Purification and fidelity

1. Reductions, extensions, and purifications

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

$$\rho^X := \text{Tr}_Y(\rho) \quad \text{and} \quad \rho^Y := \text{Tr}_X(\rho)$$

and we call them the reduced states on $X$ and $Y$ or the reductions of $\rho$ to $X$ and $Y$.

**Def (Extensions):**

Let $\sigma \in D(X)$ be a state.

Then, a state $\rho \in D(X \otimes Y)$ is called an extension of $\sigma$ if $\sigma = \text{Tr}_Y(\rho)$.

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

**Def (purifications):**

Let $\rho \in D(X)$ be a state. A pure state $\rho = uu^*$ is called a purification of $\sigma$ if $\sigma = \text{Tr}_Y(\rho) = \text{Tr}_Y(uu^*)$.

In this case, $u \in X \otimes Y$ 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 $P \in \text{Pos}(X)$.

If there exists a vector $u \in X \otimes Y$ such that $P = \text{Tr}_Y(uu^*)$, $u$ (or $uu^*$) is called a purification of $P$.

**Eg** $X = Y = C^2$.

$u = \sum_{a \in \Sigma} e_a \otimes e_a$ is a purification of $1_X = \sum_{a \in \Sigma} e_a e_a^*$.

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

Then, $u = \sum_{i=1}^{\dim(X)} \sqrt{p_i} u_i u_i^*$ is a purification of $\Sigma$.

• Existence of purification \[\text{Sec 4.2}\]

**Thm 1**

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

Then, there exists a purification $u \in X \otimes Y$ of $P$ if and only if $\dim(Y) \geq \text{rank}(P)$. 
To show Thm1, we will use the following observation.

**Lem 1**

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

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

**proof**

$(1 \Rightarrow 2)$ Suppose that a purification $U$ of $P$ exists, that is, $P = \text{Tr}_y(UU^*)$. Recall the Vec function, $(\text{Vec} : L(Y, X) \rightarrow X \otimes Y, \text{Vec}(E_{a\omega}) = E_{a\omega \otimes e_0})$. Since Vec is bijective, there exists $A \in L(Y, X)$ such that $U = \text{Vec}(A)$. Since $P = \text{Tr}_y(UU^*) = \text{Tr}_y(\text{Vec}(A)\text{Vec}(A)^*) = AA^*$, $-(\star)$

We have statement 2.

$(2 \Rightarrow 1)$ Suppose that $A \in L(Y, X)$ with $P = AA^*$ exists. Define $U = \text{Vec}(A)$. By $(\star)$, $U$ serves as a purification of $P$. 

Sec 2.4 or F2023 lecture 1.8
Now, let's show Thm1.

Proof of Thm1

Suppose that a purification $U$ of $P$ exists.

By Lem1, $\text{A} \in L(Y \times X)$ with $P = \text{AA}^*$ exists.

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

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

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

$$P = \sum_{k=1}^{r} \lambda_k x_k x_k^*,$$

where $\lambda_k \geq 0$ for $k = 1, 2, \ldots, r$

$x_1, x_2, \ldots, x_r$: orthonormal vectors on $X$.

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

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

By Lem1, a purification $U$ of $P$ exists.

(Actually, we can take $U = \text{vec}(A)$ by the proof of Lem1)

$\therefore$

Thm1 implies that a purification always exists if $Y$ is sufficiently large.

Cor1

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

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

For the proof, observe $\dim(X) \geq \text{rank}(P) \forall P \in \text{Pos}(X)$.\]
Thm 2

Let \( X \) and \( Y \) be CES, and let \( U, V \in X \otimes Y \).

Assume that \( \text{Try}(U U^*) = \text{Try}(V V^*) \).

There exists a unitary operator \( U \in U(Y) \) such that \( U = (1_Y \otimes U) U \).

**proof**

Define \( P = \text{Try}(U U^*) = \text{Try}(V V^*) \in \text{Pos}(X) \).

