



UNIVERSITY OF
ILLINOIS
URBANA - CHAMPAIGN

Math 595 Representation-theoretic methods in QIT

Mathematical setup of finite-dimensional quantum information theory

Felix Leditzky

Fall term 2025

Last update: September 9, 2025

Notation

Notation

- Complex conjugation: If $z = x + iy$ with $x, y \in \mathbb{R}$, then $z^* = x - iy$.
- Hilbert space \mathcal{H} : complete complex vector space with inner product (\cdot, \cdot) .
- Linear operators: $\mathcal{L}(\mathcal{H}) = \{X : \mathcal{H} \rightarrow \mathcal{H} : X \text{ linear}\}$.
- Hermitian adjoint of $X \in \mathcal{L}(\mathcal{H})$ is denoted by X^\dagger , defined via

$$(Xv, w) = (v, X^\dagger w) \quad \text{for all } v, w \in \mathcal{H}.$$

- We operate *exclusively* in finite dimensions, so we do not worry about domains, boundedness, etc.
- In coordinates: $X^\dagger = (X^*)^T$, where X^* is the component-wise complex conjugate.
- **Bra-ket notation:** We denote by $|\psi\rangle \in \mathcal{H}$ column vectors in \mathcal{H} .
- $\langle\psi| := (|\psi\rangle)^\dagger$; $\langle\psi|\phi\rangle$ is the inner product between $|\psi\rangle$ and $|\phi\rangle$, and $|\psi\rangle\langle\phi|$ is a rank-1 operator.
- $\langle\psi|X|\phi\rangle = \langle\psi|(X|\phi\rangle) = (\langle\psi|X)|\phi\rangle = (X^\dagger|\psi\rangle)^\dagger|\phi\rangle$.

Quantum systems and quantum states

Examples of quantum systems

Quantum system: physical system with one or more quantum-mechanical degrees of freedom (either discrete or continuous).

Some examples:

- position and momentum of a particle
- *spin of a particle* (e.g. spin along z-axis of an electron)
- polarization of a photon

Two possible “basis states”: spin up (\uparrow) and spin down (\downarrow).

Each of these is assigned a vector in the *state space* \mathbb{C}^2 :

$$|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Superposition principle

Superposition principle

Quantum system can be prepared in an arbitrary state

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle,$$

where $\alpha, \beta \in \mathbb{C}$ satisfy $|\alpha|^2 + |\beta|^2 = 1$.

When measuring the system, the probabilities of finding the electron in spin up (\uparrow) or spin down (\downarrow) are given by

$$\text{Prob}(\uparrow) = |\langle\uparrow|\psi\rangle|^2 = |\alpha|^2$$

$$\text{Prob}(\downarrow) = |\langle\downarrow|\psi\rangle|^2 = |\beta|^2.$$

Quantum systems and quantum states

State space

The state space of a quantum system is a *Hilbert space* (complete complex inner-product space).

A quantum state is a *density operator* $\rho \in \mathcal{L}(\mathcal{H})$ satisfying:

- *Positivity*: $\rho \geq 0 \iff \langle \varphi | \rho | \varphi \rangle \geq 0$ for all $|\varphi\rangle \in \mathcal{H}$.
- *Normalization*: $\text{tr} \rho = 1$.

This lecture: restrict to finite-dimensional Hilbert spaces $\mathcal{H} = \mathbb{C}^d$ equipped with the standard inner product

$$\langle \psi | \phi \rangle = \sum_{i=1}^d \psi_i^* \phi_i$$

for vectors $|\psi\rangle = (\psi_1, \dots, \psi_d)^T$ and $|\phi\rangle = (\phi_1, \dots, \phi_d)^T$.

Observables

Observable quantities are represented by *Hermitian operators*

$$A \in \{X \in \mathcal{L}(\mathcal{H}) : X^\dagger = X\}.$$

Real eigenvalues of an observable can (in principle) be measured in an experiment.

