Purification and fidelity

Sec 4.1, 4.2

1. Reductions, extensions, and purifications

Let X, Y be registers with associated CES $\mathcal{X}$ and $\mathcal{Y}$, respectively.
Suppose that (X, Y) has a state $\rho \in D(\mathcal{X} \otimes \mathcal{Y})$
The individual states of X, Y are given by

$$\rho^X := Tr_{\mathcal{Y}}(\rho) \quad \text{and} \quad \rho^Y := Tr_{\mathcal{X}}(\rho)$$

and we call them the reduced states on X and Y
or the reductions of ρ to X and Y.

Def (Extensions):

Let $\sigma \in D(\mathcal{X})$ be a state.
Then, a state $\rho \in D(\mathcal{X} \otimes \mathcal{Y})$ is called an extension of σ
if $\sigma = Tr_{\mathcal{Y}}(\rho)$.

Eg For a state $\sigma \in D(\mathcal{X})$, $\sigma \otimes \xi$ is an extension of σ for any $\xi \in D(\mathcal{Y})$.

Def (purifications):

Let $\rho \in D(\mathcal{X})$ be a state.
A pure state $\rho = uu^*$ is called a purification of σ
if $\sigma = Tr_{\mathcal{Y}}(\rho) = Tr_{\mathcal{Y}}(uu^*)$.

In this case, $u \in \mathcal{X} \otimes \mathcal{Y}$ is also called a purification.

Note: A purification is a special type of extension using a pure state.

The concepts of reductions, extensions, and purifications are naturally extended to positive semidefinite operators.

Def (purifications of positive semidefinite operators)

Let $P \in \mathrm{Pos}(\mathcal{X})$.

If there exists a vector $u \in \mathcal{X} \otimes \mathcal{Y}$ such that $P = \mathrm{Tr}_{\mathcal{Y}}(uu^*)$,

u (or uu^*) is called a purification of P.

Eg $\mathcal{X} = \mathcal{Y} = \mathbb{C}^{\Sigma}$.

$u = \sum_{a \in \Sigma} e_a \otimes e_a$ is a purification of $\mathbb{1}_{\mathcal{X}} = \sum_{a \in \Sigma} e_a e_a^*$.

Eg $\sigma = \sum_{i=1}^{\dim(\mathcal{X})} p(i)\, u_i u_i^*$; a spectral decomposition of $\sigma \in D(\mathcal{X})$.

Then, $u = \sum_{i=1}^{\dim(\mathcal{X})} \sqrt{p(i)}\, u_i \otimes u_i$ is a purification of σ.

- Existence of purification sec 4.2

Thm 1

Let $\mathcal{X}$ and $\mathcal{Y}$ be CES, and let $P \in \mathrm{Pos}(\mathcal{X})$.

Then, there exists a purification $u \in \mathcal{X} \otimes \mathcal{Y}$ of P

if and only if $\dim(\mathcal{Y}) \geq \mathrm{rank}(P)$.

To show Thm 1, we will use the following observation.

Lem 1

Let $P \in \mathrm{Pos}(\mathcal{X})$. The following are equivalent.

1. There exists a purification $u \in \mathcal{X} \otimes \mathcal{Y}$ of P
2. There exists an operator $A \in L(\mathcal{Y}, \mathcal{X})$ such that $P = AA^*$.

proof

Sec 2.4 or F2023 lecture 1.5

$(1 \Rightarrow 2)$ Suppose that a purification u of P exists. that is, $P = \mathrm{Tr}_{\mathcal{Y}}(uu^*)$

Recall the Vec function. $(\mathrm{Vec} : L(\mathcal{Y}, \mathcal{X}) \to \mathcal{X} \otimes \mathcal{Y},\ \mathrm{Vec}(E_{a,b}) = e_a \otimes e_b)$

Since Vec is bijective, there exists $A \in L(\mathcal{Y}, \mathcal{X})$ such that $u = \mathrm{Vec}(A)$.

Since $P = \mathrm{Tr}_{\mathcal{Y}}(uu^*) = \mathrm{Tr}_{\mathcal{Y}}(\mathrm{Vec}(A)\mathrm{Vec}(A)^*) \underset{\text{A1 Q1 (b)}}{=} AA^*$, $-(*)$

We have statement 2.

$(2 \Rightarrow 1)$ Suppose that $A \in L(\mathcal{Y}, \mathcal{X})$ with $P = AA^*$ exists.

Define $u = \mathrm{Vec}(A)$. By $(*)$, u serves as a purification of P.

Now, let's show Thm 1.

