12 Fidelity

Definition 1. The **fidelity** of two states ρ and σ is defined by

$$F(\rho, \sigma) := \operatorname{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}} = \|\sigma^{1/2}\rho^{1/2}\|_1.$$

It is a measure of how similar the states are.

Remark 2. For any isometry $V_{\mathsf{B}\leftarrow\mathsf{A}}$ and positive operator M_{A}, $(VMV^\dagger)^{1/2} = VM^{1/2}V^\dagger$. It follows that, for any operator L_{A}, $\|VLV^\dagger\|_1 = \|L\|_1$ and for any states $\rho_{\mathsf{A}}, \sigma_{\mathsf{A}}$, $F(V\rho V^\dagger, V\sigma V^\dagger) = F(\rho, \sigma)$.

Remark 3. When one or both of the states is pure, the fidelity simplifies, $F(|\psi\rangle\langle\psi|, \sigma) = (\langle\psi|\sigma|\psi\rangle)^{1/2}$ and $F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle|$.

For example the fidelity between the maximally mixed state $\mathbb{1}_{\mathsf{Q}}/d_{\mathsf{Q}}$ and any pure state $|\psi\rangle\langle\psi|_{\mathsf{Q}}$ is $d_{\mathsf{Q}}^{-1/2}$. It turns out that the fidelity of two states is equal to the largest absolute value of the inner-product between state vectors corresponding to purifications of the two states. This result is called "Uhlmann's theorem" and it makes it easy to derive a number of properties of the fidelity.

Theorem 4 (Uhlmann's theorem)**.** For any R with $\dim \mathsf{R} \geq \dim \mathsf{Q}$,

$$F(\rho_{\mathsf{Q}}, \sigma_{\mathsf{Q}}) = \max\{|\langle\psi|\phi\rangle| : \operatorname{Tr}_{\mathsf{R}}|\psi\rangle\langle\psi|_{\mathsf{QR}} = \rho_{\mathsf{Q}}, \operatorname{Tr}_{\mathsf{R}}|\phi\rangle\langle\phi|_{\mathsf{QR}} = \sigma_{\mathsf{Q}}\}.$$

To prove Uhlmann's theorem, we'll need a few definitions and results which we'll find other uses for. Let's denote by $\mathcal{U}(\mathcal{H})$ the set of all unitary operators in $\mathcal{L}(\mathcal{H})$

Lemma 5. Any $L \in \mathcal{L}(\mathcal{H})$ has a **polar decomposition** $L = U|L|$ for some $U \in \mathcal{U}(\mathcal{H})$.

Proof. We have $L^\dagger L = |L|^2$. Since $|L|^2 \geq 0$ it has an eigendecomposition of the form $|L|^2 = \sum_{j=1}^d \lambda_j^2 |\alpha_j\rangle\langle\alpha_j|$, with $\lambda_j \geq \lambda_{j+1}$, $\lambda_j \geq 0$, and $|L| = \sum_{j=1}^d \lambda_j|\alpha_j\rangle\langle\alpha_j|$. By Lemma 1 from section 9.1, $L = \sum_{j=1}^r \lambda_j|\phi_j\rangle\langle\alpha_j|$, where $\{|\phi_j\rangle : 1 \leq j \leq r\}$ is an orthonormal set and $r = \operatorname{rank}(|L|^2) = \operatorname{rank}(|L|)$. Extending this to an orthonormal basis $\{|\phi_j\rangle : 1 \leq j \leq d\}$ and setting $U = \sum_{j=1}^d |\phi_j\rangle\langle\alpha_j|$, we have $L = U|L|$, and U is unitary. □

Definition 6. For any $L \in \mathcal{L}(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$, the **operator norm** of L is

$$\|L\|_{op} := \max_{\||\psi\rangle_{\mathsf{A}}\| \leq 1} \|L|\psi\rangle\|.$$

Proposition 7. The operator norm has the following properties:

1. If V is an isometry then $\|V\|_{op} = 1$.
2. $\|LR\|_{op} = \max_{\||\psi\rangle\| \leq 1} \|R|\psi\rangle\| \left\| L\frac{R|\psi\rangle}{\|R|\psi\rangle\|}\right\| \leq \|R\|_{op}\|L\|_{op}$.
3. $\|L\|_{op} = \max_{\||\phi\rangle_{\mathsf{B}}\| \leq 1, \||\psi\rangle_{\mathsf{A}}\| \leq 1} |\langle|\phi\rangle, L|\psi\rangle\rangle| = \max_{\||\phi\rangle_{\mathsf{B}}\| \leq 1, \||\psi\rangle_{\mathsf{A}}\| \leq 1} |\langle L^\dagger|\phi\rangle, |\psi\rangle\rangle| = \|L^\dagger\|_{op}$.

4. For any $U \in \mathcal{U}(\mathcal{H})$, $\|LU\|_{op} \leq \|L\|_{op}\|U\|_{op} = \|L\|_{op} = \|LUU^\dagger\|_{op} \leq \|LU\|_{op}$, so $\|LU\|_{op} = \|L\|_{op}$.

Lemma 8. For any $L \in \mathcal{L}(\mathcal{H})$, with polar decomposition $L = U|L|$,

$$\|L\|_1 = \max_{Z\in\mathcal{L}(\mathcal{H}):\|Z\|_{op}\leq 1} |\mathrm{Tr}ZL| = \max_{Z\in\mathcal{U}(\mathcal{H})} |\mathrm{Tr}ZL|$$

and the maximum is achieved for $Z = U^\dagger \in \mathcal{U}(\mathcal{H})$.

Proof. Making the change of variables $Z = Z'U^\dagger$, $\|Z\|_{op} = \|Z'\|_{op}$ by property (4) of the operator norm, and the RHS is equal to $\max_{\|Z'\|_{op}\leq 1} |\mathrm{Tr}Z'|L||$. We need to show this is no more than $\|L\|_1$: Let $|L| = \sum_j \lambda_j |\alpha_j\rangle\langle\alpha_j|$ be an eigendecomposition for $|L|$. Then, for any Z' with $\|Z'\|_{op} \leq 1$,

$$|\mathrm{Tr}Z'|L|| = \left|\sum_j \lambda_j \langle\alpha_j|Z'|\alpha_j\rangle\right| \leq \sum_j \lambda_j |\langle|\alpha_j\rangle, Z'|\alpha_j\rangle\rangle| \tag{12.1}$$

$$\leq \sum_j \lambda_j \||\alpha_j\rangle\|\|Z'|\alpha_j\rangle\| \leq \sum_j \lambda_j = \mathrm{Tr}|L| = \|L\|_1. \tag{12.2}$$

using the triangle inequality, Cauchy-Schwarz and $\||\alpha_j\rangle\| = 1$. Equality is achieved when $Z' = \mathbb{1}$, which means $Z = U^\dagger$. □

Proposition 9. If $|\psi\rangle_{\mathsf{QR}}$ and $|\psi'\rangle_{\mathsf{QR'}}$ are both purifications of a state ρ_{Q}, that is

$$\mathrm{Tr}_{\mathsf{R}}|\psi\rangle\langle\psi|_{\mathsf{QR}} = \mathrm{Tr}_{\mathsf{R'}}|\psi'\rangle\langle\psi'|_{\mathsf{QR'}} = \rho_{\mathsf{Q}} \tag{12.3}$$

and $d_{\mathsf{R}} \geq d_{\mathsf{R'}}$, then there is an isometry $V \in \mathcal{L}(\mathcal{H}_{\mathsf{R'}}, \mathcal{H}_{\mathsf{R}})$ such that

$$|\psi\rangle_{\mathsf{QR}} = V_{\mathsf{R}\leftarrow\mathsf{R'}}|\psi'\rangle_{\mathsf{QR'}}.$$

