + \frac{1}{2} \begin{pmatrix} \frac{1}{5} & \frac{1}{2} - \frac{i}{3} \\ \frac{1}{2} + \frac{i}{3} & -\frac{1}{5} \end{pmatrix} \tag{27}$$

Note

$$\vec{s} \cdot \vec{\sigma} = \begin{pmatrix} s_z & s_x - i s_y \\ s_x + i s_y & -s_z \end{pmatrix} \tag{28}$$

Therfore, we can identify $s_x = \frac{1}{2}$, $s_y = \frac{1}{3}$, and $s_z = \frac{1}{5}$. Since $\|\vec{s}\| = \sqrt{\frac{1}{4} + \frac{1}{9} + \frac{1}{25}} = \frac{19}{30} < 1$, the state ρ is mixed.

Since

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{29}$$

the projector onto its $+1$ eigenspace is just $|0\rangle \langle 0|$. Therefore, the probability of getting outcome $+1$ when measuring ρ by the σ_z observable is given by

$$\mathrm{tr}[\rho \sigma_z] = |0\rangle \, \rho \, \langle 0| = \frac{1}{2} + \frac{1}{2}\frac{1}{5} = \frac{6}{10} = \frac{3}{5}. \tag{30}$$

Exercise 4 Show that the set of density operators acting on a Hilbert space $\mathcal{H}$, where $\dim \mathcal{H} = d$ is a *convex subset* of the real vector space of $d \times d$ Hermitian matrices. Show that pure states are extremal points of this set.

Solution

Let ρ, σ be density operators. To show the set of density operators is convex, we only need to show that $t\rho + (1-t)\sigma$ is a density operator for every $t \in (0, 1)$. Note $t\rho + (1-t)\sigma$ is called a *convex combination* of ρ and σ, if $t \in (0, 1)$. We have

$$\mathrm{tr}[t\rho + (1-t)\sigma] = t\mathrm{tr}[\rho] + (1-t)\mathrm{tr}[\sigma] = t + 1 - t = 1. \tag{31}$$

Additionally, for every vector $|v\rangle \in \mathcal{H}$,

$$\langle v, [t\rho + (1-t)\sigma] v \rangle = t \langle v, \rho v \rangle + (1-t) \langle v, \sigma v \rangle . \tag{32}$$

Since ρ and σ are positive semidefinite, $\langle v, \rho v \rangle \geq 0$ and $\langle v, \sigma v \rangle \geq 0$. As the sum of two positive numbers, we then have $\langle v, [t\rho + (1-t)\sigma] v \rangle \geq 0$. Since $|v\rangle \in \mathcal{H}$ is arbitrary, we therefore have that $t\rho + (1-t)\sigma$ is positive semi-definite. Thus, $t\rho + (1-t)\sigma$ is a density matrix, proving that the set of density matrices is convex.

A point x in a convex set $\mathcal{C}$ is called extremal if $\lambda y + (1-\lambda) z = x$ for $y, z \in \mathcal{C}$ and $\lambda \in (0, 1)$ implies that $x = y = z$. Consider therefore $|\psi\rangle = \lambda \rho_1 + (1-\lambda)\rho_2$ where $|\psi\rangle \in \mathcal{H}$ is a pure state and $\lambda \in (0, 1)$. Let $|\varphi\rangle \in \mathrm{span}\{|\psi\rangle\}^\perp$ be any vector from the orthogonal complement to the subspace spanned by $|\psi\rangle$. Then we have

$$0 = \langle \varphi | \psi | \varphi \rangle = \lambda \langle \varphi | \rho_1 | \varphi \rangle + (1-\lambda) \langle \varphi | \rho_2 | \varphi \rangle.$$

Since $\lambda > 0$ and $1 - \lambda > 0$, this implies $\langle \varphi | \rho_1 | \varphi \rangle = \langle \varphi | \rho_2 | \varphi \rangle = 0$ for all $|\varphi\rangle \in \mathrm{span}\{|\psi\rangle\}^\perp$. Hence, $\rho_1 = \rho_2 = \psi$.