Proof of Thm 1

Theory of Quantum Information (Textbook) p.12

Suppose that a purification u of P exists.

By Lem 1, $A \in L(\mathcal{Y}, \mathcal{X})$ with $P = AA^*$ exists.

$\therefore \quad \operatorname{rank}(P) = \operatorname{rank}(AA^*) = \operatorname{rank}(A) \leq \dim(\mathcal{Y})$.

On the other hand, suppose that $\operatorname{rank}(P) \leq \dim(\mathcal{Y})$.

Let $r = \operatorname{rank}(P)$ and consider a spectral decomposition

$$P = \sum_{k=1}^{r} \lambda_k x_k x_k^*, \quad \text{where} \begin{cases} \lambda_k \geq 0 & k = 1, 2, \cdots, r \\ x_1, \cdots, x_r : & \text{orthonormal vectors on } \mathcal{X}. \end{cases}$$

Since $\operatorname{rank}(P) \leq \dim(\mathcal{Y})$, we can choose an orthonormal vectors $y_1, y_2, \cdots, y_r \in \mathcal{Y}$.

Then, the operator $A = \sum_{k=1}^{r} \sqrt{\lambda_k} x_k y_k^*$ satisfies $P = AA^*$.

By Lem 1, a purification u of P exists.

(Actually, we can take $u = \operatorname{vec}(A)$ by the proof of Lem 1) $\blacksquare$

Thm 1 implies that a purification always exists if $\mathcal{Y}$ is sufficiently large.

Cor 1

Let $\mathcal{X}$ and $\mathcal{Y}$ be CES with $\dim(\mathcal{Y}) \geq \dim(\mathcal{X})$.

For any $P \in \operatorname{Pos}(\mathcal{X})$, there exists a purification $u \in \mathcal{X} \otimes \mathcal{Y}$ of P.

For the proof, observe $\dim(\mathcal{X}) \geq \operatorname{rank}(P) \ \forall P \in \operatorname{Pos}(\mathcal{X})$.

- Unitary equivalence of purifications Sec 4.2

Thm 2

Let $\mathcal{X}$ and $\mathcal{Y}$ be CES, and let $u, v \in \mathcal{X} \otimes \mathcal{Y}$.

Assume that $\mathrm{Tr}_{\mathcal{Y}}(uu^*) = \mathrm{Tr}_{\mathcal{Y}}(vv^*)$.

There exists a unitary operator $U \in \mathrm{U}(\mathcal{Y})$ such that $v = (\mathbb{1}_{\mathcal{X}} \otimes U) u$.

proof

Define $P = \mathrm{Tr}_{\mathcal{Y}}(uu^*) = \mathrm{Tr}_{\mathcal{Y}}(vv^*) \in \mathrm{Pos}(\mathcal{X})$.

Let $A, B \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ be (unique) linear operators such that

$u = \mathrm{Vec}(A)$ and $v = \mathrm{Vec}(B)$.

$\therefore \; AA^* = \mathrm{Tr}_{\mathcal{Y}}(uu^*) = P = \mathrm{Tr}_{\mathcal{Y}}(vv^*) = BB^*$.

$\therefore \; \mathrm{rank}(A) = \mathrm{rank}(P) = \mathrm{rank}(B) =: r$.

Let $P = \sum_{k=1}^{r} \lambda_k x_k x_k^*$ be a spectral decomposition.

(see Sec 2.1, for example)

Since $AA^* = P = BB^*$, we can choose singular value decompositions

$$A = \sum_{k=1}^{r} \sqrt{\lambda_k}\, x_k y_k^* \quad \text{and} \quad B = \sum_{k=1}^{r} \sqrt{\lambda_k}\, x_k z_k^*$$

using some orthonormal sets of vectors $\{y_1, \cdots, y_r\}$ and $\{z_1, \cdots, z_r\}$

Now, take a unitary operator $V \in \mathrm{U}(\mathcal{Y})$ such that $\underbrace{V z_k = y_k}_{(**)}$ for all k.

(For example, we can take $V = \sum_{k=1}^{\dim(\mathcal{Y})} y_k z_k^*$,

where $y_{r+1}, \cdots, y_{\dim(\mathcal{Y})}$ and $z_{r+1}, \cdots, z_{\dim(\mathcal{Y})}$ are additional vectors

so that $\{y_1, \cdots, y_{\dim(\mathcal{Y})}\}$ and $\{z_1, \cdots, z_{\dim(\mathcal{Y})}\}$ are orthonormal bases of $\mathcal{Y}$.)

