Exercise 1. *Trace distance and fidelity: Fuchs-van de Graaf inequalities*

Trace distance $\delta(\rho,\sigma)$ and fidelity $F(\rho,\sigma)$ of two quantum states $\rho,\sigma \in \mathcal{S}(\mathcal{H})$ are closely related. In some sense they can be considered equivalent measures of distance, as we will explore in this exercise. Before we start, let us repeat the quite different definitions of the two objects, δ and F.

$$\begin{aligned}\delta(\rho,\sigma) &:= \operatorname{tr}|\rho-\sigma| \equiv \operatorname{tr}\left[\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right] \\ &= \max_{P\ proj.} \operatorname{tr}\left[P(\rho-\sigma)\right] \qquad \textit{(alternative def.)} \\ F(\rho,\sigma) &:= \operatorname{tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right] \\ &= \max_{|\Psi\rangle,|\Phi\rangle\ purif.} |\langle\Psi|\Phi\rangle| \qquad \textit{(Uhlmann)}\end{aligned}$$

(a) Show that in the case of pure states $\rho = |\psi\rangle\langle\psi|$, $\sigma = |\phi\rangle\langle\phi|$ trace distance and fidelity fulfil

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

(b) Use that trace distance can only decrease under quantum operations (see last sheet) to show that for general $\rho,\sigma \in \mathcal{S}(\mathcal{H})$

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

There is yet another very useful characterization of the fidelity as an optimization over all possible POVM measurements. For two (classical) probability distributions $\{p_m\}_m$ and $\{q_m\}_m$ define the classical *fidelity to be*

$$F(\{p_m\},\{q_m\}) := \sum_m \sqrt{p_m q_m}\,.$$

The quantum *fidelity can then be written as*

$$F(\rho,\sigma) = \min_{\{E_m\}\ POVM} F(\{p_m\},\{q_m\}), \tag{3}$$

where $p_m := \operatorname{tr}[\rho\, E_m]$ and $q_m := \operatorname{tr}[\sigma\, E_m]$. Likewise, using the same notation, the quantum *trace distance can be written as*

$$\delta(\rho,\sigma) = \max_{\{E_m\}\ POVM} \delta(\{p_m\},\{q_m\}), \tag{4}$$

where $\delta(\{p_m\},\{q_m\})$ is the classical *trace distance of the respective probability distributions.*

(c) Use this way of writing $F(\rho,\sigma)$ and $\delta(\rho,\sigma)$ to prove that for any two states $\rho,\sigma \in \mathcal{S}(\mathcal{H})$

$$1 - F(\rho,\sigma) \le \delta(\rho,\sigma)\,. \tag{5}$$

In total this shows 'equivalence' of δ and F in terms of the inequalities

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

Solution.

(a) To prove this fact we only need to work in the 2-dimensional subspace of $\mathcal{H}$ spanned by $|\psi\rangle$ and $|\phi\rangle$. As a basis of this space we take $\{|\psi\rangle, |\psi^\perp\rangle\}$, where $|\psi^\perp\rangle$ is the normalized vector orthogonal to $|\psi\rangle$ that allows us to write

$$|\phi\rangle = \cos\theta|\psi\rangle + \sin\theta|\psi^\perp\rangle \tag{S.1}$$

for some $\theta \in \mathbb{R}$. We find that

$$\begin{aligned} F(\rho,\sigma) &= |\langle\psi|\phi\rangle| = |\cos\theta|\,, \\ \delta(\rho,\sigma) &= \frac{1}{2}\operatorname{tr}\left|\begin{pmatrix} 1-\cos^2\theta & -\cos\theta\sin\theta \\ -\cos\theta\sin\theta & -\sin^2\theta \end{pmatrix}\right| = |\sin\theta|\,. \end{aligned} \tag{S.2}$$

Thus we have $\sqrt{1-F(\rho,\sigma)^2} = \delta(\rho,\sigma)$ in this case.