Exercise 5 Find the Schmidt ranks for each of the following states

$$|\phi_1\rangle = \tfrac{1}{2}(|00\rangle + |11\rangle + |22\rangle + |44\rangle) \qquad |\phi_2\rangle = \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$|\phi_3\rangle = \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \qquad |\phi_4\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle)$$

Solution

$|\phi_1\rangle$ is already in Schmidt form,

$$|\phi_1\rangle = \sum_{i=1}^{4} \frac{1}{4} |ii\rangle . \tag{33}$$

For the state $|\phi_2\rangle$, we see

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{34}$$

is a separable pure state, and therefore has Schmidt rank 1.

The state $|\phi_3\rangle$ is a maximally entangled state, as can be verified by hand, and thus has Schmidt rank 2. A shorter proof proceeds as follows. We may write

$$|\phi_3\rangle = \frac{1}{2}|0\rangle(|0\rangle + |1\rangle) + \frac{1}{2}|1\rangle(|0\rangle - |1\rangle). \tag{35}$$

Often we use the notation

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{36}$$

Note $\{|+\rangle, |-\rangle\}$ is a basis of $\mathbf{C}^2$. Then (35) shows

$$|\phi_3\rangle = \frac{1}{\sqrt{2}}|0\rangle|+\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle \tag{37}$$

which is a Schmidt decomposition of $|\phi_3\rangle$, which is therefore of Schmidt rank 2.

The fourth state is $|\phi_4\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle)$. Then

$$\begin{aligned}|\phi_4\rangle\langle\phi_4| = \frac{1}{3}[&|00\rangle\langle 00| + |00\rangle\langle 01| + |00\rangle\langle 11| \\ &|01\rangle\langle 00| + |01\rangle\langle 01| + |01\rangle\langle 11| \\ &|11\rangle\langle 00| + |11\rangle\langle 01| + |11\rangle\langle 11|].\end{aligned}$$

Then

$$\begin{aligned}\mathrm{tr}_B|\phi_4\rangle\langle\phi_4| &= \frac{1}{3}[|0\rangle\langle 0| \\ &\quad |0\rangle\langle 0| + |0\rangle\langle 1| \\ &\quad + |1\rangle\langle 0| + |1\rangle\langle 1|] \\ &= \frac{1}{3}\begin{pmatrix}2 & 1\\ 1 & 1.\end{pmatrix}\end{aligned}$$

This has eigenvalues $\frac{3\pm\sqrt{5}}{2}$. Since $\mathrm{tr}_B|\phi_4\rangle\langle\phi_4|$ has exactly two non-zero eigenvalue, the Schmidt rank of $|\phi_4\rangle$ is two.

Exercise 6 Let $|\Psi_{AR}\rangle$ and $|\Phi_{AR}\rangle$ be two purifications of a state ρ of a system A to a composite system AR. Prove that there exists a unitary transformation U_R acting on system R alone such that

$$|\Phi_{AR}\rangle = (\mathbf{I}_A \otimes U_R)|\Psi_{AR}\rangle.$$

Solution

To be fully rigorous, first we need a result about Schmidt decompositions to show that we can choose the basis on the A system to be any eigenbasis we choose of ρ_A. If this part does not interest you, skip ahead.

Lemma 0.1 *If the state ρ_A has eigendecomposition $\rho_A = \sum_i p_i |i\rangle\langle i|_A$, then $|\Phi_{AR}\rangle$ has a Schmidt decomposition*

$$|\Phi_{AR}\rangle = \sum_i \sqrt{p_i}|i\rangle_A|e_i\rangle_R.$$

If ρ_A is non-degenerate (all the p_i's are unique), then it was shown in class that the Schmidt decomposition is unique, and moreover the basis on the A part is the eigenbasis of ρ_A, as was claimed here.