Take $U = V^T$. Then $(\mathbb{1}_{\mathcal{X}} \otimes U) u = (\mathbb{1}_{\mathcal{X}} \otimes V^T) \mathrm{Vec}(A) \underset{\uparrow \text{A1@1 ©}}{=} \mathrm{Vec}(AV) \underset{\uparrow (**)}{=} \mathrm{Vec}(B) = v$

2. Fidelity function   Sec 4.3, 4.4

A function that quantifies the similarity of two quantum states.

Sec 4.3.1

Def: Let $\mathcal{X}$ be a CES, and let $P, Q \in \mathrm{Pos}(\mathcal{X})$.

The fidelity between P and Q is defined as

$$F(P,Q) := \| \sqrt{P}\sqrt{Q} \|_1 = \mathrm{Tr}\left[\sqrt{\sqrt{P}\, Q \sqrt{P}} \right]$$

Sec 4.3.2

Obs.
- $F(P,Q) = F(Q,P)$ for any $P, Q \in \mathrm{Pos}(\mathcal{X})$.
- $F(uu^*, Q) = \sqrt{u^* Q u}$ for any $u \in \mathcal{X}$ and any Q.
- $F(uu^*, vv^*) = |\langle u, v \rangle|$ for any $u, v \in \mathcal{X}$.

prop 1 (multiplicativity):

Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be CES, and let $P_1, Q_1 \in \mathrm{Pos}(\mathcal{X}_1)$ and $P_2, Q_2 \in \mathrm{Pos}(\mathcal{X}_2)$.

Then, $F(P_1 \otimes P_2, Q_1 \otimes Q_2) = F(P_1, Q_1)\, F(P_2, Q_2)$.

proof

$$\begin{aligned} F(P_1 \otimes P_2, Q_1 \otimes Q_2) &= \| \sqrt{P_1 \otimes P_2}\, \sqrt{Q_1 \otimes Q_2} \|_1 \\ &= \| (\sqrt{P_1} \otimes \sqrt{P_2})(\sqrt{Q_1} \otimes \sqrt{Q_2}) \|_1 \\ &= \| \sqrt{P_1}\sqrt{Q_1} \otimes \sqrt{P_2}\sqrt{Q_2} \|_1 \\ &= \| \sqrt{P_1}\sqrt{Q_1} \|_1 \, \| \sqrt{P_2}\sqrt{Q_2} \|_1 \\ &= F(P_1, Q_1)\, F(P_2, Q_2) \quad ▨ \end{aligned}$$

- Characterizations of the fidelity function

Sec 4.3.3

Thm 3 (Uhlmann's Theorem)

Let $\mathcal{X}$ be a CES, and let $P, Q \in \mathrm{Pos}(\mathcal{X})$.
Let $\mathcal{Y}$ be a CES with $\dim(\mathcal{Y}) \geq \max\{\mathrm{rank}(P), \mathrm{rank}(Q)\}$,
and let $u \in \mathcal{X} \otimes \mathcal{Y}$ be a purification of P. ← Existence of u is ok by Thm 1
Then, $F(P, Q) = \max\{|\langle u, v\rangle| : v \in \mathcal{X} \otimes \mathcal{Y},\ \mathrm{Tr}_{\mathcal{Y}}(vv^*) = Q\}$.

proof

Since $\dim(\mathcal{Y}) \geq \max\{\mathrm{rank}(P), \mathrm{rank}(Q)\}$, there exist A and $B \in L(\mathcal{Y}, \mathcal{X})$ such that $A^*A = \Pi_{\mathrm{im}(P)}$ and $B^*B = \Pi_{\mathrm{im}(Q)}$.

(For example, let $P = \sum_{k=1}^{\mathrm{rank}(P)} \lambda_k x_k x_k^*$, $Q = \sum_{k=1}^{\mathrm{rank}(Q)} \eta_k y_k y_k^*$ be spectral decompositions.
Take sets of orthonormal vectors on $\mathcal{Y}$ $\{z_1, \cdots, z_{\mathrm{rank}(P)}\}$ and $\{w_1, \cdots, w_{\mathrm{rank}(Q)}\}$.
Define $A = \sum_{k=1}^{\mathrm{rank}(P)} z_k x_k^*$ and $B = \sum_{k=1}^{\mathrm{rank}(Q)} w_k y_k^*$)

Since $\mathrm{Tr}_{\mathcal{Y}}(\mathrm{vec}(\sqrt{P}A^*)\mathrm{vec}(\sqrt{P}A^*)^*) = \sqrt{P}A^*A\sqrt{P} = P$
and $\mathrm{Tr}_{\mathcal{Y}}(\mathrm{vec}(\sqrt{Q}B^*)\mathrm{vec}(\sqrt{Q}B^*)^*) = \sqrt{Q}B^*B\sqrt{Q} = Q$,

$\mathrm{vec}(\sqrt{P}A^*)$ and $\mathrm{vec}(\sqrt{Q}B^*)$ are purifications of P and Q, respectively.