(b) Let now $\rho,\sigma \in \mathcal{S}(\mathcal{H})$ be two arbitrary quantum states and let $|\Psi\rangle$ and $|\Phi\rangle$ be purifications s.t. $F(\rho,\sigma) = |\langle\Psi|\Phi\rangle| = F(|\Psi\rangle,|\Phi\rangle)$. The partial trace over the purifying system is a quantum operation (cptp map). Thus, together with (a),

$$\sqrt{1-F(\rho,\sigma)^2} = \sqrt{1-F(|\Psi\rangle,|\Phi\rangle)^2} = \delta(|\Psi\rangle,|\Phi\rangle) \geq \delta(\rho,\sigma)\,. \tag{S.3}$$

(c) We make use of the definition of F as a minimization over POVMs. Let $\{E_m\}_m$ be a POVM with $p_m := \operatorname{tr}[\rho\, E_m]$ and $q_m := \operatorname{tr}[\sigma\, E_m]$ that minimizes $F(\{p_m\},\{q_m\})$. Hence,

$$F(\rho,\sigma) = \sum_m \sqrt{p_m q_m}. \tag{S.4}$$

Consider

$$\sum_m (\sqrt{p_m} - \sqrt{q_m})^2 = \sum_m p_m + \sum_m q_m - 2\,F(\rho,\sigma) = 2(1-F(\rho,\sigma))\,. \tag{S.5}$$

On the other hand we have $|\sqrt{p_m} - \sqrt{q_m}| \leq |\sqrt{p_m} + \sqrt{q_m}|$ and thus

$$\begin{aligned} \sum_m (\sqrt{p_m} - \sqrt{q_m})^2 &\leq \sum_m |\sqrt{p_m} - \sqrt{q_m}|\,|\sqrt{p_m} + \sqrt{q_m}| = \sum_m |p_m - q_m| \\ &= 2\,\delta(\{p_m\},\{q_m\}) \leq 2\,\delta(\rho,\sigma)\,, \end{aligned} \tag{S.6}$$

where the last inequality is due to (4). In total this reads

$$1 - F(\rho,\sigma) \leq \delta(\rho,\sigma)\,. \tag{S.7}$$

Exercise 2. *Properties of von Neumann entropy*

The von Neumann entropy *of a density operator $\rho \in \mathcal{S}(\mathcal{H}_A)$ is defined as $H(A)_\rho := -\operatorname{tr}(\rho\log\rho)$. Given a composite system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ we write $H(AB)_\rho$ to denote the von Neumann entropy of the reduced state of a subsystem, $\rho_{AB} = \operatorname{tr}_C(\rho_{ABC})$. When the state ρ is obvious from the context we can drop the index.*
The conditional *von Neumann entropy may be defined as $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$. In the Alice-and-Bob picture this quantifies the uncertainty that Bob, who holds part of a quantum state, ρ_B, still has about Alice's state.*
The strong sub-additivity *property of the von Neumann entropy shows up a lot. It applies to a tripartite composite system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$,*

$$H(A|BC)_\rho \leq H(A|B)_\rho. \tag{6}$$

(a) Prove the following general properties of the von Neumann entropy.

(i) If ρ_{AB} is pure, then $H(A)_\rho = H(B)_\rho$.

(ii) If ρ_{ABC} is pure, then $H(A|C)_\rho = -H(A|B)_\rho$.

(iii) If two systems are independent, $\rho_{AB} = \rho_A \otimes \rho_B$, then $H(AB)_\rho = H(A)_{\rho_A} + H(B)_{\rho_B}$.

(b) Consider a bipartite state that is classical on subsystem Z: $\rho_{ZA} = \sum_z p_z |z\rangle\langle z|_Z \otimes \rho_A^z$ for some orthogonal basis $\{|z\rangle_Z\}_z$ of $\mathcal{H}_Z$ and a set of states $\{\rho_A^z\}_z \subset \mathcal{S}(\mathcal{H}_A)$. Show that:

(i) The conditional entropy of the quantum part, A, given the classical information Z is

$$H(A|Z)_\rho = \sum_z p_z \, H(A|Z = z), \tag{7}$$

where $H(A|Z = z) = H(A)_{\rho_A^z}$.

