PHYS 7895: Quantum Information Theory	Fall 2015

Lecture 15 — October 16, 2015

Prof. Mark M. Wilde — *Scribe: Mark M. Wilde*

1 Overview

In the previous lecture, we introduced the trace distance and discussed some of its mathematical properties. We also showed how it has an operational interpretation in the context of quantum hypothesis tesing.

In this lecture, we continue developing the trace distance in more detail and we eventually turn to the fidelity. We begin by recalling the following lemma:

Lemma 1. *The normalized trace distance* $\frac{1}{2}\left\|\rho-\sigma\right\|_1$ *between quantum states* $\rho,\sigma\in\mathcal{D}(\mathcal{H})$ *is equal to the largest probability difference that two states* ρ *and* σ *could give to the same measurement outcome* Λ*:*

$$\frac{1}{2}\left\|\rho-\sigma\right\|_1=\max_{0\leq\Lambda\leq I}\operatorname{Tr}\left\{\Lambda\left(\rho-\sigma\right)\right\}. \tag{1}$$

The above maximization is with respect to all positive semi-definite operators $\Lambda\in\mathcal{L}(\mathcal{H})$ *that have their eigenvalues bounded from above by one.*

1.1 Trace Distance Lemmas

We present several useful corollaries of Lemma 1 and their corresponding proofs. These corollaries include the triangle inequality, measurement on approximate states, and monotonicity of trace distance. Each of these corollaries finds application in many proofs in quantum Shannon theory.

Lemma 2 (Triangle Inequality)**.** *The trace distance obeys a triangle inequality. For any three quantum states* ρ, σ, $\tau\in\mathcal{D}(\mathcal{H})$*, the following inequality holds:*

$$\left\|\rho-\sigma\right\|_1\leq\left\|\rho-\tau\right\|_1+\left\|\tau-\sigma\right\|_1. \tag{2}$$

Proof. Pick Π as the maximizing operator for $\left\|\rho-\sigma\right\|_1$ (according to Lemma 1) so that

$$\begin{aligned}\left\|\rho-\sigma\right\|_1&=2\cdot\operatorname{Tr}\left\{\Pi\left(\rho-\sigma\right)\right\} &(3)\\ &=2\cdot\operatorname{Tr}\left\{\Pi\left(\rho-\tau\right)\right\}+2\cdot\operatorname{Tr}\left\{\Pi\left(\tau-\sigma\right)\right\} &(4)\\ &\leq\left\|\rho-\tau\right\|_1+\left\|\tau-\sigma\right\|_1. &(5)\end{aligned}$$

The last inequality follows because the operator Π maximizing $\left\|\rho-\sigma\right\|_1$ in general is not the same operator that maximizes both $\left\|\rho-\tau\right\|_1$ and $\left\|\tau-\sigma\right\|_1$. □

Corollary 3 (Measurement on Approximately Close States)**.** *Suppose we have two quantum states* $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ *and an operator* $\Pi \in \mathcal{L}(\mathcal{H})$ *such that* $0 \leq \Pi \leq I$*. Then*

$$\operatorname{Tr}\{\Pi\rho\} \geq \operatorname{Tr}\{\Pi\sigma\} - \frac{1}{2}\|\rho - \sigma\|_1 \tag{6}$$

$$\geq \operatorname{Tr}\{\Pi\sigma\} - \|\rho - \sigma\|_1 . \tag{7}$$

Proof. Consider the following arguments:

$$\frac{1}{2}\|\rho - \sigma\|_1 = \max_{0 \leq \Lambda \leq I} \{\operatorname{Tr}\{\Lambda(\sigma - \rho)\}\} \tag{8}$$

$$\geq \operatorname{Tr}\{\Pi(\sigma - \rho)\} \tag{9}$$

$$= \operatorname{Tr}\{\Pi\sigma\} - \operatorname{Tr}\{\Pi\rho\} . \tag{10}$$

The first equality follows from Lemma 1. The first inequality follows because Λ is the maximizing operator and can only lead to a probability difference greater than that for another operator Π such that $0 \leq \Pi \leq I$. □

The most common way that we employ Corollary 3 in quantum Shannon theory is in the following scenario. Suppose that a measurement with operator Π succeeds with high probability on a quantum state σ:

$$\operatorname{Tr}\{\Pi\sigma\} \geq 1 - \varepsilon, \tag{11}$$

where ε is some small positive number. Suppose further that another quantum state ρ is ε-close in trace distance to σ:

$$\|\rho - \sigma\|_1 \leq \varepsilon. \tag{12}$$

Then Corollary 3 gives the intuitive result that the measurement succeeds with high probability on the state ρ that is close to σ:

$$\operatorname{Tr}\{\Pi\rho\} \geq 1 - 2\varepsilon, \tag{13}$$

by plugging (11) and (12) into (7).