Otherwise, the Schmidt decomposition is not unique, and a priori, we don't know that the basis on the A system is the basis $|i\rangle_A$, our chosen eigenbasis for ρ_A. We can quickly show that the basis on the A system is an eigenbasis for ρ_A, however. Let

$$|\Phi_{AR}\rangle = \sum_i \sqrt{p_i}|h_i\rangle_A|e_i\rangle_R \tag{38}$$

be a Schmidt decomposition of $|\Phi_{AR}\rangle$; then, $\{|h_i\rangle_A\}_i$ is some orthonormal basis of $\mathcal{H}_\mathcal{A}$. Then

$$\begin{aligned}\rho_A &= \mathrm{tr}_R[\Phi_{AR}\langle\Phi_{AR}|] = \mathrm{tr}_R\sum_{ij}\sqrt{p_ip_j}\mathrm{tr}_R[|h_i\rangle\langle h_j|_A \otimes |e_i\rangle\langle e_j|_R] \\ &= \sum_{ij}\sqrt{p_ip_j}|h_i\rangle\langle h_j|_A\langle e_j|e_i\rangle_R \\ &= \sum_i p_i|h_i\rangle\langle h_i|_A.\end{aligned}$$

This shows that $|h_i\rangle$ is an eigenbasis of ρ_A (i.e., $\rho_A |h_i\rangle = p_i |h_i\rangle$). Now it gets a little tricky, because eigendecompositions are not unique. A diagonalizable matrix induces a unique decomposition of the full Hilbert space into subspaces corresponding to the different eigenvalues. (Recall: the set of eigenvectors of a matrix M for a particular eigenvalue e for a subspace, because you can take linear combinations of them and still get an eigenvector of M for the eigenvalue e). But these subspaces don't need to be one-dimensional (i.e., ρ_A could be degenerate).

Moreover, it's not enough that $|h_i\rangle$ is some eigenbasis of ρ_A, since we will be considering another purification of ρ_A, and we want to have the same basis on the A system in both. So we will show the above lemma, proving that even if ρ_A is degenerate, for any eigenbasis of ρ_A and any purification of $|\Phi_{AR}\rangle$ of ρ_A, there is a Schmidt decomposition with the A-basis being the eigenbasis of ρ_A that we had chosen.

Let us rewrite (38) as

$$|\Phi_{AR}\rangle = \sum_{\mu} \sum_{i:p_i=\mu} p_i |h_i\rangle \otimes |e_i\rangle \tag{39}$$

where μ ranges over the *distinct* eigenvalues of ρ_A. Let

$$E_\mu := \{|v\rangle : \rho_A |v\rangle = \mu |v\rangle\} \tag{40}$$

be the eigenspace of ρ_A associated to μ. Then since both $\{|i\rangle : p_i = \mu\}$ and $\{|h_i\rangle : p_i = \mu\}$ form an orthonormal basis of E_μ, the operator

$$U^\mu = \sum_{i:p_i=\mu} |h_i\rangle \langle i| \tag{41}$$

is a unitary transformation mapping the basis $\{|i\rangle : p_i = \mu\}$ to $\{|h_i\rangle : p_i = \mu\}$. Then,

$$|\Phi_{AR}\rangle = \sum_{\mu} \mu (U^\mu \otimes I) \sum_{i:p_i=\mu} |i\rangle \otimes |e_i\rangle . \tag{42}$$

Now, we will do something similar to the reflection trick for maximally entangled states. Let us show there exists a unitary operator U'^μ on R such that

$$(U^\mu \otimes I) \sum_{i:p_i=\mu} |i\rangle \otimes |e_i\rangle = (I \otimes U'^\mu) \sum_{i:p_i=\mu} |i\rangle \otimes |e_i\rangle . \tag{43}$$