By Thm 2, there exists $U \in U(\mathcal{Y})$ such that

$$u = (\mathbb{1}_{\mathcal{X}} \otimes U)\mathrm{vec}(\sqrt{P}A^*) = \mathrm{vec}(\sqrt{P}A^*U^T).$$

Similarly, any purification $v \in \mathcal{X} \otimes \mathcal{Y}$ of Q can be written as

$$v = (\mathbb{1}_{\mathcal{X}} \otimes V)\mathrm{vec}(\sqrt{Q}B^*) = \mathrm{vec}(\sqrt{Q}B^*V^T)$$

using some $V \in U(\mathcal{Y})$.

Note that $(\mathbb{1}_{\mathcal{X}} \otimes V)\mathrm{vec}(\sqrt{Q}B^*)$ is a purification of Q for any $V \in U(\mathcal{Y})$, conversely.

(proof of Thm 3, Cont'd)

$$\therefore \max\left\{|\langle u, v\rangle| : v \in \mathcal{X}\otimes\mathcal{Y},\ \mathrm{Tr}_{\mathcal{Y}}(vv^*) = Q\right\} = \max_{V\in U(\mathcal{Y})} \left|\langle \mathrm{vec}(\sqrt{P}A^*U^T), \mathrm{vec}(\sqrt{Q}B^*V^T)\rangle\right|$$

$\langle \mathrm{vec}(X), \mathrm{vec}(Y)\rangle = \langle X, Y\rangle$ (Sec 2.4) $\rightarrow$ $$= \max_{V\in U(\mathcal{Y})} \left|\langle \sqrt{P}A^*U^T, \sqrt{Q}B^*V^T\rangle\right|$$

$\langle AB, C\rangle = \langle A, CB^*\rangle = \langle B, A^*C\rangle$ $\rightarrow$ $$= \max_{V\in U(\mathcal{Y})} \left|\langle U^T\bar{V}, A\sqrt{P}\sqrt{Q}B^*\rangle\right|$$

$\|X\|_1 = \max_{U\in U(\mathcal{X})} |\langle U, X\rangle|$ (Sec 2.3.2) $\rightarrow$ $$= \|A\sqrt{P}\sqrt{Q}B^*\|_1$$

Since $\Pi_{\mathrm{im}(P)} = A^*A$, $\Pi_{\mathrm{im}(Q)} = B^*B$, $\|A\|_\infty, \|B\|_\infty \le 1$, and

$$\|\sqrt{P}\sqrt{Q}\|_1 = \|\Pi_{\mathrm{im}(P)}\sqrt{P}\sqrt{Q}\,\Pi_{\mathrm{im}(Q)}\|_1 = \|A^*A\sqrt{P}\sqrt{Q}B^*B\|_1$$

$\|XYZ\|_1 \le \|X\|_\infty \|Y\|_1 \|Z\|_\infty$ (Sec 2.3.2)

$$\le \|A^*\|_\infty \|A\sqrt{P}\sqrt{Q}B^*\|_1 \|B\|_\infty$$
$$\le \|A\sqrt{P}\sqrt{Q}B^*\|_1$$
$$\le \|A\|_\infty \|\sqrt{P}\sqrt{Q}\|_1 \|B^*\|_\infty$$
$$\le \|\sqrt{P}\sqrt{Q}\|_1$$

$\therefore$ $\|A\sqrt{P}\sqrt{Q}B^*\|_1 = \|\sqrt{P}\sqrt{Q}\|_1$, and

$$\max\left\{|\langle u, v\rangle| : v \in \mathcal{X}\otimes\mathcal{Y},\ \mathrm{Tr}_{\mathcal{Y}}(vv^*) = Q\right\} = \|A\sqrt{P}\sqrt{Q}B^*\|_1 = \|\sqrt{P}\sqrt{Q}\|_1 = F(P, Q) \qquad \blacksquare$$

Note: In fact, by appropriately choosing an optimal v in the statement of Thm3, we have $F(P, Q) = \langle u, v\rangle$.

Obs. For all density operators ρ, ξ, $0 \le F(\rho, \xi) \le 1$.