Quantum state ρ assigns an *expectation value* to an observable A :

$$\langle A \rangle_\rho = \text{tr}(A\rho).$$

Pure vs. mixed states

Set of density matrices is convex and compact

If ρ_i are density matrices and p_i probabilities, then $\rho = \sum_i p_i \rho_i$ is also a density matrix:

- $\sum_i p_i \rho_i \geq 0$ (set of PSD operators is convex).
- $\text{tr}(\sum_i p_i \rho_i) = \sum_i p_i \text{tr} \rho_i = \sum_i p_i = 1$ (by linearity and normalization).

Pure states

Extreme points in the convex set of density matrices are called *pure* states.

A pure density matrix has rank 1 and can be written as a *projector*:

$$\rho = |\psi\rangle\langle\psi| \text{ for some } |\psi\rangle \in \mathcal{H} \text{ with } \langle\psi|\psi\rangle = 1.$$

The vector $|\psi\rangle$ is also often called a *pure state* or *state vector*. A density matrix (state) that is not pure is called *mixed*.

Pure-state ensembles

A collection of state vectors $\{|\psi_i\rangle\}_i$ with probabilities $\{p_i\}_i$ is called a *pure state ensemble* for a mixed state ρ if

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

Every mixed state has infinitely many pure-state ensembles realizing it (see exercises).

Every quantum state ρ has a *spectral decomposition*:

$$\rho = \sum_i \lambda_i |v_i\rangle\langle v_i|,$$

with eigenvalues λ_i and an orthonormal basis of eigenvectors $\{|v_i\rangle\}_i$.

$\rho \geq 0$ and $\text{tr}\rho = 1 \implies \lambda_i \geq 0$ and $\sum_i \lambda_i = 1$.

Measurements

Measuring a quantum system

Measuring a quantum system means determining a property of a quantum system associated with an observable.

This yields different *classical* outcomes with certain probabilities determined by the state of the quantum system.

A quantum system that is measured loses its “quantum behavior”.

We will not discuss this in class, but see, e.g., [Bru17] for a discussion of the “measurement problem”.

Projective measurements

Let A be an observable on \mathcal{H} prepared in the state ρ .

Consider the spectral decomposition $A = \sum_j x_j P_j$, where:

- x_j are the (real) eigenvalues of A ;
- P_j are the orthogonal projectors satisfying:
 1. Positivity: $P_j \geq 0$.
 2. Completeness: $\sum_j P_j = \mathbb{1}_{\mathcal{H}}$.
 3. Orthogonality: $P_j P_k = \delta_{jk} P_j$.

Projective measurements

The collection of operators $\{P_j\}_j$ is called a *projective measurement* that gives the measurement outcome x_j with probability

$$p_j = \text{tr}(\rho P_j).$$

$$P_j = |v_j\rangle\langle v_j|, \rho = |\psi\rangle\langle\psi| \implies p_j = |\langle v_j | \psi \rangle|^2 \text{ (as before).}$$

The numbers $(p_j)_j$ indeed form a probability distribution:

- $p_j = \text{tr}(\rho P_j) \geq 0$ since both $\rho, P_j \geq 0$.
- $\sum_j p_j = \sum_j \text{tr}(\rho P_j) = \text{tr}(\rho \sum_j P_j) = \text{tr}(\rho \mathbb{1}_{\mathcal{H}}) = \text{tr} \rho = 1$
by linearity of the trace and normalization of ρ .

Note that we only needed properties 1 and 2 above to ensure that $(p_j)_j$ is a probability distribution.

⇒ More general measurement by dropping the orthogonality property of the measurement operators $\{P_j\}$.

Positive operator-valued measure (POVM)

Positive operator-valued measure (POVM): collection of operators $\{E_k\}_k$ satisfying:

1. Positivity: $E_k \geq 0$
2. Completeness $\sum_k E_k = \mathbb{1}_{\mathcal{H}}$

Effect operator E_k corresponds to a measurement outcome “ k ” obtained with probability $p_k = \text{tr}(\rho E_k)$.