Proof. Given the equation (12.3), our proof of the Schmidt decomposition (Theorem 3, section 9.1) shows that we can write $|\psi'\rangle_{\mathsf{QR'}} = \sum_{j=1}^r \sqrt{\lambda_j}|\alpha_j\rangle_{\mathsf{Q}}\otimes|\beta_j'\rangle_{\mathsf{R'}}$ and $|\psi\rangle_{\mathsf{QR}} = \sum_{j=1}^r \sqrt{\lambda_j}|\alpha_j\rangle_{\mathsf{Q}}\otimes |\beta_j\rangle_{\mathsf{R}}$, where $\sum_{j=1}^r \lambda_j|\alpha_j\rangle\langle\alpha_j|_{\mathsf{Q}}$ is an eigendecomposition of ρ_{Q}, and where $\{|\beta_j'\rangle_{\mathsf{R'}} : 1 \leq j \leq r\}$ and $\{|\beta_j\rangle_{\mathsf{R}} : 1 \leq j \leq r\}$ are both orthonormal sets. Extending the first of these to an orthonormal *basis* $\{|\beta_j'\rangle_{\mathsf{R'}} : 1 \leq j \leq d_{\mathsf{R'}}\}$ for $\mathcal{H}_{\mathsf{R'}}$, we see that the isometry $V = \sum_{j=1}^{d_{\mathsf{R'}}} |\beta_j\rangle_{\mathsf{R}}\langle\beta_j'|_{\mathsf{R'}}$ does the job. □

12.0.1 Proof of Uhlmann's theorem

Proof. Recall that $\mathrm{Tr}_{\mathsf{R'}}\Phi^+_{\mathsf{QR'}} = \mathbb{1}_{\mathsf{Q}}$. It follows that, for any density operator μ_{Q}, $\mu_{\mathsf{Q}}^{1/2} \otimes \mathbb{1}_{\mathsf{R'}}|\Phi^+\rangle_{\mathsf{QR'}}$ is a purification of μ_{Q}, because

$$\mathrm{Tr}_{\mathsf{R'}}\mu_{\mathsf{Q}}^{1/2} \otimes \mathbb{1}_{\mathsf{R'}}\ \Phi^+_{\mathsf{QR'}}\ \mu_{\mathsf{Q}}^{1/2} \otimes \mathbb{1}_{\mathsf{R'}} = \mu_{\mathsf{Q}}^{1/2}(\mathrm{Tr}_{\mathsf{R'}}\Phi^+_{\mathsf{QR'}})\mu_{\mathsf{Q}}^{1/2} = \mu_{\mathsf{Q}}.$$

From Proposition 9 we know that, for $\dim \mathsf{R} \geq \dim \mathsf{Q}$, $|\psi\rangle_{\mathsf{QR}}$ is a purification of ρ_{Q} iff $|\psi\rangle_{\mathsf{QR}} = \rho_{\mathsf{Q}}^{1/2} \otimes V_{\mathsf{R}\leftarrow\mathsf{R'}}|\Phi^+\rangle_{\mathsf{QR'}}$ for some isometry V and, likewise, $|\phi\rangle_{\mathsf{QR}} = \sigma_{\mathsf{Q}}^{1/2} \otimes U_{\mathsf{R}\leftarrow\mathsf{R'}}|\Phi^+\rangle_{\mathsf{QR'}}$ for some isometry U. Using these expressions for the purifications and the "transpose trick"

$$\langle\rho|\sigma\rangle = \langle\Phi^+|\sigma_{\mathsf{Q}}^{1/2}\rho_{\mathsf{Q}}^{1/2} \otimes W^{\mathrm{T}}_{\mathsf{R'}}|\Phi^+\rangle_{\mathsf{QR'}} = \langle\Phi^+|\sigma_{\mathsf{Q}}^{1/2}\rho_{\mathsf{Q}}^{1/2}W_{\mathsf{Q}} \otimes \mathbb{1}_{\mathsf{R'}}|\Phi^+\rangle_{\mathsf{QR'}} \tag{12.4}$$