Let \( A, B \in L(Y, X) \) be (unique) linear operators such that \( U = \text{Vec}(A) \) and \( V = \text{Vec}(B) \).

\[ AA^* = \text{Try}(U U^*) = P = \text{Try}(V V^*) = BB^* \]

\[ \text{rank}(A) = \text{rank}(P) = \text{rank}(B) =: r \]

Let \( p = \sum_{k=1}^{r} \lambda_k x_k x_k^* \) be a spectral decomposition.

(see Sec.2.1, for example)

Since \( AA^* = BB^* \), we can choose singular value decompositions

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

using some orthonormal sets of vectors \( \{y_1, \ldots, y_r\} \) and \( \{z_1, \ldots, z_r\} \)

Now, take a unitary operator \( V \in U(Y) \) such that \( V z_k = y_k \) for all \( k \).

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

where \( y_1, \ldots, y_{\dim(Y)} \) and \( z_1, \ldots, z_{\dim(Y)} \) are additional vectors

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

Take \( U = V^T \). Then \( (1_Y \otimes U) U = (1_Y \otimes V^T) \text{Vec}(A) = \text{Vec}(AV) = \text{Vec}(B) = V 

\[ \uparrow \quad \text{Al\&I} \quad \uparrow \]

\[ \text{(***)} \]
2. Fidelity function \[\text{Sec 4.3, 4.4}\]

A function that quantifies the similarity of two quantum states.

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

The **fidelity** between \( P \) and \( Q \) is defined as

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

**Obs.**

- \( F(P, Q) = F(Q, P) \) for any \( P, Q \in \operatorname{Pos}(X) \).
- \( F(u u^*, Q) = \sqrt{u^* Q u} \) for any \( u \in X \) and any \( Q \).
- \( F(u u^*, v v^*) = |\langle u, v \rangle| \) for any \( u, v \in X \).

**Prop (multiplicativity):**

Let \( X_1 \) and \( X_2 \) be CES, and let \( P_1, Q_1 \in \operatorname{Pos}(X_1) \) and \( P_2, Q_2 \in \operatorname{Pos}(X_2) \).

Then,

\[
F(P_1 \otimes P_2, Q_1 \otimes Q_2) = F(P_1, Q_1) F(P_2, Q_2).
\]

**proof**

\[
F(P_1 \otimes P_2, Q_1 \otimes Q_2) = \|\sqrt{P_1 \otimes P_2} \sqrt{Q_1 \otimes Q_2}\|_1
\]

\[
= \|\sqrt{P_1} \sqrt{P_2} \sqrt{Q_1} \sqrt{Q_2}\|_1
\]

\[
= \|\sqrt{P_1} \sqrt{Q_1} \sqrt{P_2} \sqrt{Q_2}\|_1
\]

\[
= \|\sqrt{P_1} \sqrt{Q_1}\|_1 \|\sqrt{P_2} \sqrt{Q_2}\|_1
\]

\[
= F(P_1, Q_1) F(P_2, Q_2).
\]
Characterizations of the fidelity function

**Thm 3 (Uhlmann's Theorem)**

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

Let $Y$ be a CES with $\dim(Y) \geq \max\{\text{rank}(P), \text{rank}(Q)\}$,

and let $U \in X \otimes Y$ be a purification of $P$. $\Leftarrow$ Existence of $U$ is ok by Thm 1.

Then, $F(P, Q) = \max \{ |\langle U, U' \rangle| : U \in X \otimes Y, \text{Tr}(U^* U) = 1 \}.$

**proof**

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

For example, let $P = \sum_{k=1}^{\text{rank}(P)} \lambda_k x_k x_k^*$, $Q = \sum_{k=1}^{\text{rank}(Q)} \eta_k y_k y_k^*$ be spectral decompositions.

Let $\{E_{1}, \ldots, E_{\text{rank}(P)}\}$ and $\{W_{1}, \ldots, W_{\text{rank}(Q)}\}$ be orthonormal bases for $X$ and $Y$, respectively.

Define $A = \sum_{k=1}^{\text{rank}(P)} E_k x_k^*$ and $B = \sum_{k=1}^{\text{rank}(Q)} W_k y_k^*$.

