QUANTUM STATES

Operations on sets

Let Σ and Γ be finite sets.

1) Direct product

$$\Sigma \times \Gamma = \{ (a,b) : a \in \Sigma, b \in \Gamma \}$$

2) Disjoint union $\Sigma \sqcup \Gamma$ consisting of $a \in \Sigma$ and $b \in \Gamma$.

More formally

$$\Sigma \sqcup \Gamma = \{ (a,0), (b,1) : a \in \Sigma, b \in \Gamma \}$$

3) Set of functions

$$F(\Sigma, \Gamma) = \{ f : \Sigma \to \Gamma \}$$

A function $f : \Sigma \to \Gamma$ is called a bijection if it is one-to-one and onto. In this case we write $\Sigma \cong \Gamma$.

Ex: $\Sigma \cong \{0, 1, \dots, |\Sigma| - 1\}$ where $|\Sigma|$ denotes the size of the set.

Registers

A register is an abstraction of a physical system on which data can be stored.

Each register has associated to it a set Σ of classical states:

$$\boxed{a \in \Sigma}$$

Given two registers we can form the compound register:

$$\boxed{\boxed{a \in \Sigma} \quad \boxed{b \in \Gamma}}$$

The set of classical states of the compound register is given by $\Sigma \times \Gamma$.

Hilbert spaces

In quantum information theory we associate the Hilbert space $\mathbb{C}\Sigma$ to a register with a set Σ of classical states. The Hilbert space $\mathbb{C}\Sigma$ has basis given by

$$\{ \underbrace{|a\rangle}_{\text{ket}} : a \in \Sigma \}.$$

A vector $v \in \mathbb{C}\Sigma$ is of the form

$$|v\rangle = \sum_{a\in\Sigma} \alpha_a |a\rangle, \quad \alpha_a \in \mathbb{C}.$$

Vector space structure

1) Addition:

$$u + v = \sum_{a\in\Sigma} \beta_a |a\rangle + \sum_{a\in\Sigma} \alpha_a |a\rangle$$

$$= \sum_{a\in\Sigma} (\beta_a + \alpha_a) |a\rangle$$

where $|u\rangle = \sum_a \beta_a |a\rangle$.

2) Scalar multiplication:

$$\alpha v = \sum_{a\in\Sigma} \alpha \alpha_a |a\rangle.$$

The inner product on $\mathbb{C}\Sigma$ is defined by

$$\langle u, v \rangle = \sum_{a \in \Sigma} \overline{\beta_a} \, \alpha_a$$

Note that

1) $\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle$

2) $\langle u, v \rangle = \overline{\langle v, u \rangle}$

3) $\langle u, u \rangle \geq 0$ and $\langle u, u \rangle = 0$ if and only if $u = 0$.

In Dirac notation we write $\langle u | v \rangle$.

The standard basis $\{ |a\rangle : a \in \Sigma \}$ is orthonormal:

$$\langle a | b \rangle = \delta_{ab} = \begin{cases} 1 & a = b \\ 0 & \text{otherwise.} \end{cases}$$

The norm of $v \in \mathbb{C}\Sigma$ is defined by

$$\| v \| = \sqrt{\langle v, v \rangle} .$$

<u>Lem</u>: Norm determines the inner product:

$$\langle u, v \rangle = \frac{\| u + v \|^2 - \| u - v \|^2 + \| u + iv \|^2 i - \| u - iv \|^2 i}{4}$$

exercise

In general, a Hilbert space is a vector space V together with an inner product

$$\langle -, - \rangle : V \times V \longrightarrow \mathbb{C}.$$

Let $S = \{ v_a : a \in \Sigma \} \subset V$.

We say S is linearly independent if $\exists \{ \alpha_a \in \mathbb{C} \}_{a \in \Sigma}$ not all zero such that

$$\sum_{a \in \Sigma} \alpha_a v_a = 0.$$

The subspace

$$\mathrm{Span}(S) = \left\{ \sum_{a \in \Sigma} \alpha_a v_a : \alpha_a \in \mathbb{C} \right\}$$

is called the span of S.

If $\mathrm{Span}(S) = V$ then we say S is spanning.

A linearly independent spanning set is called a basis.

Every vector space comes with a basis $\{ v_a : a \in \Sigma \}$.

The dimension of V is defined by

$$\dim V = |\Sigma| .$$

The set S is called orthogonal if

$$\langle v_a, v_b \rangle = 0 \quad \forall \ a \neq b$$

and orthonormal if

$$\langle v_a, v_b \rangle = \delta_{ab} = \begin{cases} 1 & a = b \\ 0 & \text{otherwise.} \end{cases}$$

We can identify $\Sigma \cong \{0, 1, .., |\Sigma| - 1\}$.

A basis $\{ v_i : i = 0, 1, .., |\Sigma| - 1 \}$ can be converted to an orthonormal basis by using the Gram-Schmidt procedure:

$$\tilde{v}_0 = \frac{1}{\|v_1\|} v_0$$

$$\tilde{v}_k = \frac{v_k - \sum_{i=0}^{k-1} \langle \tilde{v}_i, v_k \rangle \tilde{v}_i}{\| v_{k+1} - \sum_{i=0}^{k-1} \langle v_i, v_k \rangle \tilde{v}_i \|}$$

where $0 \leq k \leq |\Sigma| - 1$.

The set $\{\vec{v}_i\}$ is orthonormal:

$$\langle \vec{v}_i , \vec{v}_j \rangle = \delta_{ij} .$$

HW: Verify this.

Cauchy - Schwarz inequality

$$|\langle u, v\rangle| \leq \|u\| \, \|v\| \quad \forall \, u, v \in V$$

with equality if and only if u and v linearly dependent.

Proof in the Appendix.

Linear operators

A linear operator (map) $A: V \longrightarrow W$ is a function such that

$$A(\alpha v + \beta u) = \alpha A v + \beta A u.$$

We will write $L(V, W)$ for the set of linear operators.

$L(V, W)$ is a vector space:

1) $A + B$ is the linear operator defined by

$$(A+B)(v) = Av + Bv$$

2) αA is defined by

$$(\alpha A)(v) = \alpha A(v),$$

Ex: The zero operator

$$\mathbb{O} : V \longrightarrow V$$

$$\mathbb{O}(v) = 0 \qquad \forall v \in V$$

The identity operator

$$\mathbb{1} : V \longrightarrow V$$

$$\mathbb{1}(v) = v \qquad \forall v \in V$$

Let $\{v_a : a \in \Sigma\}$ and $\{w_b : b \in \Gamma\}$ be orthonormal basis for V and W.

A linear operator $A : V \longrightarrow W$ is uniquely specified by

$$A v_b = \sum_{a \in \Gamma} \langle w_a , A v_b \rangle w_a .$$

The coefficients can be assembled into a function

$$A : \Gamma \times \Sigma \longrightarrow \mathbb{C}$$
$$A(a,b) = \langle w_a , A v_b \rangle .$$

We call this function the matrix representation. In matrix representation the composition of $A : \Lambda \times \Sigma \longrightarrow \mathbb{C}$ and $B : \Gamma \times \Lambda \longrightarrow \mathbb{C}$ is given by

$$BA : \Gamma \times \Sigma \longrightarrow \mathbb{C}$$

$$BA(a,b) = \sum_{c \in \Lambda} B(a,c) A(c,b) .$$

We can convert $A : \Gamma \times \Sigma \longrightarrow \mathbb{C}$ to an ordinary matrix by choosing

$$\Sigma \cong \{0, 1, \dots, |\Sigma| - 1\}$$

$$\Gamma \cong \{0, 1, \dots, |\Gamma| - 1\}.$$

Then composition of operators is given by the usual matrix multiplication.