Main difference between these two types of measurements:

Available information about the quantum state of the measured system *after* the measurement.

Definition (Post-measurement state)

After performing a projective measurement $\{P_j\}_j$ on a quantum system in state ρ and obtaining outcome j , the system assumes the *post-measurement state*

$$\rho_j = \frac{1}{\text{tr}(\rho P_j)} P_j \rho P_j.$$

POVM $\{E_k\}_k$: no unique way of defining post-measurement state.

The only information we obtain are the probabilities $p_k = \text{tr}(\rho E_k)$.

Open systems formulation:

every POVM can be realized as a projective measurement on a larger system including an environment system that is inaccessible to the experimenter (see Naimark's Theorem, e.g., in [Wil16]).

Composite systems and entanglement

Marginals and partial trace

Consider two quantum systems A and B with associated Hilbert spaces \mathcal{H}_A and \mathcal{H}_B .

State space of joint system AB : Tensor product $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Marginal state

The *marginal state* ρ_A of a bipartite state ρ_{AB} is defined as the operator ρ_A satisfying the following relation for all $X_A \in \mathcal{L}(\mathcal{H}_A)$:

$$\text{tr}(\rho_{AB}(X_A \otimes \mathbb{1}_B)) = \text{tr}(\rho_A X_A)$$

Uniquely defines *partial trace* $\text{tr}_B = \text{id}_A \otimes \text{tr} : \mathcal{L}(\mathcal{H}_{AB}) \rightarrow \mathcal{L}(\mathcal{H}_A)$.

Partial trace in coordinates: For an orthonormal basis $\mathcal{E} = \{|e_i\rangle_B\}_{i=1}^{|B|}$,

$$\text{tr}_B X_{AB} = \sum_{i=1}^{\dim B} (\mathbb{1}_A \otimes \langle e_i |_B) X_{AB} (\mathbb{1}_A \otimes |e_i\rangle_B).$$

Correlations in bipartite quantum systems

One of the major goals of quantum information theory is to understand correlations between quantum systems.

In the case of bipartite systems AB , we distinguish between the following types of correlations between A and B :

1. *Product states*: $\rho_{AB} = \omega_A \otimes \sigma_B$ for states ω_A and σ_B .

Any local measurements do not depend on the other system: If $E_A, F_B \geq 0$ are measurement operators (e.g., from POVMs on A and B , respectively), then

$$\text{tr}[\rho_{AB}(E_A \otimes F_B)] = \text{tr}[(\omega_A \otimes \sigma_B)(E_A \otimes F_B)] = \text{tr}(\omega_A E_A) \text{tr}(\sigma_B F_B).$$

Hence, outcomes on A and B are **independent** and therefore **uncorrelated**.

2. *Separable states*: $\rho_{AB} = \sum_i p_i \omega_A^{(i)} \otimes \sigma_B^{(i)}$ for states $\omega_A^{(i)}$ and $\sigma_B^{(i)}$ and prob. dist. $(p_i)_i$.

Index i encodes **classical correlation** between A and B .

Pure separable states are automatically product

3. *Entangled states*: states that are not separable.

They describe **quantum correlations**.

Example: Maximally entangled states

Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis for \mathbb{C}^2 . We define the *EPR state*, *Bell state* or *maximally entangled state*

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) = \frac{1}{\sqrt{2}}(1, 0, 0, 1)^T.$$

The corresponding density matrix is

$$\Phi_{AB}^+ = |\Phi^+\rangle\langle\Phi^+|_{AB} = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

This is an example of an *entangled state*.