Since $\text{Tr}(\text{vec}(\sqrt{PA^*}) \text{vec}(\sqrt{PA^*})^*) = \sqrt{PA^* A} \sqrt{P} = P$

and $\text{Tr}(\text{vec}(\sqrt{QB^*}) \text{vec}(\sqrt{QB^*})^*) = \sqrt{QB^* B} \sqrt{Q} = Q$,

$\text{vec}(\sqrt{PA^*})$ and $\text{vec}(\sqrt{QB^*})$ are purifications of $P$ and $Q$, respectively.

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

$U = (1_x \otimes U) \text{vec}(\sqrt{PA^*}) = \text{vec}(\sqrt{PA^*} U^T)$.

Similarly, any purification $U \in X \otimes Y$ of $\mathbb{1}_X$ can be written as

$U = (1_x \otimes V) \text{vec}(\sqrt{QB^*}) = \text{vec}(\sqrt{QB^*} V^T)$

Using some $V \in U(Y)$.

Note that $(1_x \otimes V) \text{vec}(\sqrt{QB^*})$ is a purification of $\mathbb{1}_X$ for any $V \in U(Y)$, conversely.
(proof of Thm3, Cont'd)

\[
\max \left\{ |\langle u, v \rangle| : v \in \mathbb{X} \cap \mathbb{Y}, \text{Try}(v, u^*) = \emptyset \right\} = \max_{v \in \mathbb{U}(y)} \left| \langle \text{vec}(\sqrt{P} A^* u^T), \text{vec}(\sqrt{Q} B^* v^T) \rangle \right|
\]

\[
\langle \text{vec}(x), \text{vec}(y) \rangle = \langle x, y \rangle \rightarrow \max_{v \in \mathbb{U}(y)} \left| \langle \sqrt{P} A^* u^T, \sqrt{Q} B^* v^T \rangle \right|
\]  
(See 2.4)

\[
\langle AB, C \rangle = \langle A, C B^* \rangle \rightarrow \max_{v \in \mathbb{U}(y)} \left| \langle U^T v, \sqrt{A} \sqrt{B} \sqrt{Q} B^* \rangle \right|
\]

\[
\|x\|_1 = \max_{u \in \mathbb{X}(y)} |\langle u, x \rangle| \rightarrow \|A \sqrt{P} \sqrt{Q} B^*\|
\]  
(See 2.3.2)

Since \( \Pi_{\mathbb{U}(y)} = A^* A \), \( \Pi_{\mathbb{U}(x \cap \mathbb{Y})} = B^* B \), \( \|A\|_\infty, \|B\|_\infty \leq 1 \), and

\[
\|\sqrt{P} \sqrt{Q}\|_1 = \|\Pi_{\mathbb{U}(y)} \sqrt{P} \sqrt{Q} \Pi_{\mathbb{U}(x \cap \mathbb{Y})}\|_1 = \|A^* A \sqrt{P} \sqrt{Q} B^* B\|_1,
\]

\[
\|x \text{vec}(z)\|_1 \leq \|x\|_\infty \|\text{vec}(z)\|_\infty \leq \|A^* A \sqrt{P} \sqrt{Q} B^* B\| \leq \|A\|_\infty \|\sqrt{P} \sqrt{Q}\| \|B\|_\infty
\]  
(See 2.3.2)

\[
\|A \sqrt{P} \sqrt{Q} B^*\| \leq \|A\|_\infty \|\sqrt{P} \sqrt{Q}\| \|B\|_\infty \leq \|A\|_\infty \|\sqrt{P} \sqrt{Q}\| \|B\|_\infty
\]

\[
\|A \sqrt{P} \sqrt{Q} B^*\| = \|\sqrt{P} \sqrt{Q}\|_1, \quad \text{and}
\]

\[
\max \left\{ |\langle u, v \rangle| : v \in \mathbb{X} \cap \mathbb{Y}, \text{Try}(v, u^*) = \emptyset \right\} = \|A \sqrt{P} \sqrt{Q} B^*\|_1 = \|\sqrt{P} \sqrt{Q}\|_1 = F(P, Q) \tag{2}
\]

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 \( ho, \sigma \), \( 0 \leq F(\rho, \sigma) \leq 1 \).