We may expand U^μ as

$$U^\mu = \sum_{k,\ell} u_{k\ell} |\ell\rangle \langle k| \tag{44}$$

for some coefficients $u_{k\ell}$. Note we may restrict the sum to k, ℓ such that $p_k = p_\ell = \mu$, since $U^\mu |v\rangle = 0$ for $|v\rangle \notin E_\mu$. We won't write this restriction in every sum for notational simplicity, however. We have

$$\begin{aligned}(U^\mu \otimes I) \sum_{i:p_i=\mu} |i\rangle \otimes |e_i\rangle &= \sum_{i:p_i=\mu} \sum_{k,\ell} u_{k\ell} |\ell\rangle \langle k|i\rangle \otimes |e_i\rangle \\ &= \sum_{i:p_i=\mu} \sum_{\ell} u_{i\ell} |\ell\rangle \otimes |e_i\rangle\end{aligned}$$

Next, we sum over an additional variable j, but multiply by $\delta_{j\ell} = \langle e_j | e_\ell \rangle$:

$$= \sum_{i,j,\ell} u_{i\ell} |\ell\rangle \otimes (|e_i\rangle \langle e_j|e_\ell\rangle)$$

Since all the terms with $j \neq \ell$ are zero, we may change the index of the coefficent $u_{i\ell} \to u_{ij}$:

$$= \sum_{i,j,\ell} u_{ij} |\ell\rangle \otimes (|e_i\rangle \langle e_j|e_\ell\rangle)$$

Now, we use $|e_i\rangle \langle e_j|e_\ell\rangle = (|e_i\rangle \langle e_j|) |e_\ell\rangle$:

$$\begin{aligned}&= \sum_{i,j,\ell} u_{ij} |\ell\rangle \otimes (|e_i\rangle \langle e_j|) |e_\ell\rangle \\ &= \sum_{\ell} |\ell\rangle \otimes (\sum_{i,j} u_{ij} |e_i\rangle \langle e_j|) |e_\ell\rangle \\ &= \sum_{\ell} |\ell\rangle \otimes (U'^\mu |e_\ell\rangle)\end{aligned}$$

for

$$U'^\mu = \sum_{i,j} u_{ij} |e_i\rangle \langle e_j| . \tag{45}$$

We can check that U'^{μ} is unitary using that U^{μ} is unitary, proving the claim. Returning to (42),

$$\begin{aligned}|\Phi_{AR}\rangle &= \sum_{\mu} \mu (I \otimes U'^{\mu}) \sum_{i:p_i=\mu} |i\rangle \otimes |e_i\rangle \\ &= \sum_{\mu} \sum_{i:p_i=\mu} p_i \, |i\rangle \otimes (U'^{\mu} \, |e_i\rangle).\end{aligned}$$

Since $\text{span}\{U'^{\mu} \, |e_i\rangle : i \text{ such that } p_i = \mu\} = \text{span}\{|e_i\rangle : i \text{ such that } p_i = \mu\}$, and unitaries preserve orthogonality, we have simply changed the basis on the reference. Thus, defining

$$|e'_i\rangle = U^{\mu} \, |e_i\rangle : \mu \text{ is such that } \mu = p_i \tag{46}$$

we have

$$|\Phi_{AR}\rangle = \sum_i p_i \, |i\rangle \otimes |e'_i\rangle \, . \tag{47}$$

Thus, there exists a Schmidt decomposition of $|\Phi_{AR}\rangle$ with the basis on the A system being the basis $|i\rangle$.

This concludes the proof of the lemma. We will drop the $'$s from the notation, since we might as well assume we started with the right Schmidt decomposition.