(ii) The entropy of A is concave,

$$H(A)_\rho \geq \sum_z p_z \, H(A|Z = z). \tag{8}$$

(iii) The entropy of a classical probability distribution $\{p_z\}_z$ cannot be negative, even if one has access to extra quantum information, A,

$$H(Z|A)_\rho \geq 0. \tag{9}$$

Remark: *Eq (9) holds in general only for classical Z. Bell states are immediate counterexamples in the fully quantum case.*

Solution.

(a) (i) This becomes clear when you apply the Schmidt decomposition to the pure state ρ_{AB}: the reduced states of the two subsystems A and B have the same eigenvalues. If $\{\lambda_i\}_i$ are the eigenvalues of ρ_A then the von Neumann entropy of A can be written as

$$H(A)_\rho = -\sum_i \lambda_i \log \lambda_i \,. \tag{S.8}$$

Since they have the same eigenvalues, the reduced states have the same entropy.

(ii) Using (a) (i) as well as the definition of conditional entropy we find

$$H(A|C)_\rho = H(AC)_\rho - H(C)_\rho = H(B)_\rho - H(AB)_\rho = -H(A|B)_\rho \,. \tag{S.9}$$

We used twice that ρ_{ABC} is pure.

(iii) We denote by $\{\lambda_i\}_i$ and $\{\gamma_j\}_j$ the eigenvalues of ρ_A and ρ_B, respectively. Hence $\{\lambda_i \gamma_j\}_{i,j}$ are the eigenvalues of ρ_{AB} and we can write:

$$\begin{aligned} H(AB)_\rho &= -\sum_{i,j} \lambda_i \gamma_j \log(\lambda_i \gamma_j) \\ &= -\underbrace{\Big(\sum_i \lambda_i\Big)}_{=1} \cdot \Big(\sum_j \gamma_j \log \gamma_j\Big) - \underbrace{\Big(\sum_j \gamma_j\Big)}_{=1} \cdot \Big(\sum_i \lambda_i \log \lambda_i\Big) \\ &= H(A)_{\rho_A} + H(B)_{\rho_B}. \end{aligned} \tag{S.10}$$

(b) (i) First, note that the eigenvalues of $\sum_z p_z |z\rangle\langle z| \otimes \rho_A^z$ are given by $\{p_z \lambda_k^z\}_{z,k}$, where $\{\lambda_k^z\}_k$ are the eigenvalues of $\rho_A^z \equiv \rho_{A|Z=z}$. We may now write:

$$\begin{aligned} H(AZ)_\rho &= -\sum_{z,k} p_z \lambda_k^z \log(p_z \lambda_k^z) \\ &= -\sum_z p_z \underbrace{\Big(\sum_k \lambda_k^z\Big)}_{=1} \log p_z - \sum_z p_z \Big(\sum_k \lambda_k^z \log \lambda_k^z\Big) \\ &= H(Z) + \sum_z p_z \, H(A|Z=z), \end{aligned}$$

and

$$H(A|Z)_\rho = H(AZ)_\rho - H(Z)_\rho = \sum_z p_z \, H(A|Z=z), \tag{S.11}$$

(ii) First note that from strong sub-additivity follows sub-additivity, $H(AC) \leq H(A) + H(C)$, if $\mathcal{H}_B$ is empty. Applying this to a system classical in $\mathcal{H}_Z$, we get

$$H(AZ) = H(Z) + \sum_z p_z \; H(A|Z=z) \leq H(A) + H(Z) \tag{S.12}$$

from which the inequality follows immediately.

(iii) First note that from strong sub-additivity follows sub-additivity, $H(AC) \leq H(A) + H(C)$, if $\mathcal{H}_B$ is empty. Applying this to a system classical in $\mathcal{H}_Z$, we get

$$H(AZ) = H(Z) + \sum_z p_z \; H(A|Z=z) \leq H(A) + H(Z)\,, \tag{S.13}$$

from which the inequality follows immediately.