The standard basis of $L(V, W)$ consists of $\{E_{ab} : a \in \Sigma,\ b \in \Gamma\}$ defined by

$$E_{ab} : \Gamma \times \Sigma \longrightarrow \mathbb{C}$$

$$E_{ab}(c,d) = \delta_{(a,b),(c,d)}$$

$$= \begin{cases} 1 & (c,d) = (a,b) \\ 0 & \text{otherwise.} \end{cases}$$

As an ordinary matrix

$$E_{ij} = \begin{array}{cc} \begin{pmatrix} 0 & & 0 \\ & 1 & \\ 0 & & 0 \end{pmatrix} & i \\ j & \end{array}$$

Linear isometry

A linear operator $A : V \to W$ is called a linear isometry if

$$\| A v \| = \| v \| \qquad \forall\, v \in V.$$

We will write $U(V, W)$ for the set of linear isometries.

We say V is isomorphic to W if there exists a linear isometry $A : V \to W$ and $\dim V = \dim W$.

Ex: 1) Choosing a basis gives an isomorphism

$$V \cong \mathbb{C}\Sigma.$$

2) $\mathbb{C}^{\Sigma} = F(\Sigma, \mathbb{C})$ is a Hilbert space with basis given by the functions

$$e_a : \Sigma \to \mathbb{C}$$

$$e_a(b) = \delta_{ab} = \begin{cases} 1 & a = b \\ 0 & \text{otherwise.} \end{cases}$$

The linear operator

$$\mathbb{C}^{\Sigma} \longrightarrow \mathbb{C}\Sigma$$
$$e_a \longmapsto |a\rangle$$

gives an isomorphism $\mathbb{C}^{\Sigma} \cong \mathbb{C}\Sigma$.

3) Matrix representation gives an isomorphism:

$$L(\mathbb{C}^{\Sigma}, \mathbb{C}^{\Gamma}) \cong \mathbb{C}^{\Gamma \times \Sigma}.$$

Pro: For $A \in L(V,W)$ the following are equivalent.

1) A is a linear isometry.

2) $\langle Av, Au\rangle = \langle v, u\rangle \quad \forall v,u \in V$.

Proof: $(1 \Rightarrow 2)$ This follows from the fact that the inner product is determined from the norm.

$(2 \Rightarrow 1)$ Take $u = v$. $\boxtimes$

HW: Write a more detailed proof for $(1 \Rightarrow 2)$.

The adjoint of a linear operator $A : V \to W$ is the linear operator

$$A^+ : W \to V$$

uniquely specified by the equation

$$\langle w, Av \rangle = \langle A^+ w, v \rangle$$

for all $v \in V$, $w \in W$.

Pro: The matrix representation of A^+ is given by $A^+(a,b) = \overline{A(b,a)}$.

Proof: We have

$$A^+(a,b) = \langle w_a, A^+ v_b \rangle$$

$$= \overline{\langle A^+ v_b, w_a \rangle}$$

$$= \overline{\langle v_b, A w_a \rangle}$$

$$= \overline{A(b,a)}. \qquad \boxtimes$$

Notation: Transpose of a matrix

$$A^T(a,b) = A(b,a)$$

Conjugate of a matrix

$$\bar{A}(a,b) = \overline{A(a,b)}$$

A^+ is the conjugate transpose of A.

A vector $v \in V$ can be regarded as a linear operator

$$\begin{aligned} v : \mathbb{C} &\longrightarrow V \\ 1 &\longmapsto v \end{aligned}$$

Then the adjoint is the linear operator

$$v^+ : V \longrightarrow \mathbb{C}$$

given by

$$\begin{aligned} v^+(u) &= \langle 1, v^+(u) \rangle \\ &= \overline{\langle v^+(u), 1 \rangle} \\ &= \overline{\langle u, v(1) \rangle} \\ &= \overline{\langle u, v \rangle} = \langle v, u \rangle . \end{aligned}$$

Using this construction we can define a linear operator:

$$w v^+ : V \longrightarrow W .$$

This means that the composition of $v^+ : V \to \mathbb{C}$ and $w : \mathbb{C} \longrightarrow W$:

$$\begin{aligned} w v^+(u) &= w(\langle v, u \rangle) \\ &= \langle v, u \rangle w . \end{aligned}$$

In Dirac notation $v^\dagger$ is denoted by a bra $\langle v|$.

Then

$$\langle v|(|u\rangle) = \underbrace{\langle v|u\rangle}_{\text{Inner product in Dirac notation.}}.$$

The operator $wv^\dagger$ is written as $|w\rangle\langle v|$ and

$$\begin{aligned} |w\rangle\langle v|\,(|u\rangle) &= |w\rangle\,\langle v|w\rangle \\ &= \langle v|w\rangle\,|w\rangle . \end{aligned}$$

The basis operators E_{ab} will be denoted by $|a\rangle\langle b|$.

For $A : V \longrightarrow W$ we can write

$$A = \sum_{a,b} A(a,b)\ |a\rangle\langle b| .$$

Pro: $(A^+)^+ = A$

$(BA)^+ = A^+ B^+$.

HW: Prove this.

Pro: A is an isometry if and only if $A^+ A = \mathbb{1}_V$.

Proof: We have

$$\langle Av, Au \rangle = \langle v, u \rangle$$

if and only if

$$\langle A^+ A v, u \rangle = \langle v, u \rangle$$

which implies that $A^+ A = \mathbb{1}_V$. $\boxtimes$

When $V = W$ we will write $U(V)$ for $U(V, V)$.

$U(V)$ has the structure of a group:

1) $A, B \in U(V)$ then $AB \in U(V)$

2) $\mathbb{1}_V$ is the identity element:

$$A \mathbb{1}_V = \mathbb{1}_V A = A \quad , \quad \forall A$$

3) Every $A \in U(V)$ has an inverse:

$$A^+ A = A^+ A = \mathbb{1}_V$$

Direct sum

The direct sum of $\mathbb{C}\Lambda$ and $\mathbb{C}\Gamma$ is the defined as the vector space

$$\mathbb{C}\Lambda \oplus \mathbb{C}\Gamma = \mathbb{C}[\Lambda \sqcup \Gamma].$$

A vector in $\mathbb{C}\Lambda \oplus \mathbb{C}\Gamma$ can be uniquely expressed as

$$v = \sum_{a\in\Lambda} \alpha_a |a\rangle + \sum_{b\in\Gamma} \beta_b |b\rangle .$$

For a subspace $W \subset V$ we write

$$W^\perp = \{ v \in V : \langle w, v\rangle = 0, \ \forall w \in W \}$$

Pro: $V \cong W \oplus W^\perp$.

Proof: Choose an orthonormal basis $\{ w_a : a \in \Lambda \}$ for W and extend it to an orthonormal basis

$$\{ w_a : a \in \Lambda \} \sqcup \{ u_b : b \in \Gamma \}$$

for V. Then $W \cong \mathbb{C}\Lambda$, $W^\perp \cong \mathbb{C}\Gamma$ and $V \cong \mathbb{C}\Sigma$ where $\Sigma = \Lambda \sqcup \Gamma$. $\boxed{\checkmark}$

Cor: $(W^\perp)^\perp = W$.

The kernel of A is defined by

$$\ker A = \{ v \in V : Av = 0 \}$$

and the image of A is defined by

$$\operatorname{im} A = \{ Av \in W : v \in V \}.$$

We have

$$\dim V = \dim(\operatorname{im} A) + \dim(\ker A)$$

The dimension of the image is called the rank of A:

$$\operatorname{rank}(A) = \dim(\operatorname{im} A).$$

<u>Pro</u>: $\ker A^+ = (\operatorname{im} A)^\perp$

<u>Proof</u>: For $w \in W$ we have

$$\begin{aligned} A^+ w = 0 &\iff \langle A^+ w, v \rangle = 0 \quad \forall v \in V \\ &\iff \langle w, Av \rangle = 0 \quad \forall v \in V \\ &\iff w \in (\operatorname{im} A)^\perp. \quad \blacksquare \end{aligned}$$

Cor: $\operatorname{im} A = \operatorname{im} AA^t$.