We may use the lemma again to see that $|\Psi_{AR}\rangle$ has a Schmidt decomposition

$$|\Psi_{AR}\rangle = \sum_i \sqrt{p_i} \, |i\rangle_A \, |f_i\rangle_R \, .$$

Then let U_R be defined by $U_R \, |f_i\rangle_R = |e_i\rangle_R$. That is,

$$U_R = \sum_i |e_i\rangle \langle f_i|_R \, .$$

Then

$$U_R^* U_R = \sum_{i,j} |f_i\rangle \langle e_i|_R \, |e_j\rangle \langle f_j|_R = \sum_i |f_i\rangle \langle f_i|_R = I_R$$

using $\langle e_i | f_j \rangle = \delta_{ij}$. Lastly,

$$(I_A \otimes U_R) \, |\Psi_{AR}\rangle = \sum_i \sqrt{p_i} \, |i\rangle_A \, U_R \, |f_i\rangle_R = \sum_i \sqrt{p_i} \, |i\rangle_A \, |e_i\rangle_R = |\Phi\rangle_{AR} \, .$$

Exercise 7 (Unitary freedom in the Kraus decomposition)

Suppose $\{A_i\}_{i=1}^n$ and $\{B_i\}_{i=1}^n$ are Kraus operators giving rise to quantum operations Λ and Λ', respectively. Prove that $\Lambda = \Lambda'$ if and only if there exist complex numbers u_{ij} such that $A_i = \sum_{j=1}^n u_{ij} B_j$, and u_{ij} are the elements of an $n \times n$ unitary matrix.

Solution

Assume $A_i = \sum_{j=1}^n u_{ij} B_j = \sum_{j=1}^n \langle i|Uj\rangle \, B_j$. Then for any operator $X \in \mathbf{B}(\mathcal{H})$,

$$\begin{aligned}\Lambda(X) &= \sum_i A_i X A_i^* \\ &= \sum_{i,j,k=1}^n \langle i|Uj\rangle \, \overline{\langle i|Uk\rangle} B_j X B_k^* \\ &= \sum_{i,j,k=1}^n \langle i|Uj\rangle \, \langle Uk, i\rangle \, B_j X B_k^* \\ &= \sum_{i,j,k=1}^n \langle i|Uj\rangle \, \langle k, U^*i\rangle \, B_j X B_k^* \\ &= \sum_{i,j,k=1}^n \langle k, U^*i\rangle \, \langle i|Uj\rangle \, B_j X B_k^* \\ &= \sum_{j,k=1}^n \langle k, U^*Uj\rangle \, B_j X B_k^* \\ &= \sum_{j,k=1}^n \langle k, j\rangle \, B_j X B_k^* \\ &= \sum_{j=1}^n B_j X B_j^* \\ &= \Lambda'(X).\end{aligned}$$

On the other hand, if $\Lambda = \Lambda'$, then

$$(\text{id} \otimes \Lambda)\Omega = (\text{id} \otimes \Lambda')\Omega \tag{48}$$

for $\Omega = |\Omega\rangle\langle\Omega|$, the maximally entangled state, $|\Omega\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|ii\rangle$. That is,

$$(\mathrm{id}\otimes\Lambda)\Omega = \sum_{i=1}^{n}(\mathbb{1}\otimes A_i)\,|\Omega\rangle\langle\Omega|\,(\mathbb{1}\otimes A_i^*).$$

Setting $|\psi_i\rangle = (\mathbb{1}\otimes A_i)\,|\Omega\rangle$, we see

$$(\mathrm{id}\otimes\Lambda)\Omega = \sum_i |\psi_i\rangle\langle\psi_i|\,. \tag{49}$$

Likewise,

$$(\mathrm{id}\otimes\Lambda')\Omega = \sum_{i=1}^{n}(\mathbb{1}\otimes B_i)\,|\Omega\rangle\langle\Omega|\,(\mathbb{1}\otimes B_i^*)$$

so setting $|\tilde{\psi}_i\rangle = (\mathbb{1}\otimes B_i)\,|\Omega\rangle$, we have

$$(\mathrm{id}\otimes\Lambda')\Omega = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\,. \tag{50}$$

Therefore, $\Lambda = \Lambda'$ implies

$$\rho := \frac{1}{n}\sum_i |\psi_i\rangle\langle\psi_i| = \frac{1}{n}\sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\,. \tag{51}$$