$F(\rho, \xi) = 1$ if and only if $\rho = \xi$, and

$F(\rho, \xi) = 0$ if and only if $\rho\xi = 0$.

Prop 2

Let $\mathcal{X}$ be a CES, and let $P_1, \cdots, P_k, Q_1, \cdots, Q_k \in \mathrm{Pos}(\mathcal{X})$.

Then, $F\left(\sum_{j=1}^{k} P_j, \sum_{j=1}^{k} Q_j\right) \ge \sum_{j=1}^{k} F(P_j, Q_j)$.

proof

Let $\mathcal{Y}$ be a CES with $\dim(\mathcal{Y}) \ge \dim(\mathcal{X})$. Existence is due to Cor 1.

By Thm 3, we can choose purifications $u_1, u_2, \cdots, u_k, v_1, \cdots, v_k \in \mathcal{X} \otimes \mathcal{Y}$

of $P_1, P_2, \cdots, P_k, Q_1, \cdots, Q_k$ with $\langle u_j, v_j \rangle = F(P_j, Q_j)$.

Note of Thm 3

Let $\mathcal{Z} = \mathbb{C}^k$, and define $u, v \in \mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z}$ as

$$u = \sum_{j=1}^{k} u_j \otimes e_j \quad \text{and} \quad v = \sum_{j=1}^{k} v_j \otimes e_j.$$

Since $\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}(uu^*) = \sum_{j=1}^{k} \mathrm{Tr}_{\mathcal{Y}}(u_j u_j^*) = \sum_{j=1}^{k} P_j$

$\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}(vv^*) = \sum_{j=1}^{k} Q_j$,

u, v are purifications of $\sum_{j=1}^{k} P_j$, $\sum_{j=1}^{k} Q_j$, respectively.

By Thm 3,
$$\begin{aligned} F\left(\sum_{j=1}^{k} P_j, \sum_{j=1}^{k} Q_j\right) &\ge |\langle u, v \rangle| \\ &= \left|\sum_{j=1}^{k} \langle u_j, v_j \rangle\right| \\ &= \left|\sum_{j=1}^{k} F(P_j, Q_j)\right| = \sum_{j=1}^{k} F(P_j, Q_j) \end{aligned}$$ ▨

Cor 2

$F(\lambda\rho_1 + (1-\lambda)\rho_2, \lambda\xi_1 + (1-\lambda)\xi_2) \ge \lambda F(\rho_1, \xi_1) + (1-\lambda) F(\rho_2, \xi_2)$

for all $\rho_1, \rho_2, \xi_1, \xi_2 \in D(\mathcal{X})$ and $0 \le \lambda \le 1$.

Thm 4

Textbook, Sec 3.2.2, p148

Let $\mathcal{X}$ be a CES, and let $P, Q \in \mathrm{Pos}(\mathcal{X})$.

Then, $F(P,Q) = \inf\left\{\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle Q, Y^{-1}\rangle : Y \in \mathrm{Pd}(\mathcal{X})\right\}$.

the set of positive "definite" operators on $\mathcal{X}$.

proof

The proof consists of 3 steps.

① $P = Q$

In this case, we show $\underset{\substack{\| \\ F(P,P)}}{\mathrm{Tr}(P)} = \underbrace{\inf\left\{\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle P, Y^{-1}\rangle : Y \in \mathrm{Pd}(\mathcal{X})\right\}}_{(***)}$.

Observe that

$(***) \le \frac{1}{2}\mathrm{Tr}(P) + \frac{1}{2}\mathrm{Tr}(P) = \mathrm{Tr}(P)$.

By taking $Y = \mathbb{1}_{\mathcal{X}}$

Thus, it suffices to show $(***) \ge \mathrm{Tr}(P)$

For this purpose, we show $\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle P, Y^{-1}\rangle \ge \mathrm{Tr}(P)$ for all $Y \in \mathrm{Pd}(\mathcal{X})$.

Observe that $\frac{Y + Y^{-1}}{2} - \mathbb{1}_{\mathcal{X}} = \frac{1}{2}\left(Y^{\frac{1}{2}} - Y^{-\frac{1}{2}}\right)^2 \in \mathrm{Pos}(\mathcal{X})$.

$\therefore \left\langle P, \frac{Y+Y^{-1}}{2} - \mathbb{1}_{\mathcal{X}}\right\rangle \ge 0$, and thus $\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle P, Y^{-1}\rangle \ge \langle P, \mathbb{1}_{\mathcal{X}}\rangle = \mathrm{Tr}(P)$.

