Exercise 5.1 Purification

A decomposition of a state $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ is a (non-unique) convex combination of pure states $\rho_A^x = |a_x\rangle\langle a_x|$ such that $\rho_A = \sum_x \lambda_x \rho_A^x$.

a) *Show that $|\Psi\rangle = \sum_x \sqrt{\lambda_x}\, |a_x\rangle_A \otimes |b_x\rangle_B$ is a purification of ρ_A for any orthonormal basis $\{\, |b_x\rangle_B \,\}_x$ of $\mathcal{H}_B$.*

It remains to show that

$$\begin{aligned}\mathrm{Tr}_B(|\Psi\rangle\langle\Psi|) &= \sum_{x,y,z} \sqrt{\lambda_y \lambda_z} |a_y\rangle\langle a_z|_A \otimes \underbrace{\langle b_x|b_y\rangle}_{\delta_{xy}} \underbrace{\langle b_z|b_x\rangle_B}_{\delta_z x} \\ &= \sum_z \lambda_x |a_x\rangle\langle a_x|_A \;=\; \rho_A.\end{aligned}$$

b) *Show that any two purifications are related by a* local *unitary transformation on the purifying system.*

Suppose we found a state $|\psi\rangle$ of the composed system $\mathcal{H}_A \otimes \mathcal{H}_B$ that purifies ρ_A, i.e., such that $\mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \rho_A$. A Schmidt decomposition (probably the most useful tool in quantum information) of $|\psi\rangle$ gives us

$$|\psi\rangle = \sum_y \theta_y |y\rangle_A |y\rangle_B,$$

where:

- $\{\theta_y\}_y$ are the square roots of the eigenvalues of the reduced states of A and $B \Rightarrow$ they have to be $\left\{\sqrt{\lambda_x}\right\}_x$;
- $\{|y\rangle_A\}_y$ are the eigenvectors of $\rho_A \Rightarrow$ they have to be $\{|x\rangle_A\}_x$;
- $\{|y\rangle_B\}_y$ are the eigenvectors of $\rho_B \Rightarrow$ there is no restriction on these.

So the $\{|y\rangle_B\}_y$ can be changed, as long as $\{\theta_y\}_y$ and $\{|y\rangle_A\}_y$ are preserved. The only way to do this is to apply a local unitary transformation on B, $\mathbb{1}_A \otimes U_B$, because if we applied anything other than the identity on A we would change ρ_A and non-unitaries on B would not preserve eigenvalues of ρ_B.

Note also that any two *orthonormal* bases are related by a unitary: Let $\{b_x\}_B$ and $\{c_x\}_B$ be two orthonormal bases. We can define a map from one basis two the other as

$$U : \{b_x\}_B \mapsto \{c_x\}_B\,, \qquad \text{where } U = \sum_x |c_x\rangle\langle b_x|$$

We can immediately verify that $UU^\dagger = U^\dagger U = \mathbb{1}$.

c) *For ρ_A as defined above, and any purification $|\Phi\rangle$ of ρ_A on $\mathcal{H}_A \otimes \mathcal{H}_B$, find an orthogonal measurement $\{M_B^x\}_x$ on $\mathcal{H}_B$, such that*

$$\lambda_x = \mathrm{Tr}\left[|\Phi\rangle\langle\Phi|(\mathbb{1}_A \otimes M_B^x)\right] \quad \text{and} \quad \rho_A^x = \frac{\mathrm{Tr}_B\left[|\Phi\rangle\langle\Phi|(\mathbb{1}_A \otimes M_B^x)\right]}{\lambda_x}. \tag{1}$$

In this picture λ_x is the probability of measuring x and ρ_A^x is the state after such a measurement.

Note that all purifications of ρ_A in $\mathcal{H}_A \otimes \mathcal{H}_B$ are equivalent up to a unitary transformation in $\mathcal{H}_B$. In general, purifications in $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_A \otimes \mathcal{H}_{B'}$ are related by isometric maps between the two Hilbert spaces $\mathcal{H}_B$ and $\mathcal{H}_{B'}$. It is thus sufficient to find a POVM for one particular purification and show how the measurement operators can be translated to any other purification possible.