Proof: We will show that

$$\ker A^t = \ker AA^t.$$

Then the result follows from the Proposition:

$$\operatorname{im} A = (\ker A^t)^\perp = (\ker AA^t)^\perp = \operatorname{im} AA^t.$$

We have

$$\ker A^t \subset \ker AA^t:$$

if $A^t w = 0$ then $AA^t w = 0$.

For the converse let $w \in \ker AA^t$, that is, $AA^t w = 0$.

This implies that

$$A^t w \in \ker A = (\operatorname{im} A^t)^\perp.$$

Therefore

$$\langle A^t w, v \rangle = 0 \quad \forall v \in \operatorname{im} A^t.$$

Thus $A^t w = 0$ and $w \in \ker A^t$.

$\boxtimes$

Trace

We will write $L(V)$ for $L(V,V)$.

Trace is the linear operator

$$\mathrm{Tr}: L(V) \longrightarrow \mathbb{C}$$

uniquely determined by

$$\mathrm{Tr}(|u\rangle\langle v|) = \langle v|u\rangle .$$

Pro: In matrix representation

$$\mathrm{Tr}(A) = \sum_{a\in\Sigma} A(a,a)$$

Proof: We have

$$\mathrm{Tr}(A) = \mathrm{Tr}\Big(\sum_{a,b} A(a,b)\, |a\rangle\langle b|\Big)$$

$$= \sum_{a,b} A(a,b)\, \mathrm{Tr}(|a\rangle\langle b|)$$

$$= \sum_{a,b} A(a,b)\, \underbrace{\langle b|a\rangle}_{\delta_{ab}}$$

$$= \sum_{a} A(a,a) . \qquad \blacksquare$$

Cor: $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

HW: Prove this.

$L(V,W)$ is a Hilbert space:

Hilbert–Schmidt (Frobenius) inner product

$$\langle A, B\rangle = \mathrm{Tr}(A^{+}B).$$

The standard basis $\{\, |a\rangle\langle b| \,\}$ is orthonormal:

$$\langle\, |c\rangle\langle d| \,,\, |a\rangle\langle b| \,\rangle = \mathrm{Tr}\big(\, |d\rangle \overbrace{\langle c| \;\, |a\rangle}^{\langle c|a\rangle} \langle b| \,\big)$$

$$= \delta_{ca}\, \delta_{bd}$$

$$= \delta_{(c,d),(a,b)}.$$

Pro: The adjoint of Tr is the linear operator $\mathbb{1}_V : \mathbb{C} \longrightarrow L(V)$.

Proof: We have

$$\mathrm{Tr}^{+}(1) = \sum_{a,b} \langle\, |a\rangle\langle b| \,,\, \mathrm{Tr}^{+}(1) \rangle \, |a\rangle\langle b|$$

$$= \sum_{a,b} \langle\, \mathrm{Tr}\big(|a\rangle\langle b|\big) \,,\, 1 \rangle \, |a\rangle\langle b|$$

$$= \sum_{a} |a\rangle\langle a|$$

$$= \mathbb{1}_V$$

$\square$

Classes of operators

$L(V)$

Normal operators

$$\mathrm{Nor}(V) = \{ A \in L(V) : A^\dagger A = A A^\dagger \}$$

Unitary operators

$U(V)$

Hermitian operators

$$\mathrm{Her}(V) = \{ A \in L(V) : A = A^\dagger \}$$

Positive operators

$$\mathrm{Pos}(V) = \{ B^\dagger B : B \in L(V) \}$$

Projection operators

$$\mathrm{Proj}(V) = \{ \Pi \in \mathrm{Pos}(V) : \Pi^2 = \Pi \}$$

Density operators

$$\mathrm{Den}(V) = \{ \rho \in \mathrm{Pos}(V) : \mathrm{Tr}(\rho) = 1 \}$$

Quantum states

Pure states

$$P(V) = \{ \Pi \in \mathrm{Proj}(V) : \mathrm{Tr}(\Pi) = 1 \}$$

A nonzero vector $v \in V$ is called an eigenvector corresponding to $\lambda \in \mathbb{C}$ if $Av = \lambda v$.

The number λ is called an eigenvalue.

Eigenspace corresponding to λ:

$$V_\lambda = \{ v \in V : Av = \lambda v \} \cup \{0\}.$$

Eigenvalues are the roots of the characteristic polynomial

$$\det (A - \mathbb{1}_V).$$

Note that there is at least one nonzero solution.

<u>S</u>pectral decomposition theorem

Let $A \in \mathrm{Nor}(\mathbb{C}^\Sigma)$.

Then there exists an orthonormal basis $\{ |v_a\rangle : a \in \Sigma \}$ such that

$$A = \sum_{a \in \Sigma} \lambda_a |v_a\rangle\langle v_a| .$$

Proof in the Appendix.

A matrix $D : \Sigma \times \Sigma \to \mathbb{C}$ is called diagonal if $D(a,b) = 0$ when $a \neq b$.

Cor: If $A \in \mathrm{Nor}(\mathbb{C}\Sigma)$ then there exists $U \in U(\mathbb{C}\Sigma)$ such that

$$U A U^{\dagger} \text{ is diagonal.}$$

Proof: By the spectral theorem:

$$A = \sum_{a \in \Sigma} \lambda_a |v_a\rangle\langle v_a| .$$

Let U be defined by

$$U|v_a\rangle = |a\rangle.$$

Then

$$U A U^{\dagger} = \sum_a \lambda_a \, U|v_a\rangle\langle v_a| U^{\dagger}$$

$$= \sum_a \lambda_a |a\rangle\langle a| \qquad \blacksquare$$

We say A is unitarily diagonalizable if there exists $U \in U(\mathbb{C}\Sigma)$ such that $U A U^{\dagger}$ is diagonal.

Characterizations of positive operators

The following are equivalent.

1) $\langle v, Pv \rangle \in \mathbb{R}_{\geq 0} \quad \forall v \in V$.

2) $P \in \mathrm{Herm}(V)$ and eigenvalues of P belong to $\mathbb{R}_{\geq 0}$.

3) $P = A^{+} A$ for some $A \in L(V)$.

4) $\langle Q, P \rangle \in \mathbb{R}_{\geq 0} \quad \forall Q \in \mathrm{Pos}(V)$.

Proof: $(1 \Rightarrow 2)$ By spectral decomposition:

$$P = \sum_{a \in \Sigma} \lambda_a |v_a\rangle\langle v_a|$$

We have $\lambda_a = \langle v_a, P v_a \rangle \in \mathbb{R}_{\geq 0}$.

P is hermitian since its eigenvalues are real.

$(2 \Rightarrow 3)$ Let $A = \sum_a \sqrt{\lambda_a} \, |v_a\rangle\langle v_a|$.

Then $P = A^{+} A$.

$(3 \Rightarrow 4)$ We can write $Q = B^{+} B$.

Then $\langle Q, P \rangle = \mathrm{Tr}(QP)$

$$= \mathrm{Tr}(B^{+} B A^{+} A)$$

$$= \mathrm{Tr}(B A^{+} (B A^{+})^{+})$$

$$= \langle B A^{+}, B A^{+} \rangle \in \mathbb{R}_{\geq 0}$$

$(4 \Rightarrow 1)$ Take $Q = |v\rangle\langle v|$. $\boxtimes$

Polar decomposition theorem:

For $A \in L(V,W)$ we have

$$A = U\sqrt{A^+ A}$$ (left polar decomposition)

for some $U \in U(V,W)$.

Proof in the Appendix. (There is also right polar decomposition $A = \sqrt{A A^+}\, U$.)

Cor (Singular value theorem):

Let $A \in L(V,W)$ be a nonzero linear operator such that $\mathrm{rank}(A) = r$.