\( F(\rho, \sigma) = 1 \) if and only if \( \rho = \sigma \), and
\( F(\rho, \sigma) = 0 \) if and only if \( \rho \oplus \sigma = 0 \).

Prop 2

Let \( X \) be a CES, and let \( \rho_1, \ldots, \rho_k, \sigma_1, \ldots, \sigma_k \in \text{Pos}(X) \).

Then, \( F\left( \sum_{j=1}^{k} \rho_j, \sum_{j=1}^{k} \sigma_j \right) \geq \sum_{j=1}^{k} F(\rho_j, \sigma_j) \).

Proof

Let \( Y \) be a CES with \( \dim(Y) \geq \dim(X) \).

By Thm 3, we can choose purifications \( U_1, U_2, \ldots, U_k, V_1, V_2, \ldots, V_k \in X \otimes Y \)

of \( \rho_1, \rho_2, \ldots, \rho_k, \sigma_1, \ldots, \sigma_k \) with \( \langle U_j, V_j \rangle = F(\rho_j, \sigma_j) \).

Let \( Z = C^k \), and define \( u, v \in X \otimes Y \otimes Z \) 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 \( \text{Tr}_{Y \otimes Z}(uu^*) = \sum_{j=1}^{k} \text{Tr}(U_j V_j^*) = \sum_{j=1}^{k} \rho_j \)

\( \text{Tr}_{Y \otimes Z}(vv^*) = \sum_{j=1}^{k} \sigma_j \),

\( u, v \) are purifications of \( \sum_{j=1}^{k} \rho_j = \sum_{j=1}^{k} \sigma_j \), respectively.

By Thm 3,

\[ F\left( \sum_{j=1}^{k} \rho_j, \sum_{j=1}^{k} \sigma_j \right) \geq |\langle u, v \rangle| \]

\[ = \left| \sum_{j=1}^{k} \langle u_j, v_j \rangle \right| \]

\[ = \left| \sum_{j=1}^{k} F(\rho_j, \sigma_j) \right| = \sum_{j=1}^{k} F(\rho_j, \sigma_j) \]

Cor 2

\[ F(\lambda \rho_1 + (1-\lambda) \rho_2, \lambda \sigma_1 + (1-\lambda) \sigma_2) \geq \lambda F(\rho_1, \sigma_1) + (1-\lambda) F(\rho_2, \sigma_2) \]

for all \( \rho_1, \rho_2, \sigma_1, \sigma_2 \in \text{Pos}(X) \) and \( 0 \leq \lambda \leq 1 \).
Thm 4

Let \( X \) be a CES, and let \( P, Q \in \text{Pos}(X) \), the set of positive "definite" operators on \( X \).

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

**proof**

The proof consists of 3 steps.

1. \( P = Q \rightarrow F(P, P) \)

In this case, we show \( \text{Tr}(P) = \inf \left\{ \frac{1}{2} \langle P, Y \rangle + \frac{1}{2} \langle P, Y^* \rangle : Y \in \text{Pd}(X) \right\} \).

Observe that

\[
(*) \leq \frac{1}{2} \text{Tr}(P) + \frac{1}{2} \text{Tr}(P) = \text{Tr}(P).
\]

By taking \( Y = 1_X \)

Thus, it suffices to show \( (*) \geq \text{Tr}(P) \).

For this purpose, we show \( \frac{1}{2} \langle P, Y \rangle + \frac{1}{2} \langle P, Y^* \rangle \geq \text{Tr}(P) \) for all \( Y \in \text{Pd}(X) \).