We next turn to the monotonicity of trace distance under the discarding of a system. The interpretation of this corollary is that discarding of a system does not increase distinguishability of two quantum states. That is, a global measurement on the larger system might be able to distinguish the two states better than a local measurement on an individual subsystem could. In fact, the proof of monotonicity follows this intuition exactly, and Figure 1 depicts the intuition behind it.

Corollary 4 (Monotonicity)**.** *Let* $\rho_{AB}, \sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$*. The trace distance is monotone under discarding of subsystems:*

$$\|\rho_A - \sigma_A\|_1 \leq \|\rho_{AB} - \sigma_{AB}\|_1 . \tag{14}$$

Proof. Consider that

$$\|\rho_A - \sigma_A\|_1 = 2 \cdot \operatorname{Tr}\{\Lambda_A(\rho_A - \sigma_A)\} , \tag{15}$$

for some positive semi-definite operator $\Lambda_A \leq I_A$. Then

$$2 \cdot \operatorname{Tr}\{\Lambda_A(\rho_A - \sigma_A)\} = 2 \cdot \operatorname{Tr}\{(\Lambda_A \otimes I_B)(\rho_{AB} - \sigma_{AB})\} \tag{16}$$

$$\leq 2 \cdot \max_{0 \leq \Lambda_{AB} \leq I} \operatorname{Tr}\{\Lambda_{AB}(\rho_{AB} - \sigma_{AB})\} \tag{17}$$

$$= \|\rho_{AB} - \sigma_{AB}\|_1 . \tag{18}$$

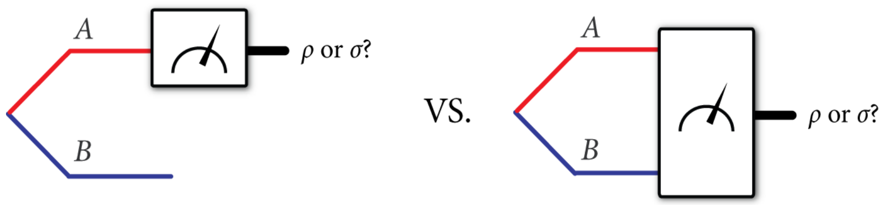

Figure 1: The task in this figure is for Bob to distinguish the state ρ_{AB} from the state σ_{AB} with a binary-valued measurement. Bob could perform an optimal measurement on system A alone if he does not have access to system B. If he has access to system B as well, then he can perform an optimal joint measurement on systems A and B. We would expect that he can distinguish the states more reliably if he performs a joint measurement because there could be more information about the state available in the other system B. Since the trace distance is a measure of distinguishability, we would expect it to obey the following inequality: $\|\rho_A - \sigma_A\|_1 \leq \|\rho_{AB} - \sigma_{AB}\|_1$ (the states are less distinguishable if fewer systems are available to be part of the distinguishability test).

The first equality follows because local predictions of the quantum theory should coincide with its global predictions. The inequality follows because the local operator Λ_A never gives a higher probability difference than a maximization over all global operators. The last equality follows from the characterization of the trace distance in Lemma 1. □

Exercise 5 (Monotonicity of Trace Distance)**.** *Let $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A)$ and $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a quantum channel. Show that the trace distance is monotone under the action of the channel $\mathcal{N}$:*

$$\|\mathcal{N}(\rho) - \mathcal{N}(\sigma)\|_1 \leq \|\rho - \sigma\|_1 . \tag{19}$$

(Hint: Use the result of Corollary 4 and the fact that the trace distance is invariant with respect to isometries.)

The result of the previous exercise deserves an interpretation. It states that a quantum channel $\mathcal{N}$ makes two quantum states ρ and σ less distinguishable from each other. That is, a noisy channel tends to "blur" two states to make them appear as if they are more similar to each other than they are before the quantum channel acts.