Let us decompose the Hilbert space $\mathcal{H}_B = \mathcal{H}_C \otimes \mathcal{H}_D$ with an orthonormal basis $\{|d_x\rangle_D\}_x$ of $\mathcal{H}_D$. We are further given $\{|\phi^x\rangle_{AC}\}_x$, the purifications of the states $\{\rho_A^x\}_x$. It is now easy to verify that

$$|\phi\rangle = \sum_x \sqrt{\lambda_x} |\phi^x\rangle_{AC} \otimes |d_x\rangle_D$$

is a purification of ρ_A by taking the partial trace over $\mathcal{H}_B$.

The measurement operators $M_B = \mathbb{1}_C \otimes |d_x\rangle\langle d_x|_D$ fulfill the requirements:

$$\begin{aligned}
\mathrm{Tr}_B\big(|\phi\rangle\langle\phi|(\mathbb{1}_A \otimes M_B)\big) &= \mathrm{Tr}_C\left(\mathrm{Tr}_D\left(\sum_{y,z}\sqrt{\lambda_y\lambda_z}(|\phi^y\rangle\langle\phi^z|_{AC}\otimes|d_y\rangle\langle d_z|_D)\cdot(\mathbb{1}_{AC}\otimes|d_x\rangle\langle d_x|_D)\right)\right)\\
&= \mathrm{Tr}_C\left(\sum_{a,y,z}\sqrt{\lambda_y\lambda_z}|\phi^y\rangle\langle\phi^z|_{AC}\otimes\langle d_a|d_y\rangle\langle d_z|d_x\rangle\langle d_x|d_a\rangle_D\right)\\
&= \lambda_x\mathrm{Tr}_C(|\phi^x\rangle\langle\phi^x|_{AC})\\
&= \lambda_x\rho_A^x.
\end{aligned}$$

In the last step we used the fact that $|\phi^x\rangle$ is a purification of ρ_A^x. The second condition, $\lambda_x = \mathrm{Tr}(|\phi\rangle\langle\phi|(\mathbb{1}_A \otimes M_B))$, follows directly since $\mathrm{Tr}\rho_A^x = 1$.

Exercise 5.2 Distinguishing two quantum states

Suppose you know the density operators of two quantum states $\rho, \sigma \in \mathcal{H}_A$. Then you are given one of the states at random—it may either be ρ with probability p, or σ with probability $1-p$. The challenge is to perform a single measurement on your state and then guess which state that is.

a) *What is your best strategy? In which basis do you think you should perform the measurement? Can you express that measurement using a projector P?*

We are looking for a measurement O that maximises our probability of guessing correctly. For each state (say eg. ρ) the probabilities of obtaining any of the possible outcomes $\{y\}_y$ of the observable $O = \sum_y yP_y$ that represents the measurement define a classical probability distribution $\mathrm{Pr}_{O,\rho}(y) = \mathrm{Tr}(P_y\rho)$.

Let $G = \{y : \mathrm{Pr}_{O,\rho}(y) \geq \mathrm{Pr}_{O,\sigma}(y)\}$ be the set of outcomes that are more likely to occur when we measure O on ρ than on σ. Naturally, if we obtain y after measuring our unknown state and obtain we should say it was ρ if $y \in G$ and vice-versa. The probability of guessing correctly is then

$$\begin{aligned}
\mathrm{Pr}_\checkmark &= \mathrm{Pr}(\rho)\cdot\mathrm{Pr}(\text{say “}\rho\text{”}|\rho) + \mathrm{Pr}(\sigma)\cdot\mathrm{Pr}(\text{say “}\sigma\text{”}|\sigma)\\
&= p\cdot\sum_{y\in G}\mathrm{Pr}_{O,\rho}(y) + (1-p)\cdot\sum_{y\in\bar{G}}\mathrm{Pr}_{O,\sigma}(y)\\
&= p\sum_{y\in G}\mathrm{Tr}(P_y\rho) + (1-p)\sum_{y\in\bar{G}}\mathrm{Tr}(P_y\sigma)\\
&= p\mathrm{Tr}\left(\left[\sum_{y\in G}P_y\right]\rho\right) + (1-p)\mathrm{Tr}\left(\left[\sum_{y\in\bar{G}}P_y\right]\sigma\right)\\
&= \mathrm{Tr}\left(pP_G\,\rho + (1-p)P_{\bar{G}}\,\sigma\right),
\end{aligned}$$

where $P_G := \sum_{y\in G}P_y$ and $P_{\bar{G}} := \sum_{y\in\bar{G}}P_y$ are projectors too, with $P_G + P_{\bar{G}} = \mathbb{1}$.