(proof of Thm 4, cont'd)

② $P, Q \in \mathrm{Pd}(\mathcal{X})$.

Define $R := \sqrt{\sqrt{P}\,Q\,\sqrt{P}}$ and

$$Z := R^{-\frac{1}{2}}\sqrt{P}\,Y\sqrt{P}\,R^{-\frac{1}{2}}.$$

$P, Q \in \mathrm{Pd}(\mathcal{X})$, so $R \in \mathrm{Pd}(\mathcal{X})$. $\therefore RR^{-1} = \mathbb{1}_{\mathcal{X}}$.

We have $\langle R, Z \rangle = \langle R, R^{-\frac{1}{2}}\sqrt{P}\,Y\sqrt{P}\,R^{-\frac{1}{2}} \rangle = \langle P, Y \rangle$

and

$$\langle R, Z^{-1} \rangle = \langle R, R^{\frac{1}{2}} P^{-\frac{1}{2}} Y^{-1} P^{-\frac{1}{2}} R^{\frac{1}{2}} \rangle$$

$$= \langle P^{-\frac{1}{2}} \underbrace{R^2}_{=\sqrt{P}\,Q\,\sqrt{P}} P^{-\frac{1}{2}}, Y^{-1} \rangle = \langle Q, Y^{-1} \rangle$$

$P \in \mathrm{Pd}(\mathcal{X})$, so $PP^{-1} = \mathbb{1}_{\mathcal{X}}$.

Since $P, R \in \mathrm{Pd}(\mathcal{X})$, there is a one-to-one correspondence between Y and Z, and when Y ranges over all positive definite operators, so does Z.

$$\therefore \inf_{Y \in \mathrm{Pd}(\mathcal{X})} \left[\frac{1}{2}\langle P, Y \rangle + \frac{1}{2}\langle Q, Y^{-1} \rangle \right] = \inf_{Z \in \mathrm{Pd}(\mathcal{X})} \left[\frac{1}{2}\langle R, Z \rangle + \frac{1}{2}\langle R, Z^{-1} \rangle \right]$$

$$= \mathrm{Tr}(R) = F(P, Q)$$

step ①

(Proof of Thm 4, cont'd)

③ General case ($P, Q \in \mathrm{Pos}(\mathcal{X})$)

Let $\varepsilon > 0$ be an arbitrary positive real number.

We have $\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle Q, Y^{-1}\rangle < \frac{1}{2}\langle P+\varepsilon \mathbb{1}_{\mathcal{X}}, Y\rangle + \frac{1}{2}\langle Q+\varepsilon \mathbb{1}_{\mathcal{X}}, Y^{-1}\rangle$

Since $\mathrm{Tr}(Y), \mathrm{Tr}(Y^{-1}) > 0$.

$P+\varepsilon \mathbb{1}_{\mathcal{X}}, Q+\varepsilon \mathbb{1}_{\mathcal{X}} \in \mathrm{Pd}(\mathcal{X})$.

Taking the infimum over all $Y \in \mathrm{Pd}(\mathcal{X})$, by step ②,

$$\inf_{Y \in \mathrm{Pd}(\mathcal{X})} \left[\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle Q, Y^{-1}\rangle\right] < F(P+\varepsilon \mathbb{1}_{\mathcal{X}}, Q+\varepsilon \mathbb{1}_{\mathcal{X}}) \quad - (****)$$

Since (****) holds for all $\varepsilon > 0$,

Considering the continuity of the fidelity, ($F(P,Q) = \|\sqrt{P}\sqrt{Q}\|_1$)

$$\inf_{Y \in \mathrm{Pd}(\mathcal{X})} \left[\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle Q, Y^{-1}\rangle\right] \le F(P, Q) \quad - ①$$

Take the limit $\varepsilon \to 0$

On the other hand, for any $Y \in \mathrm{Pd}(\mathcal{X})$ and any $\varepsilon > 0$,

$$\frac{1}{2}\langle P+\varepsilon \mathbb{1}_{\mathcal{X}}, Y\rangle + \frac{1}{2}\langle Q+\varepsilon \mathbb{1}_{\mathcal{X}}, Y^{-1}\rangle \ge F(P+\varepsilon \mathbb{1}_{\mathcal{X}}, Q+\varepsilon \mathbb{1}_{\mathcal{X}}).$$

By taking $\varepsilon \to 0$ on both sides, by continuity of fidelity and inner-product,

$$\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle Q, Y^{-1}\rangle \ge F(P, Q)$$

$\therefore$ By taking the infimum over all $Y \in \mathrm{Pd}(\mathcal{X})$,

$$\inf_{Y \in \mathrm{Pd}(\mathcal{X})} \left[\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle Q, Y^{-1}\rangle\right] \ge F(P, Q) \quad - ②$$

① and ② yield the desired expression. $\blacksquare$

Cor 2 (Alberti's Theorem) textbook Sec 3.2.2 p148

Let $\mathcal{X}$ be a CES, and let $P, Q \in \mathrm{Pos}(\mathcal{X})$.