Observe that \( \frac{Y + Y^*}{2} - 1_X = \frac{1}{2} \left( Y^{1/2} - Y^{-1/2} \right)^2 \in \text{Pos}(X) \).

\[
\langle P, \frac{Y + Y^*}{2} - 1_X \rangle \geq 0,
\]

and thus \( \frac{1}{2} \langle P, Y \rangle + \frac{1}{2} \langle P, Y^* \rangle \geq \langle P, 1_X \rangle = \text{Tr}(P) \).
(Proof of Thm 4, cont’d)

2. \( P, Q \in \text{Pd}(X) \).

Define \( R := \sqrt{PQ} \sqrt{P} \) and
\[
Z := R^{-\frac{1}{2}} \sqrt{P} \ Y \sqrt{P} \ R^{-\frac{1}{2}}.
\]

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
\[
\langle R, Z^{-1} \rangle = \langle R, R^{-\frac{1}{2}} P^{-\frac{1}{2}} Y^{-1} P^{-\frac{1}{2}} R^{-\frac{1}{2}} \rangle
\]
\[
= \langle P^{-\frac{1}{2}} R^2 P^{-\frac{1}{2}}, Y^{-1} \rangle = \langle P, Y^{-1} \rangle
\]
\[
\sqrt{PQ} \sqrt{P}
\]

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

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

\[
\text{Step 1}
\]
(Proof of Thm 4, cont'd)

3. General Case (P, Q ∈ Pos(X))

Let ε > 0 be an arbitrary positive real number.

We have \[ \frac{1}{2} <P, Y> + \frac{1}{2} <Q, Y'> < \frac{1}{2} <P + ε I_x, Y> + \frac{1}{2} <Q + ε I_x, Y'> \]

Since Tr(Y), Tr(Y') > 0.

Taking the infimum over all Y ∈ Pd(x), by Step 2,

\[ \inf_{Y ∈ Pd(x)} \left[ \frac{1}{2} <P, Y> + \frac{1}{2} <Q, Y'> \right] < F(P + ε I_x, Q + ε I_x) - (****) \]

Since (****) holds for all ε > 0,

Considering the continuity of the fidelity, \( F(P, Q) = \|PQ\|_1 \)

\[ \inf_{Y ∈ Pd(x)} \left[ \frac{1}{2} <P, Y> + \frac{1}{2} <Q, Y'> \right] \leq F(P, Q) - 0 \]

\[ \text{Take the limit } \varepsilon \to 0 \]

On the other hand, for any Y ∈ Pd(x) and any ε > 0,

\[ \frac{1}{2} <P + ε I_x, Y> + \frac{1}{2} <Q + ε I_x, Y'> \geq F(P + ε I_x, Q + ε I_x) \]

By taking ε → 0 on both sides, by continuity of fidelity and inner product,

\[ \frac{1}{2} <P, Y> + \frac{1}{2} <Q, Y'> \geq F(P, Q) \]

By taking the infimum over all Y ∈ Pd(x),

\[ \inf_{Y ∈ Pd(x)} \left[ \frac{1}{2} <P, Y> + \frac{1}{2} <Q, Y'> \right] \geq F(P, Q) - (2) \]

1 and 2 yield the desired expression.
Cor 2 (Alberti's Theorem)

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

Then, \[ F(P, Q)^2 = \inf \left \{ \langle P, Y \rangle \langle Q, Y^{-1} \rangle : Y \in Pd(X) \right \} \]

(****)  

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

\[ \Rightarrow \quad \text{By Thm 4,} \]

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

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

\[ = F(P, Q)^2 \]
(Proof of Cor 2, cont'd)

On the other hand, observe that

$$\sqrt{\langle p, y \rangle \langle q, y \rangle} = \sqrt{\langle p, dy \rangle \langle q, (dy)^{-1} \rangle}$$

for any $p \in Pd(x)$ and $d \neq 0$.