Continuing, we obtain

$$\begin{aligned}
\mathrm{Pr}_\checkmark &= \mathrm{Tr}(pP_G\,\rho + (1-p)P_{\bar{G}}\,\sigma)\\
&= \mathrm{Tr}(pP_G\,\rho + (1-p)[\mathbb{1}-P_G]\,\sigma)\\
&= \mathrm{Tr}(P_G\,[p\rho-(1-p)\sigma]) + (1-p)\mathrm{Tr}(\mathbb{1}\sigma)\\
&= \mathrm{Tr}(P_G\,[p\rho-(1-p)\sigma]) + 1 - p, \qquad {}^{(*)}
\end{aligned}\tag{2}$$

where $^{(*)}$ comes from the fact that σ is a density matrix and therefore $\mathrm{Tr}(\sigma) = 1$.

To maximise this probability, we need to find the optimal set G that maximises $\mathrm{Tr}(P_G\,[p\rho-(1-p)\sigma])$.

First we express G in another way,

$$\begin{aligned}
G &= \{y : \mathrm{Pr}_{O,\rho}(y) \geq \mathrm{Pr}_{O,\sigma}(y)\}\\
&= \{y : \mathrm{Tr}(pP_y\rho) \geq \mathrm{Tr}((1-p)P_y\sigma)\}\\
&= \{y : \mathrm{Tr}(P_y(p\rho-(1-p)\sigma)) \geq 0\}.
\end{aligned}$$

Now we will try a clever choice of G. Let $\{y\}_y$ be the eigenbasis of $p\rho - (1-p)\sigma = \sum_y \lambda_y |y\rangle\langle y|$. Notice that $p\rho - (1-p)\sigma$ is *not* a density matrix — in particular it has trace $2p-1$. If we choose $\{P_y\}_y$ to be the projectors on that basis, $P_y = |y\rangle\langle y|$, we obtain

$$\begin{aligned} G &= \{y : \mathrm{Tr}(P_y(p\rho - (1-p)\sigma)) \geq 0\} \\ &= \left\{ y : \mathrm{Tr}\left(|y\rangle\langle y| \sum_{y'} \lambda_{y'} |y'\rangle\langle y'| \right) \geq 0 \right\} \\ &= \{y : \mathrm{Tr}\left(|y\rangle\langle y| \lambda_y\right) \geq 0\} \\ &= \{y : \lambda_y \geq 0\}. \end{aligned}$$

i.e. G is the set of projectors on states that correspond to non negative eigenvalues of $p\rho - (1-p)\sigma$. In this case, $\mathrm{Tr}(P_G\ [p\rho - (1-p)\sigma])$ is the sum of all positive eigenvalues of $p\rho - (1-p)\sigma$.

This result is promising, but now we have to prove that is is indeed optimal, i.e. that no other choice of projector P could give better results. We can write $p\rho - (1-p)\sigma$ as $R - S$, where $R = \sum_{y\in G} \lambda_y |y\rangle\langle y|$ and $S = \sum_{y\in \bar{G}} -\lambda_y |y\rangle\langle y|$. Both operators R and S are positive and diagonal.

We have that

$$\mathrm{Tr}(P_G\ [p\rho - (1-p)\sigma]) = \sum_{y\in G} \lambda_y = \mathrm{Tr}(R). \tag{3}$$

For any other operator, however,

$$\begin{aligned} \mathrm{Tr}(P\ [p\rho - (1-p)\sigma]) &= \mathrm{Tr}(P\ [R - S]) \\ &= \mathrm{Tr}(P\ R) - \mathrm{Tr}(P\ S) \\ &\leq \mathrm{Tr}(R) - \mathrm{Tr}(P\ S) \qquad {}^{(*)} \\ &\leq \mathrm{Tr}(R), \qquad {}^{(**)} \end{aligned}$$

where $^{(*)}$ stands because projectors can only decrease the trace and $^{(**)}$ because $P\sigma$ is positive.