$$= \mathrm{Tr}_{\mathsf{QR'}}|\Phi^+\rangle\langle\Phi^+|_{\mathsf{QR'}}\sigma_{\mathsf{Q}}^{1/2}\rho_{\mathsf{Q}}^{1/2}W_{\mathsf{Q}} \otimes \mathbb{1}_{\mathsf{R'}} = \mathrm{Tr}_{\mathsf{Q}}\sigma_{\mathsf{Q}}^{1/2}\rho_{\mathsf{Q}}^{1/2}W_{\mathsf{Q}}, \tag{12.5}$$

where $W_{\mathsf{R}'}^{\mathrm{T}} := U^\dagger V$ and $W_{\mathsf{Q}} := \mathbf{id}^{\mathsf{Q}\leftarrow\mathsf{R}'} W_{\mathsf{R}'}$. Since U and V are isometries, from the properties of the operator norm, $\|W_{\mathsf{Q}}\|_{op} \leq 1$. Furthermore, provided $d_{\mathsf{R}} \geq d_{\mathsf{Q}}$, given any unitary W_{Q} we can find a suitable choice of U and V such that $W_{\mathsf{R}'}^{\mathrm{T}} := U^\dagger V$ (e.g. taking $V = \mathbb{1}_{\mathsf{R}\leftarrow\mathsf{R}'} W_{\mathsf{R}'}^T$ and $U = \mathbb{1}_{\mathsf{R}\leftarrow\mathsf{R}'}$ does the trick). Therefore, by Lemma 8,

$$\max\{|\langle\psi|\phi\rangle| : \mathrm{Tr}_{\mathsf{R}}|\psi\rangle\langle\psi|_{\mathsf{QR}} = \rho_{\mathsf{Q}}, \mathrm{Tr}_{\mathsf{R}}|\phi\rangle\langle\phi|_{\mathsf{QR}} = \sigma_{\mathsf{Q}}\} \tag{12.6}$$

$$= \max_{\|W\|_{op}\leq 1} |\mathrm{Tr}_{\mathsf{Q}}\sigma_{\mathsf{Q}}^{1/2}\rho_{\mathsf{Q}}^{1/2}W_{\mathsf{Q}}| = \|\sigma_{\mathsf{Q}}^{1/2}\rho_{\mathsf{Q}}^{1/2}\|_1 = F(\rho_{\mathsf{Q}}, \sigma_{\mathsf{Q}}). \tag{12.7}$$

□

Proposition 10. The fidelity has the following properties (♣♣: Prove this)

1. $F(\rho, \sigma) = F(\sigma, \rho)$.
2. $0 \leq F(\rho, \sigma) \leq 1$, and $F(\rho, \sigma) = 1$ iff $\rho = \sigma$.
3. $F(V\rho_{\mathsf{A}}V^\dagger, V\sigma_{\mathsf{A}}V^\dagger) = F(\rho, \sigma)$ for any isometry $V_{\mathsf{B}\leftarrow\mathsf{A}}$.
4. $F(\mathrm{Tr}_{\mathsf{B}}\rho_{\mathsf{AB}}, \mathrm{Tr}_{\mathsf{B}}\sigma_{\mathsf{AB}}) \geq F(\rho_{\mathsf{AB}}, \sigma_{\mathsf{AB}})$.
5. $F(\mathcal{M}^{\mathsf{B}\leftarrow\mathsf{A}}\rho_{\mathsf{A}}, \mathcal{M}^{\mathsf{B}\leftarrow\mathsf{A}}\sigma_{\mathsf{A}}) \geq F(\rho_{\mathsf{A}}, \sigma_{\mathsf{A}})$ for any operation $\mathcal{M}^{\mathsf{B}\leftarrow\mathsf{A}}$.
6. $F(\rho \otimes \tau, \sigma \otimes \tau) = F(\rho, \sigma)$.

12.0.2 Relationship to trace norm

The fidelity gives us a way quantify the similarity between two states. We have already seen a way to measure their distinguishability: The trace norm.

Definition 11. The **trace distance** between two states is the function

$$D(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1. \tag{12.8}$$

The factor of $1/2$ means that $0 \leq D(\rho, \sigma) \leq 1$ for any two states.