Exercise 6. *Prove that a measurement achieves the trace distance, in the following sense:*

$$\|\rho - \sigma\|_1 = \max_{\{\Lambda_x\}} \sum_x |\text{Tr}\{\Lambda_x \rho\} - \text{Tr}\{\Lambda_x \sigma\}| , \tag{20}$$

where $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ and the optimization is with respect to all POVMs $\{\Lambda_x\}$. Hint: Use the result of Exercise 5 to show the following bound for any choice of POVM:

$$\|\rho - \sigma\|_1 \geq \sum_x |\text{Tr}\{\Lambda_x \rho\} - \text{Tr}\{\Lambda_x \sigma\}| . \tag{21}$$

Next, use the developments in the proof of Lemma 1 to construct an optimal measurement that saturates this bound. (Further hint: Consider the measurement $\{\Pi_P, \Pi_Q\}$.)

2 Fidelity

2.1 Pure-State Fidelity

An alternate measure of the closeness of two quantum states is the *fidelity*. We introduce its most simple form first. Suppose that we input a particular pure state $|\psi\rangle$ to a quantum information-processing protocol. Ideally, we may want the protocol to output the same state that is input, but suppose that it instead outputs a pure state $|\phi\rangle$. The pure-state fidelity $F(\psi, \phi)$ is a measure of how close the output state is to the input state.

Definition 7 (Pure-State Fidelity)**.** *Let $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ be pure states. The pure-state fidelity is the squared overlap of the states $|\psi\rangle$ and $|\phi\rangle$:*

$$F(\psi, \phi) \equiv |\langle\psi|\phi\rangle|^2 . \tag{22}$$

The pure-state fidelity has the operational interpretation as the probability that the output state $|\phi\rangle$ would pass a test for being the same as the input state $|\psi\rangle$, conducted by someone who knows the input state (see Exercise 10).

The pure-state fidelity is symmetric $F(\psi, \phi) = F(\phi, \psi)$, and it obeys the following bounds:

$$0 \leq F(\psi, \phi) \leq 1. \tag{23}$$

It is equal to one if and only if the two states are the same, and it is equal to zero if and only if the two states are orthogonal to each other. The fidelity measure is *not* a distance measure in the strict mathematical sense because it is equal to one when two states are equal, whereas a distance measure should be equal to zero when two states are equal.

Exercise 8. *Suppose that two pure quantum states $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ are as follows:*

$$|\psi\rangle \equiv \sum_x \sqrt{p(x)}|x\rangle, \qquad |\phi\rangle \equiv \sum_x \sqrt{q(x)}|x\rangle, \tag{24}$$

where $\{|x\rangle\}$ is some orthonormal basis for $\mathcal{H}$. Show that the fidelity $F(\psi, \phi)$ between these two states is equivalent to the Bhattacharyya distance between the distributions $p(x)$ and $q(x)$:

$$F(\psi, \phi) = \left[\sum_x \sqrt{p(x)q(x)}\right]^2 . \tag{25}$$

2.2 Expected Fidelity

Now let us suppose that the output of a given protocol is not a pure state, but it is rather a mixed state with density operator ρ. In general, a quantum information-processing protocol could be noisy and map the pure input state $|\psi\rangle$ to a mixed state. We would like a way to compare these two states.

Definition 9 (Expected Fidelity)**.** *The expected fidelity $F(\psi, \rho)$ between a pure state $|\psi\rangle \in \mathcal{H}$ and a mixed state $\rho \in \mathcal{D}(\mathcal{H})$ is*

$$F(\psi, \rho) \equiv \langle\psi|\rho|\psi\rangle. \tag{26}$$

We now justify the above definition of fidelity. Let us decompose ρ according to a spectral decomposition $\rho = \sum_x p_X(x)|\phi_x\rangle\langle\phi_x|$. Recall that we can think of this output density operator as arising from the ensemble $\{p_X(x), |\phi_x\rangle\}$. We generalize the pure-state fidelity from the previous paragraph by defining it as the expected pure-state fidelity, where the expectation is with respect to states in the ensemble:

$$F(\psi, \rho) \equiv \mathbb{E}_X \left[|\langle\psi|\phi_X\rangle|^2 \right] \tag{27}$$

$$= \sum_x p_X(x) \, |\langle\psi|\phi_x\rangle|^2 \tag{28}$$

$$= \sum_x p_X(x) \, \langle\psi|\phi_x\rangle \, \langle\phi_x|\psi\rangle \tag{29}$$