We have proved that a measurement represented by $O = \sum_y o_y |y\rangle\langle y|$, where $\{|y\rangle\}_y$ is the eigenbasis of $p\rho - (1-p)\sigma$ optimises the probability of guessing correctly which state we were given.

This solution corresponds to the following strategy. We measure our state (ρ or σ) in the eigenbasis of $p\rho - (1-p)\sigma$. If we obtain a state that corresponds to a positive eigenvalue of $p\rho - (1-p)\sigma$ (i.e. $y \in G$) then it is more likely that we have measured ρ. If we get a negative eigenvalue of $p\rho - (1-p)\sigma$ (i.e. $y \in \bar{G}$) we should say the state was σ.

In the particular case where the two density operators share the same eigenbasis, this corresponds to following the classical strategy for distinguishing two probability distributions after measuring the state in their common eigenbasis.

b) *What is the probability of guessing correctly,* $\mathrm{Pr}^p_{\checkmark}(\rho, \sigma)$*? Compare that with the case where the states are evenly distributed,* $\mathrm{Pr}^{0.5}_{\checkmark}(\rho,\sigma) = \frac{1}{2}[1 + \delta(\rho,\sigma)]$*, where* $\delta(\rho,\sigma)$ *is the trace distance between the two quantum states.*

We have solved this in the previous exercise (Eq. 2), and when $p = 0.5$ we get:

$$\frac{1}{2}(\mathrm{Tr}(P_G\ [\rho - \sigma]) + 1) = \frac{1}{2}(\delta(\rho,\sigma) + 1),$$

where we use the definition of the trace distance as $\delta(\rho,\sigma) := \mathrm{Tr}(|\rho - \sigma|)$, which was shown in Eq. 3.

Exercise 5.3 Distance bounds

a) *Given a trace-preserving quantum operation* $\mathcal{E}$ *and two states* ρ *and* σ*, show that*

$$\delta\left(\mathcal{E}(\sigma), \mathcal{E}(\rho)\right) \leq \delta(\sigma, \rho). \tag{4}$$

We use the fact that $\rho - \sigma = R - S$, where R and S are positive operators with orthogonal support. Then we have

$$\begin{aligned}
\delta(\sigma,\rho) &= \frac{1}{2}\mathrm{Tr}(|\rho-\sigma|) \\
&= \frac{1}{2}\left(\mathrm{Tr}(R)+\mathrm{Tr}(S)\right) \\
&= \mathrm{Tr}(R) \qquad {}^{(*)} \\
&= \mathrm{Tr}\left[\mathcal{E}(R)\right] \\
&\geq \max_P \left\{\mathrm{Tr}\left[P\mathcal{E}(R)\right] - \mathrm{Tr}\left[P\mathcal{E}(S)\right]\right\} \qquad {}^{(**)} \\
&= \max_P \mathrm{Tr}\left[P(\mathcal{E}(R-S))\right] \qquad {}^{(***)} \\
&= \delta\left(\mathcal{E}(\sigma),\mathcal{E}(\rho)\right),
\end{aligned}$$

where ${}^{(*)}$ stands because $\mathrm{Tr}(R)=\mathrm{Tr}(S)$, as

$$\mathrm{Tr}(R)-\mathrm{Tr}(S) = \mathrm{Tr}(R-S) = \mathrm{Tr}(|\rho-\sigma|) = |\mathrm{Tr}(\rho)-\mathrm{Tr}(\sigma)| = |1-1| = 0,$$

and the inequality ${}^{(**)}$ follows from $\mathrm{Tr}[P\mathcal{E}(R)] \leq \mathrm{Tr}(\mathcal{E}(R))$ and $\mathrm{Tr}(P\mathcal{E}(S)) \geq 0$ for any projector P, since projectors are positive operators and can only decrease the trace. Finally, linearity of TPMs allows us to perform step ${}^{(***)}$.