Then, $$F(P,Q)^2 = \underbrace{\inf \left\{ \langle P, Y \rangle \langle Q, Y^{-1} \rangle : Y \in \mathrm{Pd}(\mathcal{X}) \right\}}_{(*****)}$$

proof

If $P=0$ or $Q=0$, $F(P,Q)=0$ and $(*****)=0$.

So, the statement trivially holds.

In the following, we assume $P \neq 0$ and $Q \neq 0$.

By the arithmetic-geometric mean inequality, $\rightarrow$ $\sqrt{ab} \leq \frac{a+b}{2}$ for all $a, b \geq 0$.
Can be shown by $(\sqrt{a}-\sqrt{b})^2 \geq 0$.

$$\sqrt{\langle P, Y \rangle \langle Q, Y^{-1} \rangle} \leq \frac{1}{2}\langle P, Y \rangle + \frac{1}{2}\langle Q, Y^{-1} \rangle \quad \text{for any } Y \in \mathrm{Pd}(\mathcal{X}).$$

$\therefore$ By Thm 4,

$$(*****) = \inf_{Y \in \mathrm{Pd}(\mathcal{X})} \left[\langle P, Y \rangle \langle Q, Y^{-1} \rangle \right] \leq \inf_{Y \in \mathrm{Pd}(\mathcal{X})} \left[\left(\frac{1}{2}\langle P, Y \rangle + \frac{1}{2}\langle Q, Y^{-1} \rangle \right) \right]^2$$

$$\frac{1}{2}\langle P, Y \rangle + \frac{1}{2}\langle Q, Y^{-1} \rangle \geq 0 \rightarrow = \left(\inf_{Y \in \mathrm{Pd}(\mathcal{X})} \left[\frac{1}{2}\langle P, Y \rangle + \frac{1}{2}\langle Q, Y^{-1} \rangle \right] \right)^2$$

$$= F(P,Q)^2$$

(Proof of Cor 2, cont'd)

On the other hand, observe that

$$\sqrt{\langle P, Y\rangle\langle Q, Y^{-1}\rangle} = \sqrt{\langle P, \alpha Y\rangle\langle Q, (\alpha Y)^{-1}\rangle} \quad \text{for any } P \in Pd(\mathcal{X}) \text{ and } \alpha \neq 0.$$

For $\alpha = \sqrt{\dfrac{\langle Q, Y^{-1}\rangle}{\langle P, Y\rangle}}$, $\quad \langle P, \alpha Y\rangle = \langle Q, (\alpha Y)^{-1}\rangle = \sqrt{\langle P, Y\rangle\langle Q, Y^{-1}\rangle}$.

For this choice of α, the arithmetic mean and the geometric mean of $\langle P, \alpha Y\rangle$ and $\langle Q, (\alpha Y)^{-1}\rangle$ become equal. (For $a, b \geq 0$ $\sqrt{ab} = \frac{a+b}{2}$ iff $a = b$)

$$\therefore \sqrt{\langle P, Y\rangle\langle Q, Y^{-1}\rangle} = \frac{1}{2}\langle P, \alpha Y\rangle + \frac{1}{2}\langle Q, (\alpha Y)^{-1}\rangle \geq F(P, Q)$$

Using Thm 4 since $\alpha Y \in Pd(\mathcal{X})$.

$$\therefore (*****) = \inf_{Y \in Pd(\mathcal{X})}\left[\langle P, Y\rangle\langle Q, Y^{-1}\rangle\right] \geq F(P, Q)^2$$

$\blacksquare$

Note: In textbook, another proof of Thm 4 is also shown, which makes use of semidefinite programming (SDP).
In fact, Thm3 and Thm4 are related by the property called "strong duality", which is an important concept of SDP.

- Fuchs - van de Graaf inequality   Sec 4.4

A relation between the fidelity and the distance induced by the Trace norm.

We first show the following technical lemma.

Lem 2

Let $\mathcal{X}$ be a CES, and let $P, Q \in \mathrm{Pos}(\mathcal{X})$.