That is, we have two decompositions of a state ρ into pure states. We can purify ρ:

$$\rho = \mathrm{tr}_C\,|\Psi\rangle\langle\Psi|\,, \qquad |\Psi\rangle = \sum_j |\psi_j\rangle\otimes|j\rangle_C\,. \tag{52}$$

We can construct another purification from the other decomposition, namely

$$\rho = \mathrm{tr}_C\,|\Phi\rangle\langle\Phi|\,, \qquad |\Phi\rangle = \sum_j |\tilde{\psi}_j\rangle\otimes|j\rangle_C\,. \tag{53}$$

Therefore, by the previous question, for some unitary U_C, we have

$$|\Psi\rangle = \mathbb{1}\otimes U_C\,|\Phi\rangle\,. \tag{54}$$

That is,

$$\sum_j |\psi_j\rangle\otimes|j\rangle_C = \sum_j |\tilde{\psi}_j\rangle\otimes U_C\,|j\rangle_C\,. \tag{55}$$

Since these two states are equal, the results of acting on them by the linear operator $\mathrm{id}\otimes\langle k|$ must be equal, for any vector $|k\rangle$. Note we can see $\mathrm{id}\otimes\langle k|$ as shorthand for the linear map

$$|\chi\rangle\otimes|\chi'\rangle \mapsto \langle k|\chi'\rangle\,|\chi\rangle \tag{56}$$

defined for any vectors $|\chi\rangle, |\chi'\rangle$ which we define on all of $\mathbf{C}^d\otimes\mathbf{C}^d$ by extending by linearity.

Hence,

$$\sum_j |\psi_j\rangle\langle k|j\rangle_C = \sum_j |\tilde{\psi}_j\rangle\langle k|\,U_C\,|j\rangle_C\,. \tag{57}$$

Since $\langle k|j\rangle_C = \delta_{kj}$,

$$|\psi_k\rangle = \sum_j \langle k|\,U_C\,|j\rangle\,|\tilde{\psi}_j\rangle\,. \tag{58}$$

Writing $u_{kj} = \langle k|\,U_C\,|j\rangle$, we have

$$|\psi_k\rangle = \sum_j u_{kj}\,|\tilde{\psi}_j\rangle\,. \tag{59}$$

Substituting our definitions of $|\psi_j\rangle$ and $|\tilde{\psi}_j\rangle$, we have

$$(\mathbb{1}\otimes A_k)\,|\Omega\rangle = \sum_j u_{kj}(\mathbb{1}\otimes B_j)\,|\Omega\rangle\,. \tag{60}$$

That is,

$$\frac{1}{\sqrt{n}}\sum_\ell(|\ell\rangle\otimes A_k\,|\ell\rangle) = \frac{1}{\sqrt{n}}\sum_\ell\sum_j u_{kj}(|\ell\rangle\otimes B_j\,|\ell\rangle). \tag{61}$$

Now, acting by $\langle\ell|\otimes\mathbb{1}$, we have

$$\frac{1}{\sqrt{n}}A_k\,|\ell\rangle = \frac{1}{\sqrt{n}}\sum_j u_{kj}B_j\,|\ell\rangle\,. \tag{62}$$

That is, for any basis vector $|\ell\rangle$,

$$A_k\,|\ell\rangle = \sum_j u_{kj}B_j\,|\ell\rangle\,. \tag{63}$$

Thus,

$$A_k = \sum_j u_{kj}B_j. \tag{64}$$

This concludes the proof.

Exercise 8 (Number of Kraus operators)

1. Consider a quantum operation $\Lambda : \mathcal{B}(\mathcal{H}_\mathcal{A}) \to \mathcal{B}(\mathcal{H}_\mathcal{B})$. What is the maximal rank of its Choi state $J(\Lambda)$?

2. Prove that any quantum operation Λ on the state ρ of a system with a d–dimensional Hilbert space, there exists a Kraus decomposition with at most d^2 elements, i.e.,

$$\Lambda(\rho) = \sum_{i=1}^{n} A_i \rho A_i^\dagger,$$

where $n \leq d^2$.