b) *Show that any purification of the state $\rho_{AB} = \frac{\mathbb{1}_A}{|\mathcal{H}_A|}\otimes\rho_B$ has the form*

$$|\psi\rangle_{AA'BB'} = |\Psi\rangle_{AA'}\otimes|\psi\rangle_{BB'},$$

where $|\Psi\rangle_{AA'} = |\mathcal{H}_A|^{-\frac{1}{2}}\sum_i |i\rangle_A|i\rangle_{A'}$ is a maximally entangled state, and $|\psi\rangle_{BB'}$ is a purification of ρ_B.

There are several ways of solving this exercise. For instance, let $|\Psi\rangle_{AA'}$ be a purification of ρ_A, and $|\psi\rangle_{BB'}$ a purification of ρ_B,

$$\begin{aligned}
\rho_A &= \frac{1}{|\mathcal{H}_A|}\sum_k |k\rangle\langle k|_A &\quad\Rightarrow\quad |\Psi\rangle_{AA'} &= \frac{1}{\sqrt{|\mathcal{H}_A|}}\sum_k |k\rangle_A|k\rangle_{A'} \\
\rho_B &= \sum_\ell \lambda_\ell\, |\ell\rangle\langle\ell|_B &\quad\Rightarrow\quad |\psi\rangle_{BB'} &= \sum_\ell \sqrt{\lambda_\ell}\,|\ell\rangle_B|\ell\rangle_{B'}.
\end{aligned}$$

Then $|\Psi\rangle_{AA'}\otimes|\psi\rangle_{BB'}$ is a purification of ρ_{AB},

$$\begin{aligned}
\mathrm{Tr}_{A'B'}\Big(|\Psi\rangle\langle\Psi|_{AA'}\otimes|\psi\rangle\langle\psi|_{BB'}\Big) &= \mathrm{Tr}_{A'}\big(|\Psi\rangle\langle\Psi|_{AA'}\big)\otimes\mathrm{Tr}_{B'}\big(|\psi\rangle\langle\psi|_{BB'}\big) \\
&= \rho_A\otimes\rho_B.
\end{aligned}$$

All purifications are equivalent up to a unitary transformation on the purifying system, in this case $\mathcal{H}_{A'}\otimes\mathcal{H}_{B'}$. The unitary operators that express such transformations can be written as

$$U = \sum_{k,\ell} |\phi_{k\ell}\rangle_P\big(\langle k|_{A'}\otimes\langle\ell|_{B'}\big).$$

The states $\{|\phi_{k\ell}\rangle\}_{k,\ell}$ form a basis for $\mathcal{H}_P$. In particular, they have to be orthonormal, $\langle\phi_{k\ell}|\phi_{mn}\rangle = \delta_{km}\delta_{\ell n}$. If we fix the first index we get $\langle\phi_{k\ell}|\phi_{kn}\rangle = \delta_{km}$, and conclude that the states have to have the form $|\phi_{k\ell}\rangle = |\phi_k\rangle\otimes|\phi_\ell\rangle$.

An alternative solution uses a Schmidt decomposition of the purification to prove that the purification of a product state is a product of pure states.

c) *Show that $1 - F(\rho,\sigma) \leq \delta(\rho,\sigma) \leq \sqrt{1-F(\rho,\sigma)^2}$.*

i) First we show that $1 - F(\rho,\sigma) \leq \delta(\rho,\sigma)$.
Let $\{E_m\}$ be a POVM such that

$$F(\rho,\sigma) = \sum_m \sqrt{p_m q_m}, \tag{5}$$

where $p_m = \mathrm{Tr}(\rho E_m)$ and $q_m = \mathrm{Tr}(\sigma E_m)$. Observe that

$$\sum_m (\sqrt{p_m} - \sqrt{q_m})^2 = \sum_m p_m + \sum_m q_m - 2F(\rho,\sigma) = 2(1 - F(\rho,\sigma)). \tag{6}$$