$$= \langle\psi| \left(\sum_x p_X(x) \, |\phi_x\rangle \, \langle\phi_x| \right) |\psi\rangle \tag{30}$$

$$= \langle\psi|\rho|\psi\rangle. \tag{31}$$

The compact formula $F(\psi, \rho) = \langle\psi|\rho|\psi\rangle$ is a good way to characterize the fidelity when the input state is pure and the output state is mixed. We can see that the above fidelity measure is a generalization of the pure-state fidelity in (22). It obeys the same bounds:

$$0 \leq F(\psi, \rho) \leq 1, \tag{32}$$

being equal to one if and only if the state ρ is equal to $|\psi\rangle\langle\psi|$ and equal to zero if and only if the support of ρ is orthogonal to $|\psi\rangle\langle\psi|$.

Exercise 10. *Given a state $\sigma \in \mathcal{D}(\mathcal{H})$, we would like to see if it would pass a test for being close to a pure state $|\varphi\rangle \in \mathcal{H}$. We can measure the POVM $\{|\varphi\rangle\langle\varphi|, I - |\varphi\rangle\langle\varphi|\}$ with result φ corresponding to a "pass" and the result $I - \varphi$ corresponding to a "fail." Show that the fidelity is then equal to* $\Pr\{$*"pass"*$\}$.

Exercise 11. *Using the result of Corollary 3, show that the following inequality holds for a pure state $|\phi\rangle \in \mathcal{H}$ and mixed states $\rho, \sigma \in \mathcal{D}(\mathcal{H})$:*

$$F(\phi, \rho) \leq F(\phi, \sigma) + \tfrac{1}{2} \left\| \rho - \sigma \right\|_1 . \tag{33}$$

2.3 Uhlmann Fidelity

What is the most general form of the fidelity when both quantum states are mixed? We can borrow the above idea of the pure-state fidelity that exploits the overlap between two pure states. Suppose that we would like to determine the fidelity between two mixed states ρ_A and σ_A that represent different states of some quantum system A. Let $|\phi^\rho\rangle_{RA}$ and $|\phi^\sigma\rangle_{RA}$ denote particular respective purifications of the mixed states to some reference system R. We can define the Uhlmann fidelity $F(\rho_A, \sigma_A)$ between two mixed states ρ_A and σ_A as the maximum overlap between their respective purifications, where the maximization is with respect to all purifications $|\phi^\rho\rangle_{RA}$ and $|\phi^\sigma\rangle_{RA}$ of the respective states ρ_A and σ_A:

$$F(\rho_A, \sigma_A) \equiv \max_{|\phi^\rho\rangle_{RA}, \; |\phi^\sigma\rangle_{RA}} |\langle\phi^\rho|\phi^\sigma\rangle_{RA}|^2 . \tag{34}$$

We can express the fidelity as a maximization over unitaries instead (recall the result of Theorem **??** that all purifications are equivalent up to unitaries on the reference system):

$$F(\rho_A,\sigma_A) = \max_{U^\rho,U^\sigma} \left| \langle\phi^\rho|_{RA} \left(\left(U_R^\rho\right)^\dagger \otimes I_A \right) \left(U_R^\sigma \otimes I_A\right) |\phi^\sigma\rangle_{RA} \right|^2 \tag{35}$$

$$= \max_{U^\rho,U^\sigma} \left| \langle\phi^\rho|_{RA} \left(U_R^\rho\right)^\dagger U_R^\sigma \otimes I_A |\phi^\sigma\rangle_{RA} \right|^2 . \tag{36}$$

It is unnecessary to maximize over two sets of unitaries because the product $\left(U_R^\rho\right)^\dagger U_R^\sigma$ represents only a single unitary. The final expression for the fidelity between two mixed states is then defined as the Uhlmann fidelity.

Definition 12 (Uhlmann Fidelity)**.** *The Uhlmann fidelity $F(\rho_A,\sigma_A)$ between two mixed states ρ_A and σ_A is the maximum overlap between their respective purifications, where the maximization is with respect to all unitaries U acting on the purification system R:*

$$F(\rho_A,\sigma_A) = \max_U \left|\langle\phi^\rho|_{RA} U_R \otimes I_A |\phi^\sigma\rangle_{RA}\right|^2 . \tag{37}$$

We will find that this notion of fidelity generalizes both the pure-state fidelity in (22) and the expected fidelity in (31). This holds because the following formula for the fidelity of two mixed states, characterized in terms of the Schatten 1-norm, is equivalent to the above Uhlmann characterization:

$$F(\rho_A,\sigma_A) = \left\|\sqrt{\rho_A}\sqrt{\sigma_A}\right\|_1^2 . \tag{38}$$

We state this result as Uhlmann's theorem.