Note that if we know that a system is either in state σ or state ρ, and each case has equal probability, then the Holevo-Helstrom theorem says that the probability of correctly identifying which state the system is in is $(1 + D(\rho, \sigma))/2$.

The fidelity and the trace distance between two states are related by the **Fuchs-van de Graaf inequalities**:

Proposition 12. $1 - D(\rho, \sigma) \leq F(\rho, \sigma) \leq \sqrt{1 - D(\rho, \sigma)^2}$. (♣♣: See example sheet 2.)

12.0.3 Fidelity of PPT states with ϕ^+

Proposition 13. Let σ_{AB} be a state of AB where $d_{\mathsf{A}} = d_{\mathsf{B}} = d$. If $\sigma_{\mathsf{AB}} \in \mathbf{ppt}(\mathsf{A} : \mathsf{B})$ then $F(\phi^+_{\mathsf{AB}}, \sigma_{\mathsf{AB}}) \leq 1/\sqrt{d}$.

Proof. It is easy to check that the transpose map $\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}$ is its own adjoint w.r.t. the Hilbert-Schmidt inner product, and it is clearly its own inverse. Since the adjoint of a tensor product of maps is the tensor product of the adjoints of the maps, the same remarks apply to the partial transposition $\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}} \otimes \mathbf{id}^{\mathsf{B}\leftarrow\mathsf{B}}$. Therefore,

$$\begin{aligned} F(\phi^+_{\mathsf{AB}}, \sigma_{\mathsf{AB}})^2 =& \mathrm{Tr}\phi^+_{\mathsf{AB}}\sigma_{\mathsf{AB}} = \langle \phi^+_{\mathsf{AB}}, \sigma_{\mathsf{AB}}\rangle = \langle \phi^+_{\mathsf{AB}}, \mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\sigma_{\mathsf{AB}}\rangle \\ =& \langle \mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\phi^+_{\mathsf{AB}}, \mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\sigma_{\mathsf{AB}}\rangle = \frac{1}{d}\mathrm{Tr}[(\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\Phi^+_{\mathsf{AB}})(\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\sigma_{\mathsf{AB}})] = \frac{1}{d}\mathrm{Tr}\mathbb{F}_{\mathsf{AB}}\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\sigma_{\mathsf{AB}} \\ \leq& \frac{1}{d}\max_{\|Z_{\mathsf{AB}}\|_{op}\leq 1}\left|\mathrm{Tr}Z_{\mathsf{AB}}\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\sigma_{\mathsf{AB}}\right| = \frac{1}{d}\|\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\sigma_{\mathsf{AB}}\|_1 = \frac{1}{d}\mathrm{Tr}\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\sigma_{\mathsf{AB}} = \frac{1}{d}. \end{aligned}$$

We used the fact that $\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}\Phi^+_{\mathsf{AB}} =: \mathbb{F}_{\mathsf{AB}} = \sum_{0\leq i,j<d} |i\rangle\langle j|_{\mathsf{A}}\otimes|j\rangle\langle i|_{\mathsf{B}}$ is the unitary 'flip' operator, and therefore has operator norm equal to one; the characterisation of the trace norm proven in handout 8; and the fact that the trace norm of a positive operator is simply its trace, and that $\mathbf{t}^{\mathsf{A}\leftarrow\mathsf{A}}$ preserves trace. □

12.1 The fidelity of an operation

Definition 14. For any operation $\mathcal{N}^{\mathsf{B}\leftarrow\mathsf{A}}$ where $d_{\mathsf{A}} = d_{\mathsf{B}}$ and state ρ_{A} we define