Then, $\| P - Q \|_1 \geq \| \sqrt{P} - \sqrt{Q} \|_2^2$.

proof

Consider a spectral decomposition $\sqrt{P} - \sqrt{Q} = \sum_{j=1}^{\dim(\mathcal{X})} \lambda_j x_j x_j^*$.

$\| \sqrt{P} - \sqrt{Q} \|_2^2 = \sum_{j=1}^{\dim(\mathcal{X})} |\lambda_j|^2$. $-①$

Define $U = \sum_{j=1}^{\dim(\mathcal{X})} \mathrm{sign}(\lambda_j) x_j x_j^*$, where $\mathrm{sign}(\lambda) := \begin{cases} 1 & (\lambda \geq 0) \\ -1 & (\lambda < 0) \end{cases}$.

Then, $(\sqrt{P} - \sqrt{Q}) U = U (\sqrt{P} - \sqrt{Q}) = \sum_{j=1}^{\dim(\mathcal{X})} |\lambda_j| x_j x_j^*$. $-②$

Using the identity $A^2 - B^2 = \frac{1}{2}\left[(A-B)(A+B) + (A+B)(A-B) \right]$, $-③$

$$
\begin{aligned}
\| P - Q \|_1 &\geq \left| \mathrm{Tr}[(P-Q)U] \right| \\
&\underset{③}{=} \left| \frac{1}{2} \mathrm{Tr}\left[(\sqrt{P}-\sqrt{Q})(\sqrt{P}+\sqrt{Q})U\right] + \frac{1}{2} \mathrm{Tr}\left[(\sqrt{P}+\sqrt{Q})(\sqrt{P}-\sqrt{Q})U\right] \right| \\
&\underset{②}{=} \sum_{j=1}^{\dim(\mathcal{X})} |\lambda_j| \, \underbrace{x_j (\sqrt{P}+\sqrt{Q}) x_j^*}_{\substack{\geq |x_j \sqrt{P} x_j^* - x_j \sqrt{Q} x_j^*| \\ = |x_j (\sqrt{P}-\sqrt{Q}) x_j^*| \; = \; |\lambda_j|}} \\
&\geq \sum_{j=1}^{\dim(\mathcal{X})} |\lambda_j|^2 \\
&\underset{①}{=} \| \sqrt{P} - \sqrt{Q} \|_2^2
\end{aligned}
$$

$\boxtimes$

Thm 5 (Fuchs - van de Graaf)

Let $\mathcal{X}$ be a CES, and let $\rho, \xi \in D(\mathcal{X})$ be states.

Then, $1 - \frac{1}{2}\|\rho - \xi\|_1 \leq F(\rho, \xi) \leq \sqrt{1 - \frac{1}{4}\|\rho - \xi\|_1^2}$

proof

First, we show the left-side inequality.

Observe that $\|\sqrt{\rho} - \sqrt{\xi}\|_2^2 = \mathrm{Tr}\left[(\sqrt{\rho} - \sqrt{\xi})^2\right] = \mathrm{Tr}\left[\rho + \xi - \sqrt{\rho}\sqrt{\xi} - \sqrt{\xi}\sqrt{\rho}\right]$

$$= 2 - 2\mathrm{Tr}\left[\sqrt{\rho}\sqrt{\xi}\right] = 2 - 2F(\rho, \xi).$$

Since $\|\rho - \xi\|_1 \geq \|\sqrt{\rho} - \sqrt{\xi}\|_2^2$ by Lem 2,

We have $\|\rho - \xi\|_1 \geq 2 - 2F(\rho, \xi)$, which is equivalent to the desired inequality.

Next, we show the right-side inequality.

Let $\mathcal{Y}$ be a CES with $\dim(\mathcal{Y}) \geq \dim(\mathcal{X})$, and take purifications $u, v \in \mathcal{X} \otimes \mathcal{Y}$ of ρ and ξ satisfying $|\langle u, v \rangle| = F(\rho, \xi)$. (Cor 1 and Thm 3)

By the monotonicity of the trace norm, (Sec 2.3.2)

$\|\rho - \xi\|_1 \leq \|uu^* - vv^*\|_1$ — ①

Also, the trace norm of the difference of two pure states is evaluated as

$\|uu^* - vv^*\|_1 = 2\sqrt{1 - |\langle u, v \rangle|^2} = 2\sqrt{1 - F(\rho, \xi)^2}$ — ②

By ①, ②, $F(\rho, \xi) \leq \sqrt{1 - \frac{1}{4}\|\rho - \xi\|_1^2}$ $\blacksquare$