Then there exist orthonormal sets

$\{v_a : a \in \Lambda\} \subset V$ and

$\{w_a : a \in \Lambda\} \subset W$ such that

$$A = \sum_{a \in \Lambda} s_a |w_a\rangle\langle v_a|$$

where $|\Lambda| = r$ and $s_a \in \mathbb{R}_{>0}$.

Proof: Since $A^+A \in \mathrm{Pos}(V)$, by the spectral decomposition we have

$$A^+A = \sum_{a \in \Lambda} \lambda_a |v_a\rangle\langle v_a|.$$

where $\lambda_a \in \mathbb{R}_{>0}$.

Then

$$A = U\sqrt{A^+A} = \sum_{a \in \Lambda} \underbrace{\sqrt{\lambda_a}}_{s_a}\, \underbrace{U|v_a\rangle}_{|w_a\rangle}\langle v_a|$$

include: UDV $\square$

Quantum states

We have seen that a register comes with a set Σ of classical states.
A probabilistic state on the register is a probability distribution, i.e., a function

$$p : \Sigma \to \mathbb{R}_{\geq 0}$$

such that $\displaystyle\sum_{a \in \Sigma} p(a) = 1$.

We will write $\mathrm{Dist}(\Sigma)$ for the set of probability distributions on Σ.

In quantum information theory states of registers are represented by quantum states.

A quantum state is a density operator of the form $\rho \in \mathrm{Den}(\mathbb{C}^{\Sigma})$.
By spectral decomposition

$$\rho = \sum_{a \in \Sigma} p_a |v_a\rangle\langle v_a|$$

where $p_a \geq 0$ and $\displaystyle\sum_a p_a = 1$.

That is $p : \Sigma \to \mathbb{R}_{\geq 0}$ defined by $p(a) = p_a$ is a probability distribution.

A probabilistic state p can be regarded as a quantum state represented by a diagonal density operator.

A quantum state is said to be pure if $\rho^2 = \rho$.

Pro: Every pure state is of the form $|v\rangle\langle v|$ for some unit vector $v \in V$.

Moreover,

$$|v\rangle\langle v| = |u\rangle\langle u|$$

if and only if $u = \alpha v$ for some $\alpha \in U(\mathbb{C})$.

HW: Prove this.

An ensemble of states is a function

$$\eta : \Gamma \longrightarrow \mathrm{Pos}(\mathbb{C}\Sigma)$$

satisfying $\mathrm{Tr}\left(\sum_{a \in \Gamma} \eta(a) \right) = 1$.

Note that

$$\begin{aligned} p : \Gamma &\longrightarrow \mathbb{R}_{\geq 0} \\ a &\longmapsto \mathrm{Tr}(\eta(a)) \end{aligned}$$

is a probability distribution.

Given $\rho \in \mathrm{Den}(\mathbb{C}\Sigma)$ we have

$$\rho = \sum_{a \in \Sigma} \lambda_a |v_a\rangle\langle v_a| .$$

Then $\eta : \Sigma \longrightarrow \mathrm{Pos}(\mathbb{C}\Sigma)$ defined

by $\eta(a) = \lambda_a |v_a\rangle\langle v_a|$ is an ensemble of pure states.

Pro: $\mathrm{Den}(\mathbb{C}\Sigma)$ coincides with the set of ensembles of pure states.

Tensor product

The tensor product of $\mathbb{C}\Sigma$ and $\mathbb{C}\Gamma$ is the Hilbert space

$$\mathbb{C}\Sigma \otimes \mathbb{C}\Gamma = \mathbb{C}[\Sigma \times \Gamma] .$$

A vector in the tensor product is represented by $v \otimes u$:

$$v \otimes u = \sum_a \alpha_a |a\rangle \otimes \sum_b \beta_b |b\rangle$$

$$= \sum_{a,b} \alpha_a \beta_b \underbrace{|a\rangle \otimes |b\rangle}$$

We also write $|a\rangle|b\rangle$ or $|ab\rangle$.

The inner product is given by

$$\langle v \otimes u , v' \otimes u' \rangle = \langle v, v' \rangle \langle u, u' \rangle .$$

The Hilbert space associated to a compound register is $\mathbb{C}\Sigma \otimes \mathbb{C}\Gamma$.

Hence a quantum state for such a register is a density operator $\rho \in \mathrm{Den}(\mathbb{C}\Sigma \otimes \mathbb{C}\Gamma)$.

Given $A: \mathbb{C}\Sigma \to \mathbb{C}\Sigma'$ and $B: \mathbb{C}\Gamma \to \mathbb{C}\Gamma'$ the tensor product $A \otimes B$ is defined by

$$A \otimes B : \mathbb{C}\Sigma \otimes \mathbb{C}\Gamma \to \mathbb{C}\Sigma' \otimes \mathbb{C}\Gamma'$$

$$A \otimes B \, (v \otimes u) = Av \otimes Bu.$$

<u>Pro</u>: $(A \otimes B)^+ = A^+ \otimes B^+.$

$$\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\,\mathrm{Tr}(B)$$

In Dirac notation we write

$$\begin{aligned} |v'\rangle\langle v| \otimes |u'\rangle\langle u| &= |v'\rangle \otimes |u'\rangle \, \langle v| \otimes \langle u| \\ &= |v'\rangle|u'\rangle \, \langle v|\langle u| \\ &= |v'u'\rangle\langle vu|. \end{aligned}$$

The operators $\{ |a'b'\rangle\langle ab| \}$ form an orthonormal basis for

$$L(\mathbb{C}\Sigma \otimes \mathbb{C}\Gamma, \mathbb{C}\Sigma' \otimes \mathbb{C}\Gamma').$$

Partial trace

Given $V \otimes W$ the partial trace Tr_W is the linear operator

$$\mathrm{Tr}_W : L(V \otimes W) \longrightarrow L(V)$$

defined by

$$\mathrm{Tr}_W = \mathbb{1}_V \otimes \mathrm{Tr}.$$

We have

$$\mathrm{Tr}_W(A \otimes B) = A \otimes \mathrm{Tr}(B).$$

Partial trace

$$\mathrm{Tr}_V : L(V \otimes W) \longrightarrow L(W)$$

is similarly defined.

For a compound register with a quantum state

$$\rho \in \mathrm{Den}(V \otimes W)$$

the state associated to each register is given by

$$\rho^V = \mathrm{Tr}_W \rho \quad \text{and} \quad \rho^W = \mathrm{Tr}_V \rho.$$

Operator – vector correspondence

There is an isomorphism (of Hilbert spaces)

$$\mathrm{vec}: L(\mathbb{C}\Sigma, \mathbb{C}\Gamma) \longrightarrow \mathbb{C}\Gamma \otimes \mathbb{C}\Sigma$$

defined by

$$\mathrm{vec}(|a\rangle\langle b|) = |a\rangle|b\rangle .$$

We have

$$\langle |a\rangle\langle b| , |c\rangle\langle d| \rangle = \mathrm{Tr}(|b\rangle\langle a| \, |c\rangle\langle d|)$$

$$= \langle a|c\rangle \langle d|b\rangle$$

$$= \langle ab|cd\rangle$$

$$= \langle |ab\rangle , |cd\rangle\rangle .$$

For arbitrary vectors we have

$$\mathrm{vec}(|v\rangle\langle u|) = \sum_{a,b} v_a \bar{u}_b \, \mathrm{vec}(|a\rangle\langle b|)$$

$$= \sum_{a,b} v_a \bar{u}_b \, |a\rangle|b\rangle$$

$$= |v\rangle|\bar{u}\rangle .$$

Lem: $(A_0 \otimes A_1)\,\mathrm{vec}(B) = \mathrm{vec}(A_0 B A_1^T)$

Proof: By linearity it suffices to prove this for $B = |a\rangle\langle b|$.