Also note that $|\sqrt{p_m} - \sqrt{q_m}| \leq |\sqrt{p_m} + \sqrt{q_m}|$ and so

$$\sum_m (\sqrt{p_m} - \sqrt{q_m})^2 \leq \sum_m |\sqrt{p_m} - \sqrt{q_m}||\sqrt{p_m} + \sqrt{q_m}| = \sum_m |p_m - q_m| \tag{7}$$

$$= 2\delta(p_m, q_m) \leq 2\delta(\rho,\sigma), \tag{8}$$

where we use part (a) in the last line. Comparing Eqs. 6 and 8, we get the result.

ii) Now we show that $\delta(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}$.
First we prove that $\delta(|a\rangle, |b\rangle) \leq \sqrt{1 - F(|a\rangle, |b\rangle)^2}$, where $|a\rangle$ and $|b\rangle$ are pure states, and it is implicit that $\delta(|a\rangle, |b\rangle) := \delta(|a\rangle\langle a|, |b\rangle\langle b|)$ (and similarly for the fidelity).
We may fix a basis with which to represent the states $|a\rangle$ and $|b\rangle$, namely $|a\rangle = |0\rangle$ and $|b\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$. Note that $F(|a\rangle, |b\rangle) = |\langle a|b\rangle| = |\cos\theta|$. Also the trace distance is:

$$\delta(|a\rangle, |b\rangle) = \frac{1}{2}\mathrm{Tr}\left|\begin{array}{cc} 1 - \cos^2\theta & -\cos\theta\sin\theta \\ -\cos\theta\sin\theta & -\sin^2\theta \end{array}\right| = |\sin\theta| = \sqrt{1 - F(|a\rangle, |b\rangle)^2}. \tag{9}$$

For mixed states ρ and σ we can pick purifications ($|\psi\rangle$ and $|\phi\rangle$, respectively) of these states such that $F(\rho,\sigma) = |\langle\psi|\phi\rangle| = F(|\psi\rangle, |\phi\rangle)$ (using Uhlmann's theorem). Using part (a) with the partial trace as the completely positive map, we get:

$$D(\rho,\sigma) \leq D(|\psi\rangle, |\phi\rangle) = \sqrt{1 - F(|\psi\rangle, |\phi\rangle)^2} = \sqrt{1 - F(\rho,\sigma)^2} \tag{10}$$

d) Consider a state that is ε-distant from ρ_{AB} according to the trace distance, i.e.

$$\delta\left(\sigma_{AB}, \frac{\mathbb{1}_A}{|\mathcal{H}_A|} \otimes \rho_B\right) \leq \varepsilon.$$

Find an upper bound for

$$\delta\left(\tau_{AA'}, |\Psi\rangle_{AA'}\langle\Psi|_{AA'}\right),$$

where $|\phi\rangle_{AA'BB'}$ is a purification of σ_{AB} and $\tau_{AA'} = Tr_{BB'}(|\phi\rangle_{AA'BB'}\langle\phi|_{AA'BB'})$.

We know that

$$1 - F(\rho,\sigma) \leq \delta(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}.$$

from which follows

$$\sqrt{1 - F(\rho,\sigma)^2} \leq \sqrt{2\delta(\rho,\sigma) - \delta(\rho,\sigma)^2}.$$

We also know that fidelity can be preserved under purifications (theorem 4.3.8), leaving us with

$$\begin{aligned}
\delta\left(\tau_{AA'}, |\Psi\rangle_{AA'}\langle\Psi|_{AA'}\right) &\leq \sqrt{1 - F\left(|\phi\rangle_{AA'BB'}, |\Psi\rangle_{AA'} \otimes |\psi\rangle_{BB'}\right)^2} \\
&= \sqrt{1 - F(\sigma_{AB}, \rho_{AB})^2} \\
&\leq \sqrt{2\delta(\sigma_{AB}, \rho_{AB}) - \delta(\sigma_{AB}, \rho_{AB})^2} \\
&\leq \sqrt{2\varepsilon - \epsilon^2},
\end{aligned}$$

where the last inequality stands because the function $\sqrt{2x - x^2}$ is monotonically increasing for $x \in [0,1]$.