Solution

1. Let $\mathcal{H}_\mathcal{A} \cong \mathbf{C}^{d_\mathcal{A}}$. Then for $|\Omega\rangle = \frac{1}{\sqrt{d_A}} \sum_{i=1}^{d_A} |ii\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathbf{C}^{d_\mathcal{A}}$, the Choi state of Λ is

$$(\Lambda \otimes \mathrm{id}_{d_A})(\Omega) = \frac{1}{d_A} \sum_{ij} \Lambda(|i\rangle\langle j|) \otimes |i\rangle\langle j| . \tag{65}$$

As an operator on $\mathcal{H}_\mathcal{B} \otimes \mathbf{C}^{d_\mathcal{A}}$, it has rank at most $d_A d_B$, for $d_B = \dim \mathcal{H}_\mathcal{B}$.

2. Since $J(\Lambda)$ has rank at most d^2, it has an eigendecomposition

$$J(\Lambda) = \sum_{i=1}^{d^2} \lambda_i |\psi_i\rangle\langle\psi_i| . \tag{66}$$

Since $|\psi_i\rangle$ is a bipartite pure state, we know there is an operator B_i such that

$$|\psi_i\rangle = (I \otimes B_i)|\Omega\rangle . \tag{67}$$

That is,

$$J(\Lambda) = \sum_{i=1}^{d^2} \lambda_i (I \otimes B_i)|\Omega\rangle\langle\Omega|(I \otimes B_i^*). \tag{68}$$

Defining $A_i = \sqrt{\lambda_i} B_i$,

$$J(\Lambda) = \sum_{i=1}^{d^2} (I \otimes A_i)|\Omega\rangle\langle\Omega|(I \otimes A_i^*). \tag{69}$$

Now,

$$\begin{aligned}
\mathrm{tr}[C\Lambda(D)] = d\mathrm{tr}[J(\Lambda)(C \otimes D^T)] &= \sum_{i=1}^{d^2} d\mathrm{tr}[(I \otimes A_i)|\Omega\rangle\langle\Omega|(I \otimes A_i^*)C \otimes D^T] \\
&= \sum_{i=1}^{d^2} d\mathrm{tr}[|\Omega\rangle\langle\Omega| C \otimes A_i^* D^T A_i] \\
&= \sum_{i=1}^{d^2} d\,\langle\Omega|C \otimes A_i^* D^T A_i|\Omega\rangle .
\end{aligned}$$

Now, we can use Equation (1.4) of notes 7, which is a trick with the maximally entangled state: $\langle\Omega|A \otimes B|\Omega\rangle = \frac{1}{d}\mathrm{tr}[A^T B]$ for any two matrices A and B. Then

$$\begin{aligned}
\mathrm{tr}[C\Lambda(D)] &= \sum_{i=1}^{d^2} \mathrm{tr}[C^T A_i^* D^T A_i] \\
&= \sum_{i=1}^{d^2} \mathrm{tr}[(C^T A_i^* D^T A_i)^T] \\
&= \sum_{i=1}^{d^2} \mathrm{tr}[(A_i)^T D (A_i^*)^T C] \\
&= \sum_{i=1}^{d^2} \mathrm{tr}[(A_i)^T D (A_i^*)^T C] \\
&= \mathrm{tr}[C \sum_{i=1}^{d^2} (A_i)^T D (A_i^*)^T].
\end{aligned}$$

Since C and D are arbitrary, we've found that $\{A_i^T\}$ is a set of Kraus operators for Λ.

Exercise 9 Consider two quantum operations Λ_1 and Λ_2 acting on a single qubit, having Kraus representations

$$\Lambda_1(\rho) = \sum_{k=1}^{2} A_k \rho A_k^\dagger; \quad \Lambda_2(\rho) = \sum_{k=1}^{2} V_k \rho V_k^\dagger,$$

with

$$A_1 = \frac{1}{\sqrt{2}}\sigma_0 \; ; A_2 = \frac{1}{\sqrt{2}}\sigma_z$$

and

$$V_1 = |0\rangle\langle 0| \; ; V_2 = |1\rangle\langle 1|.$$

How do the actions of Λ_1 and Λ_2 differ from each other?