(iv) Let us introduce a copy of the classical subsystem Z, Y, as follows:

$$\rho_{AZY} = \sum_z p_z |z\rangle\langle z|_Z \otimes |z\rangle\langle z|_Y \otimes \rho_A^z. \tag{S.14}$$

Note that, for this state, $H(AZ) = H(AY) = H(AZY)$.
We may now appply the strong sub-additivity,

$$\begin{aligned} & H(AZY) + H(A) \leq H(AZ) + \underbrace{H(AY)}_{=H(AZY)} \\ \Leftrightarrow \;\; & 0 \leq H(AZ) - H(A) \\ \Leftrightarrow \;\; & 0 \leq H(Z|A)\,. \end{aligned} \tag{S.15}$$

Exercise 3. ***Upper bound on von Neumann entropy***

(a) Given a state $\rho \in \mathcal{S}(\mathcal{H}_A)$, show that

$$H(A)_\rho \leq \log |\mathcal{H}_A|\,. \tag{10}$$

Hints: *Consider the state $\bar{\rho} = \int U \rho U^\dagger dU$, where the integral is over all unitaries $U \in \mathcal{U}(\mathcal{H}_A)$ and dU is the Haar measure. Find $\bar{\rho}$ and use concavity, (8), to show (10). The Haar measure satisfies $d(UV) = d(VU) = dU$, where $V \in \mathcal{U}(\mathcal{H}_A)$ is any fixed unitary.*

(b) For $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, show that the conditional entropy satisfies

$$-\log |\mathcal{H}_A| \leq H(A|B)_\rho \leq \log |\mathcal{H}_A|\,. \tag{11}$$

Solution.

(a) We use the properties of the Haar measure to verify that $\bar{\rho}$ commutes with all unitaries V on $\mathcal{H}$:

$$V\bar{\rho}V^\dagger = \int (VU)\rho(VU)^\dagger \, dU = \int \tilde{U}\rho\tilde{U}^\dagger \, d(V^\dagger\tilde{U}) = \int \tilde{U}\rho\tilde{U}^\dagger \, d\tilde{U} = \bar{\rho}. \tag{S.16}$$

The only density operator on $\mathcal{H}$ that has this property is the completely mixed state: suppose that $\bar{\rho}$ had distinct eigenvalues $\{\lambda_i\}$, and corresponding eigenvectors $\{|i\rangle\}$. Take V to be a unitary transformation that permutes the eigenvectors, for instance $V = |1\rangle\langle 2| + |2\rangle\langle 1|$. Then we would have that $V\bar{\rho}V^\dagger|1\rangle = \lambda_2|1\rangle$, while $\bar{\rho}|1\rangle = \lambda_1|1\rangle$, so $\rho \neq V\rho V^\dagger$. Since all the eigenvalues of $\bar{\rho}$ must be the same, and must be positive and sum up to one, we have that $\bar{\rho} = \mathbb{1}/|\mathcal{H}|$

The concavity property of the von Neumann entropy (8) naturally extends to integrals and we get

$$\begin{aligned} \log|\mathcal{H}| = H\left(\frac{\mathbb{1}}{|\mathcal{H}|}\right) = H(\bar{\rho}) &\geq \int H(U\rho U^\dagger) \, dU \\ &\overset{(*)}{=} \int H(\rho) \, dU = H(\rho)\int dU = H(\rho), \end{aligned} \tag{S.17}$$

where $^{(*)}$ stands because the entropy is independent of the basis.

(b) We first use (a) to show $H(A|B)_\rho \leq \log|\mathcal{H}_A|$: due to (strong) sub-additivity we have

$$H(A|B)_\rho \leq H(A)_\rho \leq \log|\mathcal{H}_A|\,. \tag{S.18}$$

For the other inequality we make use of exercise 2 (a) (ii) and the above. Let ρ_{ABC} be a purification of ρ_{AB}. Then

$$H(A|B)_\rho = -H(A|C)_\rho \geq -H(A)_\rho \leq -\log|\mathcal{H}_A|\,. \tag{S.19}$$