Then

$$(A_0 \otimes A_1)\,\mathrm{vec}(B) = A_0|a\rangle A_1|b\rangle$$
$$= A_0|a\rangle\left(\langle b| A_1^{\dagger}\right)^{\dagger}$$
$$= \mathrm{vec}\left(A_0|a\rangle\langle b| A_1^T\right). \quad \boxed{}$$

Lem: $\mathrm{Tr}_V\left(\mathrm{vec}(A)\,\mathrm{vec}(B)^{\dagger}\right) = A B^{\dagger}$.

Proof: By anti-linearity it suffices to prove this for $B = |a\rangle\langle b|$.

We have

$$\mathrm{Tr}_V\left(\mathrm{vec}(A)\,\mathrm{vec}(B)^{\dagger}\right) = \mathrm{Tr}_V\left(\mathrm{vec}(A)\left(|ab\rangle\right)^{\dagger}\right)$$
$$= \mathrm{Tr}_V\left(\mathrm{vec}(A)\,\langle ab|\right)$$
$$= \sum_{c,d} A(c,d)\,\mathrm{Tr}_V\big(\underbrace{|cd\rangle\langle ab|}_{|c\rangle\langle d|\,|b\rangle\langle a|}\big)$$
$$= \sum_{c,d} A(c,d)\,|c\rangle\langle d|\,|b\rangle\langle a|$$
$$= A B^{\dagger} \quad \boxed{}$$

HW: $\mathrm{Tr}_W\left(\mathrm{vec}(A)\,\mathrm{vec}(B)^{\dagger}\right) = A^T \overline{B}$.

Schmidt decomposition

Let $|v\rangle \in V \otimes W$ be a nonzero vector.

Then there exist orthonormal sets

$\{ v_a : a \in \Lambda \} \subset V$ and

$\{ w_a : a \in \Lambda \} \subset W$ such that

$$|u\rangle = \sum_{a \in \Lambda} s_a \, |v_a w_a\rangle$$

where $s_a \in \mathbb{R}_{>0}$ and $\sum_{a \in \Lambda} s_a^2 = 1$.

Proof: Let $A \in L(W, V)$ be such that

$$\mathrm{vec}(A) = |u\rangle .$$

By singular value decomposition

$$A = \sum_{a \in \Lambda} s_a \, |v_a\rangle \langle w'_a| .$$

Then $|u\rangle = \mathrm{vec}(A) = \sum_a s_a \, |v_a \underbrace{\overline{w'_a}}_{w_a}\rangle .$

We have

$$1 = \mathrm{Tr}(|u\rangle\langle u|)$$

$$= \sum_a s_a^2$$

$\square$

Purification

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

A vector $|u\rangle \in V \otimes W$ is said to be a purification of P if

$$P = \mathrm{Tr}_W (|u\rangle\langle u|).$$

Lem: The following are equivalent.

1) There exists a purification $|u\rangle$ of P.

2) There exists $A \in L(W, V)$ such that

$$P = A A^{+}.$$

Proof: Since vec is an isomorphism any vector can be written as

$$|u\rangle = \mathrm{vec}(A).$$

We have

$$\mathrm{Tr}_W (|u\rangle\langle u|) = \mathrm{Tr}_W (\mathrm{vec}(A)\, \mathrm{vec}(A)^{+})$$

$$\overset{(\text{Lem})}{=} A A^{+}. \qquad \boxtimes$$

Purification theorem

There exists a purification $|u\rangle \in V \otimes W$ of P if and only if

$$\dim W \geq \operatorname{rank} P.$$

Proof: Purification exists if and only if there exists $A \in L(W, V)$ such that $P = A A^{+}$. (Lem)

This implies that

$$\operatorname{rank}(P) = \operatorname{rank}(A) \quad \text{(Cor.)}$$

and therefore $\operatorname{rank} P \leq \dim W$.

Conversely, by spectral decomposition

$$P = \sum_{a \in \Sigma} \underbrace{\lambda_a}_{\in \mathbb{R}_{>0}} |v_a\rangle\langle v_a| .$$

Since $\dim W \geqslant \operatorname{rank} P$ there exists an orthonormal set $\{ |w_a\rangle : a \in \Sigma \}$. (of size $|\Sigma|$)

Then letting

$$A = \sum_{a \in \Sigma} \sqrt{\lambda_a} |v_a\rangle\langle w_a|$$

gives $A A^{+} = P$. $\boxtimes$

Unitary equivalence of purification

Let $u, v \in V \otimes W$ be such that

$$\operatorname{Tr}_W |u\rangle\langle u| = \operatorname{Tr}_W |v\rangle\langle v| .$$

Then there exists $U \in U(W)$ such that $|v\rangle = \mathbb{1}_V \otimes U |u\rangle$.

Proof: Let A and B be such that

$$|u\rangle = \mathrm{vec}(A) \quad \text{and} \quad |v\rangle = \mathrm{vec}(B).$$

We have

$$AA^{\dagger} = BB^{\dagger}.$$

By singular value decomposition

$$A = \sum_{a \in \Lambda} \sqrt{\lambda_a}\, |v_a\rangle\langle w_a|$$

$$B = \sum_{a \in \Lambda} \sqrt{\lambda_a}\, |v_a\rangle\langle \tilde{w}_a|.$$

Let $\tilde{U} \in U(V)$ be such that

$$\tilde{U}|\tilde{w}_a\rangle = |w_a\rangle.$$

Then $A\tilde{U} = B$ and setting $U = \tilde{U}^T$ we obtain

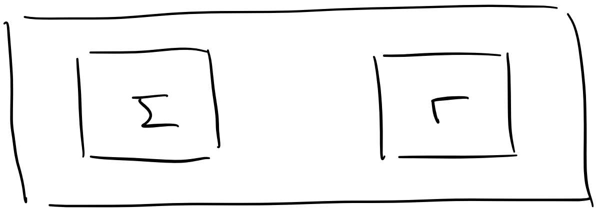
$$\mathbb{1}_V \otimes U\, |u\rangle = \mathbb{1}_V \otimes \tilde{U}^T\, \mathrm{vec}(A)$$

$$= \mathrm{vec}(A\tilde{U}) \quad \text{(Lem.)}$$

$$= \mathrm{vec}(B)$$

$$= |v\rangle \qquad \blacksquare$$

Consider a compound register



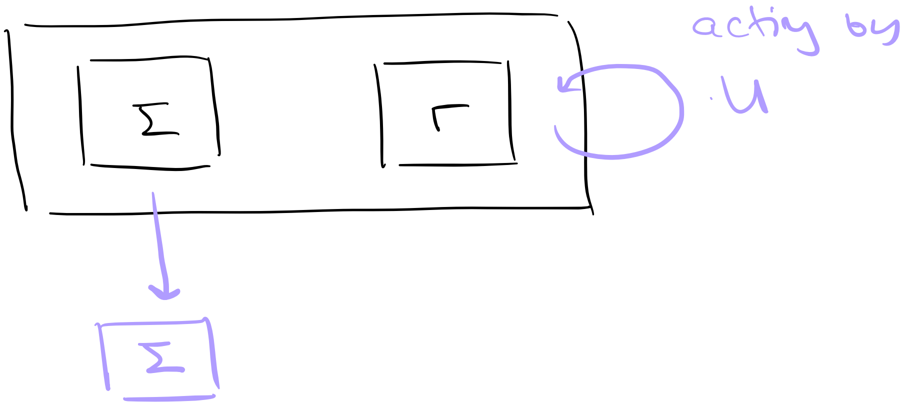
$$|v\rangle\langle v| \in \mathrm{Den}(\mathbb{C}\Sigma \otimes \mathbb{C}\Gamma)$$

Let $\rho = \mathrm{Tr}_{\mathbb{C}\Gamma} |v\rangle\langle v|$.