For $d = \frac{\langle q, y \rangle}{\sqrt{\langle p, y \rangle}}$, we have

$$\langle p, dy \rangle = \langle q, (dy)^{-1} \rangle = \sqrt{\langle p, y \rangle \langle q, y^{-1} \rangle}.$$

For this choice of $d$, the arithmetic mean and the geometric mean of $\langle p, dy \rangle$ and $\langle q, (dy)^{-1} \rangle$ become equal. (For $a, b \geq 0$, $\sqrt{ab} = \frac{a+b}{2}$ iff $a = b$)

$$\sqrt{\langle p, y \rangle \langle q, y^{-1} \rangle} = \frac{1}{2} \langle p, dy \rangle + \frac{1}{2} \langle q, (dy)^{-1} \rangle \geq F(p, q)$$

Using Thm 4

Since $dy \in Pd(x)$.

$$(***) = \inf_{y \in Pd(x)} \left[ \langle p, y \rangle \langle q, y^{-1} \rangle \right] \geq F(p, q)^2$$

**Note:** In Textbook, another proof of Thm 4 is also shown, which makes use of Semi definite programming (SDP).

In fact, Thm 3 and Thm 4 are related by the property called "strong duality", which is an important concept of SDP.
Fuchs-Van de Graaf inequality

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

We first show the following technical lemma.

\textbf{Lemma 2}

Let $\mathbf{x}$ be a CES, and let $P, Q \in \text{Pos}(X)$.

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

\textbf{Proof}

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

\[ \|\sqrt{P} - \sqrt{Q}\|_2^2 = \sum_{j=1}^{\text{dim}(X)} |\lambda_j|^2. \] \hfill (1)

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

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

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

\[ \|P - Q\|_1 \geq \frac{1}{2} \left| \text{Tr}[(P - Q)U] \right| \]

\[ = \frac{1}{2} \left| \sum_{j=1}^{\text{dim}(X)} \lambda_j |x_j y_j|^2 (\sqrt{P} + \sqrt{Q}) x_j^* \right| \\
\geq \sum_{j=1}^{\text{dim}(X)} |\lambda_j| |x_j y_j^*|^2 \\
= \sum_{j=1}^{\text{dim}(X)} |\lambda_j|^2 \\
= \|\sqrt{P} - \sqrt{Q}\|_2^2. \] \hfill (4)
Theorem (Fuchs–van de Graaf)
Let \( X \) be a CES, and let \( \rho, 3 \in D(X) \) be states.
Then, 
\[
1 - \frac{1}{2} \| 3 - \rho \|_1 \leq F(\rho, 3) \leq \sqrt{1 - \frac{1}{4} \| 3 - \rho \|_1^2}
\]

Proof
First, we show the left-side inequality.
Observe that 
\[
\| \sqrt{\rho} - \sqrt{3} \|_2^2 = \text{Tr} \left[ (\sqrt{\rho} - \sqrt{3})^2 \right] = \text{Tr} \left[ \rho + 3 - \sqrt{\rho} \sqrt{3} - \sqrt{3} \sqrt{\rho} \right] 
= 2 - 2 \text{Tr} \left[ \sqrt{\rho} \sqrt{3} \right] = 2 - 2 F(\rho, 3).
\]
Since \( \| 3 - \rho \|_1 \geq \| \sqrt{\rho} - \sqrt{3} \|_2 \) by Lem 2,
We have \( \| 3 - \rho \|_1 \geq 2 - 2 F(\rho, 3) \), which is equivalent to the desired inequality.

Next, we show the right-side inequality.
Let \( Y \) be a CES with \( \dim(Y) \geq \dim(X) \), and take purifications \( u, v \) of \( \rho \) and \( 3 \) satisfying \( \langle u, v \rangle = F(\rho, 3) \). (Cor 1 and Thm 3)

By the monotonicity of the trace norm, (Sec 2.3.2)
\[
\| \rho - 3 \|_1 \leq \| u^* v - v^* u \|_1 - 0
\]
Also, the trace norm of the difference of two pure states is evaluated as
\[
\| u^* v - v^* u \|_1 = 2 \sqrt{1 - |\langle u, v \rangle|^2} = 2 \sqrt{1 - F(\rho, 3)^2} - 2
\]
By \( 0, 2 \), \( F(\rho, 3) \leq \sqrt{1 - \frac{1}{4} \| 3 - \rho \|_1^2} \)