Solution

A straightforward calculation of the action of Λ_1 and Λ_2 on

$$\rho = \begin{pmatrix} a & b - ic \\ b + ic & 1 - a \end{pmatrix}$$

(cf. Ex. 2) shows that

$$\Lambda_1(\rho) = \Lambda_2(\rho) = \begin{pmatrix} a & 0 \\ 0 & 1 - a \end{pmatrix}.$$

Hence, the Kraus representation of a CPTP map is not unique.

Exercise 10 Show that the following three operators form a POVM.

$$\begin{aligned} E_1 &= \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1| \\ E_2 &= \frac{\sqrt{2}}{2+2\sqrt{2}} (|0\rangle - |1\rangle)(\langle 0| - \langle 1|) \\ E_3 &= \mathbb{1} - E_1 - E_2 \end{aligned}$$

Suppose Alice gives Bob a state prepared in one of the two states $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Show that if Bob does a measurement characterized by these POVM elements on the state he receives, he never makes an error of misidentification. Discuss the possible outcomes.

Solution

Let us first show that $\{E_1, E_2, E_3\}$ indeed forms a POVM. First,

$$E_1 + E_2 + E_3 = \mathbb{1} \tag{70}$$

by definition of E_3. Clearly, E_1 and E_2 are positive. For E_3, we may write a matrix representation. In the computational basis, writing $c = \frac{\sqrt{2}}{1+\sqrt{2}}$,

$$\begin{aligned} E_1 &= c \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ E_2 &= \frac{c}{2}[|0\rangle\langle 0| - |1\rangle\langle 0| - |0\rangle\langle 1| + |1\rangle\langle 1|] = \frac{c}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \\ E_3 &= \mathbb{1} - E_1 - E_2 = \begin{pmatrix} 1 - \frac{c}{2} & \frac{c}{2} \\ \frac{c}{2} & 1 - \frac{3}{2}c. \end{pmatrix} \end{aligned}$$

From this matrix form, we can compute the eigenvalues of E_3, and find they are

$$\lambda_\pm = \frac{2 - 2c \pm \sqrt{2}c}{2}. \tag{71}$$

Substituting our value of c, we find the two eigenvalues are 0 and c. Thus, E_3 is positive semi-definite (since it has all *non-negative* eigenvalues).

The probabilities for the different outcomes given that the system is in either the state $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ can be computed by

$$p_i(j) := \mathbb{P}(\text{measurement outcome is } j \mid \text{the state had index } i) = \langle\psi_i|E_j|\psi_i\rangle,$$

which gives:

$$\begin{aligned} p_1(1) &= 0 & p_2(1) &= \frac{\sqrt{2}}{2+2\sqrt{2}} \\ p_1(2) &= \frac{\sqrt{2}}{2+2\sqrt{2}} & p_2(2) &= 0 \\ p_1(3) &= \frac{2+\sqrt{2}}{2+2\sqrt{2}} & p_2(3) &= \frac{2+\sqrt{2}}{2+2\sqrt{2}} \end{aligned}$$

Therefore, Bob can infer the state of the system with certainty if he measures either outcome 1 or 2, since the system in the state $|\psi_1\rangle$ ($|\psi_2\rangle$)

will never yield outcome 1 (2). Of course, $p_1(3) = p_2(3)$ and hence, outcome 3 is indecisive and Bob can only guess the state of the system.

The advantage here is that *sometimes* Bob can say what happened with certainty. Since the two states are not orthogonal, no measurement can perfectly distinguish them, but this scheme has the advantage of allowing Bob to sometimes know with certainty what the state was, and sometimes having it be a 50-50 guess, instead of always having to guess (but being right $> 50\%$ of the time).