Theorem 13 (Uhlmann's Theorem)**.** *The following two expressions for fidelity are equal:*

$$F(\rho_A,\sigma_A) = \max_U \left|\langle\phi^\rho|_{RA} U_R \otimes I_A |\phi^\sigma\rangle_{RA}\right|^2 = \left\|\sqrt{\rho_A}\sqrt{\sigma_A}\right\|_1^2 . \tag{39}$$

Proof. Let $|\phi^\rho\rangle_{RA}$ denote the canonical purification of ρ_A (see Exercise **??**):

$$|\phi^\rho\rangle_{RA} \equiv (I_R \otimes \sqrt{\rho_A})\, |\Gamma\rangle_{RA} , \tag{40}$$

where $|\Gamma\rangle_{RA}$ is the unnormalized maximally entangled vector:

$$|\Gamma\rangle_{RA} \equiv \sum_i |i\rangle_R |i\rangle_A . \tag{41}$$

Therefore, the state $|\phi^\rho\rangle_{RA}$ is a particular purification of ρ. Let $|\phi^\sigma\rangle_{RA}$ denote the canonical purification of σ_A:

$$|\phi^\sigma\rangle_{RA} \equiv (I_R \otimes \sqrt{\sigma_A})\, |\Gamma\rangle_{RA} . \tag{42}$$

Consider that the overlap $\left|\langle\phi^\rho|U_R \otimes I_A|\phi^\sigma\rangle\right|^2$ is as follows:

$$\left|\langle\phi^\rho|U_R \otimes I_A|\phi^\sigma\rangle\right|^2 = \left|\langle\Gamma|_{RA} \left(U_R \otimes \sqrt{\rho_A}\right) \left(I_R \otimes \sqrt{\sigma_A}\right) |\Gamma\rangle_{RA}\right|^2 \tag{43}$$

$$= \left|\langle\Gamma|_{RA} \left(U_R \otimes \sqrt{\rho_A}\sqrt{\sigma_A}\right) |\Gamma\rangle_{RA}\right|^2 \tag{44}$$

$$= \left|\langle\Gamma|_{RA} \left(I_R \otimes \sqrt{\rho_A}\sqrt{\sigma_A} U_A^T\right) |\Gamma\rangle_{RA}\right|^2 \tag{45}$$

$$= \left|\text{Tr}\left\{\sqrt{\rho_A}\sqrt{\sigma_A} U_A^T\right\}\right|^2 . \tag{46}$$

The first equality follows by plugging in (40) and (42). The third equality follows from Exercise **??**. The last equality follows from Exercise **??**. We can finally invoke Property **??** to establish that

$$\max_{U_A} \left|\text{Tr}\left\{\sqrt{\rho_A}\sqrt{\sigma_A}U_A^T\right\}\right|^2 = \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1^2, \tag{47}$$

from which (39) follows. □

Exercise 14. *Use the expression* $\left\|\sqrt{\rho_A}\sqrt{\sigma_A}\right\|_1^2$ *for the fidelity and the Cauchy-Schwarz inequality for the Hilbert-Schmidt inner product to prove that the quantum fidelity between two density operators never exceeds one.*

2.4 Properties of Fidelity

We discuss some further properties of the fidelity that often prove useful. Some of these properties are the counterpart of similar properties of the trace distance. From the characterization of fidelity in (39), we observe that it is symmetric in its arguments:

$$F(\rho,\sigma) = F(\sigma,\rho). \tag{48}$$

It obeys the following bounds:

$$0 \leq F(\rho,\sigma) \leq 1. \tag{49}$$

The lower bound applies if and only if the respective supports of the two states ρ and σ are orthogonal. To see this, suppose that the supports of ρ and σ are orthogonal. This implies that $\sqrt{\rho}\sqrt{\sigma} = 0$, so that $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2 = 0$. On the other hand, suppose that $F(\rho,\sigma) = 0$. Then by definition, this means that $\|\sqrt{\rho}\sqrt{\sigma}\|_1^2 = 0$, and from non-negative definiteness of the trace norm, we find that $\sqrt{\rho}\sqrt{\sigma} = 0$. This then implies that the supports of ρ and σ are orthogonal. The upper bound in (49) applies if and only if the two states ρ and σ are equal to each other.