$$\begin{aligned} F_{op}(\mathcal{N}^{\mathsf{B}\leftarrow\mathsf{A}}, \rho_{\mathsf{A}}) :=& \inf_{\mathsf{R},\ \rho_{\mathsf{RA}}}\{F(\mathbf{id}^{\mathsf{B}\leftarrow\mathsf{A}}\rho_{\mathsf{RA}}, \mathcal{N}^{\mathsf{B}\leftarrow\mathsf{A}}\rho_{\mathsf{RA}}) : \mathrm{Tr}_{\mathsf{R}}\rho_{\mathsf{RA}} = \rho_{\mathsf{A}}\} && (12.9) \\ =& F(\mathbf{id}^{\mathsf{B}\leftarrow\mathsf{A}}\psi_{\mathsf{RA}}, \mathcal{N}^{\mathsf{B}\leftarrow\mathsf{A}}\psi_{\mathsf{RA}}), && (12.10) \end{aligned}$$

where ψ_{RA} is any purification of ρ_{A}. The equality is because we can always purify ρ_{RA} without increasing the fidelity (see property 4), and since any two purifications are equivalent up to an isometry between the purifying systems, which does not change the fidelity (property 3), it doesn't matter which one we use.

F_{op} measures how well the operation $\mathcal{N}^{\mathsf{B}\leftarrow\mathsf{A}}$ preserves the state of any *composite* system RA when the part on which the operation acts is initially in the state ρ_{A}. This quantity (or its square) is sometimes called the "entanglement fidelity". Given a Kraus decomposition for the operation, F_{op} has a simple expression in terms of the Kraus operators. For simplicity we take $\mathsf{B} = \mathsf{A}$.

Proposition 15. If $\mathcal{N}^{\mathsf{A}\leftarrow\mathsf{A}} : \rho_{\mathsf{A}} \mapsto \sum_m K_m\rho_{\mathsf{A}}K_m^\dagger$ then $F_{op}(\mathcal{N}^{\mathsf{A}\leftarrow\mathsf{A}}, \rho_{\mathsf{A}}) = \sqrt{\sum_m \left|\mathrm{Tr}K_m\rho_{\mathsf{A}}\right|^2}$.

Proof. Let $\psi_{\mathsf{RA}} = |\psi\rangle\langle\psi|_{\mathsf{RA}}$ be a purification of ρ_{A}.

$$\begin{aligned} F(\psi_{\mathsf{RA}}, \mathcal{N}^{\mathsf{A}\leftarrow\mathsf{A}}\psi_{\mathsf{RA}})^2 =& \langle\psi|(\mathbf{id}^{\mathsf{R}\leftarrow\mathsf{R}} \otimes \mathcal{N}^{\mathsf{A}\leftarrow\mathsf{A}}|\psi\rangle\langle\psi|_{\mathsf{RA}})|\psi\rangle_{\mathsf{RA}} && (12.11) \\ =& \sum_m |\langle\psi|\mathbb{1}_{\mathsf{R}}\otimes K_m|\psi\rangle_{\mathsf{RA}}|^2. && (12.12) \end{aligned}$$

Now, let $|\psi\rangle_{\mathsf{RA}} = \sum_k \sqrt{\lambda_k}|\phi_k\rangle_{\mathsf{R}} \otimes |\alpha_k\rangle_{\mathsf{A}}$ be a Schmidt decomposition for $|\psi\rangle_{\mathsf{RA}}$. Using the orthonormality of the $|\phi_k\rangle$:

$$\langle\psi|\mathbb{1}_{\mathsf{R}}\otimes K_m|\psi\rangle_{\mathsf{RA}} = \sum_{j,k}\sqrt{\lambda_j}\langle\phi_j|_{\mathsf{R}}\otimes\langle\alpha_j|_{\mathsf{A}}\mathbb{1}_{\mathsf{R}}\otimes K_m\sqrt{\lambda_k}|\phi_k\rangle_{\mathsf{R}}\otimes|\alpha_k\rangle_{\mathsf{A}} \tag{12.13}$$

$$= \sum_j \lambda_j\langle\alpha_j|_{\mathsf{A}}K_m|\alpha_j\rangle_{\mathsf{A}} = \mathrm{Tr}K_m\left(\sum_j \lambda_j|\alpha_j\rangle\langle\alpha_j|\right) = \mathrm{Tr}K_m\rho_{\mathsf{A}}. \tag{12.14}$$

□