Note that for any $U \in U(\mathbb{C}\Gamma)$

For $|u\rangle = \mathbb{1}_{\mathbb{C}\Gamma} \otimes U |v\rangle$ we have.

$$\rho = \mathrm{Tr}_{\mathbb{C}\Gamma} |u\rangle\langle u|.$$



ρ unchanged

The theorem implies the converse:

$\forall \; |u\rangle \in \mathbb{C}\Sigma \otimes \mathbb{C}\Gamma$ such that

$$\rho = \mathrm{Tr}_{\mathbb{C}\Gamma} |u\rangle\langle u|$$

then $\exists \, U \in U(\mathbb{C}\Gamma)$ such that

$$|u\rangle = \mathbb{1}_{\mathbb{C}\Sigma} \otimes U |v\rangle.$$

Fidelity

For $A \in L(Y, W)$ the trace norm is defined by

$$\| A \|_1 = \mathrm{Tr} \sqrt{A^\dagger A} .$$

(show that this is a norm)

Prop: For $A \in L(Y)$ we have

$$\| A \|_1 = \max \{ |\langle U, A \rangle| : U \in U(Y) \} .$$

Proof: By singular value decomposition:

$$A = \sum_a s_a |w_a\rangle\langle v_a| .$$

Then

$$
\begin{aligned}
|\langle U, A \rangle|^2 &= | \mathrm{Tr}(U^\dagger A) | \\
&= \sum_a s_a | \langle v_a, U^\dagger w_a \rangle | \\
&\leq \sum_a s_a \underbrace{\| v_a \|}_{1} \underbrace{\| U^\dagger w_a \|}_{1} \quad \text{Cauchy-Schwarz} \\
&= \sum_a s_a \\
&= \| A \|_1 .
\end{aligned}
$$

$$
\begin{aligned}
\| A \|_1 &= \mathrm{Tr}(\sqrt{A^\dagger A}) \\
&= \mathrm{Tr}\left(\sum_a s_a |v_a\rangle\langle v_a| \right) \\
&= \sum_a s_a
\end{aligned}
$$

This maximum is achieved at U that satisfies

$$A = U \sqrt{A^\dagger A} .$$

$\boxtimes$

Cor: Let $A \in L(V)$ and $U_1, U_2 \in U(W,V)$. Then

$$\| U_1^{\dagger} A U_2 \|_1 = \| A \|_1 .$$

Proof: Follows from

$$\begin{aligned} \langle U, U_1^{\dagger} A U_2 \rangle &= \mathrm{Tr}(U^{\dagger} U_1^{\dagger} A U_2) \\ &= \mathrm{Tr}(U_2 U^{\dagger} U_1^{\dagger} A) \\ &= \mathrm{Tr}((U_1 U U_2^{\dagger})^{\dagger} A) \\ &= \langle U_1 U U_2^{\dagger} , A \rangle \end{aligned}$$

and the Proposition. $\square$

For $P, Q \in \mathrm{Pos}(V)$ the fidelity between P and Q is defined by

$$F(P,Q) = \| \sqrt{P} \sqrt{Q} \|_1 .$$

More explicitly, we have

$$F(P,Q) = \mathrm{Tr}\left(\sqrt{\sqrt{Q} P \sqrt{Q}} \right)$$

In particular, for a unit vector $v \in V$:

$$\begin{aligned} F(P, |v\rangle\langle v|) &= \mathrm{Tr} \sqrt{|v\rangle\langle v, Pv\rangle\langle v|} \\ &= \mathrm{Tr}\left(\sqrt{\langle v, Pv\rangle} \, |v\rangle\langle v| \right) \\ &= \sqrt{\langle v, Pv \rangle} . \end{aligned}$$

In particular

$$F(|u\rangle\langle u|, |v\rangle\langle v|) = |\langle u, v\rangle| .$$

Pro: The following properties hold.

1) $F(P,Q) \geq 0$ with equality if and only if $PQ = \mathbb{0}$

2) $F(P,Q)^2 \leq \mathrm{Tr}(P)\,\mathrm{Tr}(Q)$ with equality if and only if P and Q are linearly dependent.

Proof: We have

$$F(P,Q) = \| \sqrt{P}\sqrt{Q} \|_1 \geq 0$$

with equality if and only if $\sqrt{P}\sqrt{Q} = \mathbb{0}$ since $\|\cdot\|_1$ is a norm. The latter condition is equivalent to $PQ = \mathbb{0}$. (Exercise: $\sqrt{P}\sqrt{Q} = \mathbb{0} \iff \|\sqrt{P}\sqrt{Q}\| = 0$.)

For the second property we have

$$\begin{aligned}
\| \sqrt{P}\sqrt{Q} \|_1^2 &\overset{\text{Pro}}{=} |\langle U, \sqrt{P}\sqrt{Q} \rangle|^2 \\
&= |\langle \sqrt{P}U, \sqrt{Q} \rangle|^2 \\
&\leq \| \sqrt{P}U \|^2 \, \| \sqrt{Q} \|^2 \\
&= \mathrm{Tr}(U^\dagger \sqrt{P}\sqrt{P}U)\,\mathrm{Tr}(\sqrt{Q}\sqrt{Q}) \\
&= \mathrm{Tr}(P)\,\mathrm{Tr}(Q)
\end{aligned}$$

Cauchy-Schwarz

When P and Q are linearly dependent, i.e. $\alpha P + \beta Q = \mathbb{0}$ where $\underbrace{\alpha, \beta}_{\text{not all zero}} \in \mathbb{C}$, we can directly show that

$$\| \sqrt{P}\sqrt{Q} \|_1 = \mathrm{Tr}(P)\,\mathrm{Tr}(Q).$$

On the other hand, if P and Q are linearly independent then (exercise) so are $\sqrt{P}U$ and $\sqrt{Q}$. This implies a strict inequality. (by Cauchy-Schwarz) $\boxtimes$

Cor: For $\rho, \sigma \in \mathrm{Den}(V)$ we have

$$0 \leq F(\rho, \sigma) \leq 1$$

where

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

Pro: For $U \in L(V,W)$ we have

$$F(UPU^{+}, UQU^{+}) = F(P,Q).$$

Proof: We have

$$\| \sqrt{UPU^{+}} \sqrt{UQU^{+}} \|_1 = \| U\sqrt{P}U^{+}U\sqrt{Q}U^{+} \|_1$$
$$= \| \sqrt{P} \sqrt{Q} \|_1 \quad \boxtimes$$

Cor

By spectral decomposition $P = \sum_a \lambda_a |v_a\rangle\langle v_a|$

Then $UPU^{+} = \sum_a \lambda_a U|v_a\rangle\langle v_a|U^{+}$.

Therefore
$$\sqrt{UPU^{+}} = \sum_a \sqrt{\lambda_a}\, U|v_a\rangle\langle v_a|U^{+}$$
$$= U\left(\sum_a \sqrt{\lambda_a}\, |v_a\rangle\langle v_a|\right)U^{+}$$
$$= U\sqrt{P}\,U^{+}.$$

Uhlmann's theorem

Let V and W be Hilbert spaces.

Let $P, Q \in \mathrm{Pos}(V)$ be such that

$$\mathrm{rank}(P), \mathrm{rank}(Q) \leq \dim(W).$$

Let $u \in V \otimes W$ be a purification of P.