Exercise 15. *Show that the definition of fidelity in* (38) *reduces to* (22) *when the two states are pure and to* (26) *when one state is pure and the other is mixed.*

Property 16 (Multiplicativity)**.** *Let* $\rho_1, \sigma_1 \in \mathcal{D}(\mathcal{H}_1)$ *and* $\rho_2, \sigma_2 \in \mathcal{D}(\mathcal{H}_2)$*. The fidelity is multiplicative with respect to tensor products:*

$$F(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = F(\rho_1,\sigma_1)F(\rho_2,\sigma_2). \tag{50}$$

This result holds by employing the definition of the fidelity in (38)*.*

The following monotonicity lemma is similar to the monotonicity lemma for trace distance (Lemma 4) and also bears the similar interpretation that quantum states become more similar (less distinguishable) under the discarding of subsystems.

Lemma 17 (Monotonicity)**.** *Let* $\rho_{AB}, \sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$*. The fidelity is non-decreasing with respect to partial trace:*

$$F(\rho_{AB},\sigma_{AB}) \leq F(\rho_A,\sigma_A), \tag{51}$$

where

$$\rho_A = \text{Tr}_B\left\{\rho_{AB}\right\}, \qquad \sigma_A = \text{Tr}_B\left\{\sigma_{AB}\right\}. \tag{52}$$

Proof. Consider a fixed purification $|\psi\rangle_{RAB}$ of ρ_A and ρ_{AB} and a fixed purification $|\phi\rangle_{RAB}$ of σ_A and σ_{AB}. Then

$$\left|\langle\psi|_{RAB} U_R \otimes I_A \otimes I_B\, |\phi\rangle_{RAB}\right|^2 \leq \max_{U_{RB}} \left|\langle\psi|_{RAB} U_{RB} \otimes I_A |\phi\rangle_{RAB}\right|^2 \tag{53}$$

$$= F(\rho_A, \sigma_A), \tag{54}$$

where the first inequality follows because the maximization over unitaries U_{RB} includes $U_R \otimes I_A$ and the equality is a consequence of Uhlmann's theorem. Given that the inequality holds for all unitaries U_R, we can conclude that

$$F(\rho_{AB}, \sigma_{AB}) = \max_{U_R} \left|\langle\psi|_{RAB} U_R \otimes I_A \otimes I_B |\phi\rangle_{RAB}\right|^2 \leq F(\rho_A, \sigma_A), \tag{55}$$

where the equality is again a consequence of Uhlmann's theorem. □

Property 18 (Joint Concavity)**.** *Let $\rho_x, \sigma_x \in \mathcal{D}(\mathcal{H})$ for all x and let p_X be a probability distribution. The root fidelity is jointly concave with respect to its input arguments:*

$$\sqrt{F}\left(\sum_x p_X(x)\rho_x, \sum_x p_X(x)\sigma_x\right) \geq \sum_x p_X(x)\sqrt{F}\left(\rho_x, \sigma_x\right). \tag{56}$$

Proof. We prove joint concavity by exploiting the result of Exercise **??**. Suppose $|\phi^{\rho_x}\rangle_{RA}$ and $|\phi^{\sigma_x}\rangle_{RA}$ are respective Uhlmann purifications of ρ_x and σ_x (these are purifications that maximize the Uhlmann fidelity). Then

$$F\left(\phi^{\rho_x}_{RA}, \phi^{\sigma_x}_{RA}\right) = F\left(\rho_x, \sigma_x\right). \tag{57}$$