Then

$$F(P,Q) = \max \{ |\langle v, u \rangle| : v \in V \otimes W, \mathrm{Tr}_W(|v\rangle\langle v|) = Q \}$$

Lem: For $A, B \in L(W, V)$ we have

$$F(AA^\dagger, BB^\dagger) = \| A^\dagger B \|_1$$

Proof: Consider the polar decomposition

$$L(V \oplus W) \ni \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} = PU$$

We have $$P^2 = \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}^\dagger$$

$$= \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ A^\dagger & 0 \end{pmatrix}$$

$$= \begin{pmatrix} AA^\dagger & 0 \\ 0 & 0 \end{pmatrix}$$

and $$P = \begin{pmatrix} \sqrt{AA^\dagger} & 0 \\ 0 & 0 \end{pmatrix}.$$

Similarly we have

$$\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} = QV$$

where

$$Q = \begin{pmatrix} \sqrt{BB^\dagger} & 0 \\ 0 & 0 \end{pmatrix}.$$

Then

$$F(AA^\dagger, BB^\dagger) = \left\| \sqrt{AA^\dagger} \sqrt{BB^\dagger} \right\|_1$$

$$= \left\| \underbrace{\begin{pmatrix} \sqrt{AA^\dagger} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \sqrt{BB^\dagger} & 0 \\ 0 & 0 \end{pmatrix}}_{\begin{pmatrix} \sqrt{AA^\dagger}\sqrt{BB^\dagger} & 0 \\ 0 & 0 \end{pmatrix}} \right\|_1$$

$$= \| PQ \|_1$$

cor

$$= \| U^\dagger P Q V \|_1$$

$$= \| (PU)^\dagger (QV) \|_1$$

$$= \left\| \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}^\dagger \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \right\|_1$$

$$= \left\| \begin{pmatrix} 0 & 0 \\ A^\dagger & 0 \end{pmatrix} \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \right\|_1$$

$$= \left\| \begin{pmatrix} 0 & 0 \\ 0 & A^\dagger B \end{pmatrix} \right\|_1$$

$$= \| A^\dagger B \|_1 . \qquad \boxtimes$$

Cor: For $u, v \in V \otimes W$ we have

$$F(\mathrm{Tr}_W |u\rangle\langle u|, \mathrm{Tr}_W |v\rangle\langle v|) = \| \mathrm{Tr}_V |v\rangle\langle u| \|_1$$

Proof: Let $A, B \in L(W, V)$ be such that $\mathrm{vec}(A) = u$ and $\mathrm{vec}(B) = v$.

We have

$$\begin{aligned} F(\mathrm{Tr}_W |u\rangle\langle u|, \mathrm{Tr}_W |v\rangle\langle v|) &= F(AA^\dagger, BB^\dagger) \\ &= \| A^\dagger B \|_1 \\ &= \| (A^\dagger B)^T \|_1 \\ &\overset{\text{Lem}}{=} \| \mathrm{Tr}_V |v\rangle\langle u| \|_1 . \end{aligned}$$

$\boxtimes$

Proof of Uhlmann's theorem

By the unitary equivalence of purifications:

$$\max \{ |\langle u, v\rangle| : v \in V \otimes W, \ \mathrm{Tr}_W |v\rangle\langle v| = Q \}$$
$$= \max \{ |\langle u, (\mathbb{1}_V \otimes U) w\rangle| : U \in U(V) \}$$

some fixed purification

Let A, B be such that

$$\mathrm{vec}(A) = u$$
$$\mathrm{vec}(B) = w.$$

HW: $BU^T = \mathbb{1}_V \otimes U \ \mathrm{vec}(B)$

Then

$$\langle u, \mathbb{1}_V \otimes U w\rangle = \langle A, BU^T\rangle$$
$$= \langle \overline{U}, A^\dagger B \rangle$$

$$= \max \{ |\langle \overline{u}, A^+ B \rangle| : u \in U(W) \}$$

$$\overset{\text{Pro}}{=} \| A^+ B \|_1$$

$$\overset{\text{Lem}}{=} F(AA^+, BB^+) = F(P, Q). \qquad \boxtimes$$

Cor: $F(P,Q) = F(Q,P)$.

Proof: This follows from unitary equivalence of purifications:

$$F(P,Q) = \max \{ |\langle u, \mathbb{1} \otimes U w \rangle| : U \in U(W) \}$$

$$= \max \{ |\langle \mathbb{1} \otimes U^+ u, w \rangle| : U \in U(W) \}$$

$$= \max \{ |\langle w, \mathbb{1} \otimes U^+ u \rangle| : U \in U(W) \}$$

$$= \max \{ |\langle w, \mathbb{1} \otimes U u \rangle| : U \in U(W) \}$$

$$= F(P, Q). \qquad \boxtimes$$

Alternatively this also follows from

$$\| A \|_1 = \| A^+ \|_1 .$$

Alternative proof of Uhlmann's theorem

$$F(P,Q) = \max\{|\langle u, \mathbb{1}\otimes U v\rangle| : U \in U(W)\}$$

$$|u\rangle = \sum_a \sqrt{P} \otimes \mathbb{1}_W \; |aa\rangle$$

$$|v\rangle = \sum_a \sqrt{Q} \otimes \mathbb{1}_W \; |aa\rangle$$

$|u\rangle$ purifies P
$|v\rangle$ purifies Q. } Exercise

$$|\langle u, \mathbb{1}\otimes U v\rangle|$$

$$= \left|\sum_{a,b} \langle aa| \sqrt{P}\otimes \mathbb{1}_W \sqrt{Q} \otimes U \; |bb\rangle\right|$$

$$= \left|\sum_{a,b} \langle aa| \sqrt{P}\sqrt{Q} \otimes U \; |bb\rangle\right|$$

$$= \left|\sum_{a,b} \langle aa| \sqrt{P}\sqrt{Q} \otimes \sum_{c,d} U(c,d)\, |c\rangle\langle d| \; |bb\rangle\right|$$

$$= \left|\sum_{a,b} \underbrace{\langle a| \sqrt{P}\sqrt{Q}\; U(a,b)\, |b\rangle}_{\mathrm{Tr}(\langle a|\sqrt{P}\sqrt{Q}\, U(a,b)\, |b\rangle)}\right|$$

$$= \left|\mathrm{Tr}\left(\sqrt{P}\sqrt{Q} \underbrace{\sum_{a,b} U(a,b)\, |b\rangle\langle a|}_{U^T}\right)\right|$$

$$= |\mathrm{Tr}(\sqrt{P}\sqrt{Q}\, U^T)|$$

Lem

$$\leq \mathrm{Tr}(|\sqrt{P}\sqrt{Q}|) \qquad |A| = \sqrt{A^\dagger A}$$

$$= \|\sqrt{P}\sqrt{Q}\|_1$$

Taking $U^T = B^+$ where $B \in U(V)$ is such that

$$\sqrt{P}\sqrt{Q} = |\sqrt{P}\sqrt{Q}|\, B \qquad \text{(polar decomposition)}$$

we get

$$
\begin{aligned}
|\mathrm{Tr}(\sqrt{P}\sqrt{Q}\,U^T)| &= |\mathrm{Tr}(\sqrt{P}\sqrt{Q}\,B^+)| \\
&= |\underbrace{\mathrm{Tr}(|\sqrt{P}\sqrt{Q}|)}_{\in \mathbb{R}_{\geq 0}}| \\
&= \mathrm{Tr}(|\sqrt{P}\sqrt{Q}|)
\end{aligned}
$$

Thus max gives the fidelity. $\boxed{\text{S}}$

Lem: For $A \in L(V)$ and $U \in U(V)$ we have

$$|\mathrm{Tr}(AU)| \leq \mathrm{Tr}\,|A|$$

with equality for $U = B^+$ where $A = |A|B$ is the polar decomposition.

Proof: We have

$$
\begin{aligned}
|\mathrm{Tr}(AU)| &= |\mathrm{Tr}(|A|\,B\,U)| \\
&= |\mathrm{Tr}(\sqrt{|A|}\sqrt{|A|}\,B\,U)| \qquad |\langle \sqrt{|A|}, \sqrt{|A|}\,BU\rangle| \\
&\leq \sqrt{\mathrm{Tr}(|A|)\,\underbrace{\mathrm{Tr}(U^+B^+|A|\,B\,U)}_{\mathrm{Tr}(|A|)}} \qquad \text{Cauchy-Schwarz} \\
&= \mathrm{Tr}\,|A|.
\end{aligned}
$$

When $U = B^+$ the equality holds in Cauchy-Schwarz ineq. $\boxed{\text{S}}$

Strong concavity of fidelity

For $p, q \in \mathrm{Dist}(\Lambda)$

$$F\left(\sum_{a\in\Lambda} p_a P_a, \sum_{a\in\Lambda} q_a Q_a\right) \geq \sum_{a\in\Lambda} \sqrt{p_a q_a}\, F(P_a, Q_a).$$

Proof: By Uhlmann's theorem there exists purifications u_a and v_a such that

$$F(P_a, Q_a) = |\langle u_a | v_a \rangle|.$$

purifies P_a purifies Q_a

Let $\mathcal{U} = \mathbb{C}\Lambda$. Then

$$|u\rangle = \sum_{a\in\Lambda} \sqrt{p_a}\, |u_a\rangle |a\rangle \quad \text{and} \quad |v\rangle = \sum_{a\in\Lambda} \sqrt{q_a}\, |v_a\rangle |a\rangle$$

are purifications for

$$P = \sum_a p_a P_a \quad \text{and} \quad Q = \sum_a q_a Q_a.$$

Verify $\mathrm{Tr}_{W\otimes U} |u\rangle\langle u| = P$, similarly for Q.

Again by Uhlmann's theorem

$$F(P,Q) \geq |\langle u | v \rangle| = \sum_a \sqrt{p_a q_a}\, |\langle u_a | v_a \rangle| = \sum_a \sqrt{p_a q_a}\, F(P_a, Q_a)$$

$\boxed{}$

Appendix: Proofs of some theorems

Proof of Cauchy–Schwarz inequality

If $u = \alpha v$ then the inequality holds.

Assume $u \neq 0$ and $\{v, u\}$ linearly independent.

Gram–Schmidt gives an orthonormal set $\{\tilde{v}_1, \tilde{v}_2\}$ where $\tilde{v}_1 = v / \|v\|$.

We can express v as

$$u = \langle \tilde{v}_1, u \rangle \tilde{v}_1 + \langle \tilde{v}_2, u \rangle \tilde{v}_2 .$$

Then $\langle u, u \rangle \langle v, v \rangle$ is given by

$$\Big\langle \sum_i \langle \tilde{v}_i, u \rangle \tilde{v}_i , \sum_i \langle \tilde{v}_i, u \rangle \tilde{v}_i \Big\rangle \langle v, v \rangle$$

$$= \Big(\sum_i \langle u, \tilde{v}_i \rangle \langle \tilde{v}_i, u \rangle \Big) \langle v, v \rangle$$

$$\geq \langle u, \tilde{v}_1 \rangle \langle \tilde{v}_1, u \rangle \langle v, v \rangle$$

$$= \langle u, v \rangle \langle v, u \rangle \frac{\langle v, v \rangle}{\|v\|^2}$$

$$= |\langle u, v \rangle|^2 \qquad \boxtimes$$

Proof of the spectral decomposition theorem

We will do induction on $|\Sigma|$.

For $|\Sigma| = 1$ we have

$$A = \lambda |a\rangle\langle a| .$$

Assume $|\Sigma| \geq 2$.

Let λ be an eigenvalue of A and let Π be the projector onto V_λ:

$$\Pi = \sum_{b \in \Gamma} |v_b\rangle\langle v_b|$$

where $\{|v_b\rangle : b \in \Gamma\}$ is an orthonormal basis of V_λ.

Define another projector

$$\Pi^\perp = \mathbb{1}_V - \Pi .$$

Observe that

$$\Pi \Pi^\perp = \Pi^\perp \Pi = 0.$$

We have

$$\begin{aligned} A &= \mathbb{1}_V \, A \, \mathbb{1}_V \\ &= (\Pi + \Pi^\perp) \, A \, (\Pi + \Pi^\perp) \\ &= \Pi A \Pi + \underbrace{\Pi^\perp A \Pi + \Pi A \Pi^\perp}_{\text{claim: this is } 0.} + \Pi^\perp A \Pi^\perp \end{aligned}$$

Claim 1: $\Pi^\perp A \Pi = 0$:

$$\Pi^\perp A \underbrace{\Pi v}_{\text{in } V_\lambda} = \lambda \underbrace{\Pi^\perp \Pi}_{0} v = 0 \qquad \forall v \in V.$$

Claim 2: $\Pi A \Pi^\perp = 0$:

For $w \in V_\lambda$ we have

$$A A^+ w = A^+ A w = \lambda \underbrace{A^+ w}_{}$$

Therefore in V_λ.

Then similar to claim 1 we can show

$$\Pi^\perp \overbrace{A^+ \underbrace{\Pi v}_{\text{in } V_\lambda}}^{\text{in } V_\lambda} = 0.$$

$$\Pi^\perp A^+ \underbrace{\Pi v}_{\text{in } V_\lambda} = \lambda \underbrace{\Pi^\perp \Pi}_{0} v = 0.$$

$$\Rightarrow \Pi^\perp A^+ \Pi = 0 \quad \underset{\text{adjoint}}{\Longrightarrow} \quad \Pi A \Pi^\perp = 0.$$

Therefore $A = \Pi A \Pi + \Pi^\perp A \Pi^\perp$.

Claim 3: $\Pi^\perp A \Pi^\perp$ is normal:

First observe that

(A) $\Pi^\perp A = \Pi^\perp A (\Pi + \Pi^\perp) = \Pi^\perp A \Pi^\perp$

(B) $\Pi^\perp A^+ = \Pi^\perp A^+ (\Pi + \Pi^\perp) = \Pi^\perp A^+ \Pi^\perp$.

Then

$(\Pi^\perp A \Pi^\perp)(\Pi^\perp A^+ \Pi^\perp)$

$$
\begin{aligned}
&= (\Pi^\perp A \Pi^\perp) A^+ \Pi^\perp \\
&\underset{(A)}{=} \Pi^\perp A A^+ \Pi^\perp \\
&= \Pi^\perp A^+ A \Pi^\perp \\
&\underset{(B)}{=} (\Pi^\perp A^+ \Pi^\perp) A \Pi^\perp \\
&= (\Pi^\perp A \Pi^\perp)(\Pi^\perp A \Pi^\perp).
\end{aligned}
$$

Let $\quad \mathcal{U} = \{ \Pi^\perp v : v \in V \}$.

Then $\quad \Pi^\perp A \Pi^\perp \in L(\mathcal{U})$

where

$$\dim(\mathcal{U}) < \dim(V).$$

By induction we have

$$\Pi^\perp A \Pi^\perp = \sum_a \lambda_a |u_a\rangle\langle u_a|$$

for some orthonormal basis $\{ |u_a\rangle : a \in \Gamma \}$ of $\mathcal{U}$.

Let $\{|w_b\rangle\}_{b \in \Lambda}$ be an orthonormal basis for V_λ.

Then

$$A = \sum_{b \in \Lambda} \lambda |w_b\rangle\langle w_b| + \sum_{a \in \Gamma} \lambda_a |u_a\rangle\langle u_a|$$

$\boxtimes$

Proof of polar decomposition

The unitary U is constructed as follows: By spectral decomposition

$$\sqrt{A^\dagger A} = \sum_{a \in \Lambda} \sqrt{\lambda_a} \, |v_a\rangle\langle v_a|$$

where $\sqrt{\lambda_a} \in \mathbb{R}_{\geq 0}$

Let

$$|u_a\rangle = \frac{1}{\sqrt{\lambda_a}} A |v_a\rangle$$

where $a \in \Lambda' = \{ a \in \Lambda : \lambda_a \neq 0 \}$.

The set $\{ u_a : a \in \Lambda' \}$ and can be extended to an orthonormal basis $\{ u_a : a \in \Lambda \}$.

Let

$$U = \sum_{a \in \Sigma} |u_a\rangle\langle v_a| .$$

(Omitted: Proving that $A = U\sqrt{A^\dagger A}$.) $\boxtimes$

For linear algebra background see Linear Algebra Done Right by Axler.