Choose some orthonormal basis $\{|x\rangle_X\}$. Then

$$|\phi^\rho\rangle \equiv \sum_x \sqrt{p_X(x)}|\phi^{\rho_x}\rangle_{RA}|x\rangle_X, \qquad |\phi^\sigma\rangle \equiv \sum_x \sqrt{p_X(x)}|\phi^{\sigma_x}\rangle_{RA}|x\rangle_X \tag{58}$$

are respective purifications of $\sum_x p_X(x)\rho_x$ and $\sum_x p_X(x)\sigma_x$. The first inequality below holds by Uhlmann's theorem:

$$\sqrt{F}\left(\sum_x p_X(x)\rho_x, \sum_x p_X(x)\sigma_x\right) \geq |\langle\phi^\rho|\phi^\sigma\rangle| \tag{59}$$

$$= \left|\sum_x p_X(x)\langle\phi^{\rho_x}|\phi^{\sigma_x}\rangle\right| \tag{60}$$

$$\geq \sum_x p_X(x)\left|\langle\phi^{\rho_x}|\phi^{\sigma_x}\rangle\right| \tag{61}$$

$$= \sum_x p_X(x)\sqrt{F}\left(\rho_x, \sigma_x\right). \tag{62}$$

□

Property 19 (Concavity)**.** *Let $\rho, \sigma, \tau \in \mathcal{D}(\mathcal{H})$ and $\lambda \in [0,1]$. The fidelity is concave with respect to one of its arguments:*

$$F(\lambda\rho + (1-\lambda)\,\tau, \sigma) \geq \lambda F(\rho, \sigma) + (1-\lambda)\, F(\tau, \sigma). \tag{63}$$

Proof. Let $|\psi^\sigma\rangle_{RS}$ be a fixed purification of σ_S. Let $|\psi^\rho\rangle_{RS}$ be a purification of ρ_S such that

$$|\langle\psi^\sigma|\psi^\rho\rangle|^2 = F(\rho, \sigma). \tag{64}$$

Similarly, let $|\psi^\tau\rangle_{RS}$ be a purification of τ_S such that

$$|\langle\psi^\sigma|\psi^\tau\rangle|^2 = F(\tau, \sigma). \tag{65}$$

Then consider that

$$\begin{aligned}
&\lambda F(\rho, \sigma) + (1-\lambda) F(\tau, \sigma) \\
&= \lambda |\langle\psi^\sigma|\psi^\rho\rangle|^2 + (1-\lambda) |\langle\psi^\sigma|\psi^\tau\rangle|^2 && (66)\\
&= \lambda \langle\psi^\sigma|\psi^\rho\rangle \langle\psi^\rho|\psi^\sigma\rangle + (1-\lambda) \langle\psi^\sigma|\psi^\tau\rangle \langle\psi^\tau|\psi^\sigma\rangle && (67)\\
&= \langle\psi^\sigma|_{RS} (\lambda |\psi^\rho\rangle \langle\psi^\rho|_{RS} + (1-\lambda) |\psi^\tau\rangle \langle\psi^\tau|_{RS}) |\psi^\sigma\rangle_{RS} && (68)\\
&= F(|\psi^\sigma\rangle \langle\psi^\sigma|_{RS}, \lambda |\psi^\rho\rangle \langle\psi^\rho|_{RS} + (1-\lambda) |\psi^\tau\rangle \langle\psi^\tau|_{RS}) && (69)\\
&\leq F\left(\psi^\sigma_S, \lambda\psi^\rho_S + (1-\lambda)\psi^\tau_S\right) && (70)\\
&= F(\lambda\rho + (1-\lambda)\tau, \sigma) && (71)
\end{aligned}$$

The first step is a rewriting using (64) and (65). The fourth equality is a consequence of Exercise 15. The inequality follows from monotonicity of the fidelity under partial trace (Lemma 17). □

Exercise 20. *Let $\rho, \sigma \in \mathcal{D}(\mathcal{H})$. Show that we can express the root fidelity as*

$$\sqrt{F}(\rho, \sigma) = \operatorname{Tr}\left\{\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right\} = \operatorname{Tr}\left\{\sqrt{\sigma^{1/2}\rho\sigma^{1/2}}\right\}, \tag{72}$$

using the definition in (38)*.*

Exercise 21. *Let $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ and let $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a quantum channel. Show that the fidelity is monotone with respect to the channel $\mathcal{N}$:*

$$F(\rho, \sigma) \leq F(\mathcal{N}(\rho), \mathcal{N}(\sigma)). \tag{73}$$

Exercise 22. *Let $\rho, \sigma \in \mathcal{D}(\mathcal{H})$. Show that the fidelity is invariant with respect to an isometry $U \in \mathcal{L}(\mathcal{H}, \mathcal{H}')$:*

$$F(\rho, \sigma) = F(U\rho U^\dagger, U\sigma U^\dagger). \tag{74}$$