Example: Maximally entangled states

There are actually three more such maximally entangled states on two qubits:

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) = \frac{1}{\sqrt{2}}(1, 0, 0, -1)^T$$

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) = \frac{1}{\sqrt{2}}(0, 1, 1, 0)^T$$

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) = \frac{1}{\sqrt{2}}(0, 1, -1, 0)^T.$$

The four states $\{|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}, |\Psi^-\rangle_{AB}\}$ are orthonormal and thus form an orthonormal basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ known as the **Bell basis**. We call them maximally entangled because for each state both marginals on A and B are *completely mixed*:

$$\text{tr}_A \Phi_{AB}^+ = \frac{1}{2} \mathbb{1} = \text{tr}_B \Phi_{AB}^+,$$

and similarly for $|\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}, |\Psi^-\rangle_{AB}$.

Testing entanglement with the partial transpose

How can we check whether a state is entangled?

Partial transpose

We define the partial transpose as $(\cdot)^{T_B} := \text{id}_A \otimes (\cdot)^T$.

In coordinates: Write $X_{AB} = \sum_{i,j} c_{ij} Q_{A,i} \otimes P_{B,j}$ in terms of operator bases $\{Q_{A,i}\}_i$ for $\mathcal{L}(\mathcal{H}_A)$ and $\{P_{B,j}\}_j$ for $\mathcal{L}(\mathcal{H}_B)$, then

$$X_{AB}^{T_B} = \sum_{i,j} c_{ij} Q_{A,i} \otimes (P_{B,j})^T.$$

PPT states

A state ρ_{AB} is called **PPT** (for *positive partial transpose*), if

$$\left(\rho_{AB}^{T_B} \geq 0 \iff \rho_{AB}^{T_A} \geq 0 \right).$$

PPT criterion

Every separable state σ_{AB} satisfies $\sigma_{AB}^{T_B} \geq 0$. Hence, if $\rho_{AB}^{T_B}$ has a negative eigenvalue, then ρ_{AB} is entangled.

Proof.

Let $\sigma_{AB} = \sum_i p_i \sigma_A^{(i)} \otimes \sigma_B^{(i)}$ be separable. Recall that this means in particular that $\sigma_A^{(i)}, \sigma_B^{(i)} \geq 0$, and $p_i \geq 0$. Since $(\cdot)^{T_B}$ is linear and X is positive semidefinite iff X^T is positive semidefinite, we have

$$\sigma_{AB}^{T_B} = \sum_i p_i \sigma_A^{(i)} \otimes \left(\sigma_B^{(i)}\right)^T \geq 0,$$

as a convex combination of positive semidefinite operators. □

Bell states are entangled

Proof.

We use the PPT criterion to show this:

$$2(\Phi^+)^{T_B} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}^{T_B} = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^T \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^T \right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =: \mathbb{F}_{AB}.$$

The operator \mathbb{F}_{AB} is called *swap operator*. It acts on the tensor product space $\mathbb{C}^2 \otimes \mathbb{C}^2$ by swapping the two systems,

$$\mathbb{F}_{AB}(|\psi\rangle \otimes |\phi\rangle) = |\phi\rangle \otimes |\psi\rangle \quad \text{for all } |\psi\rangle, |\phi\rangle \in \mathbb{C}^2.$$

Bell states $|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}, |\Psi^-\rangle_{AB}$ are **eigenvectors** of the swap operator.

Eigenvalue corresponding to $|\Psi^-\rangle$ is $-1 \implies (\Phi^+)^{T_B} \not\geq 0 \implies \Phi^+$ is entangled! \square

A first contact with representations

We consider the **symmetric group** $S_2 = \{e, (12)\}$.

Swap operator \mathbb{F}_{AB} : example of a *representation* of the transposition $(12) \in S_2$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Identity permutation e is represented by identity operator $\mathbb{1}_{AB} = \mathbb{1}_A \otimes \mathbb{1}_B$.

Bell basis $\{|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}, |\Psi^-\rangle_{AB}\}$ is an orthonormal basis *adapted* to representation $e \mapsto \mathbb{1}_{AB}, (12) \mapsto \mathbb{F}_{AB}$:

- $|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}$ are eigenvectors of both $\mathbb{1}_{AB}$ and \mathbb{F}_{AB} with eigenvalue +1.
- $|\Psi^-\rangle_{AB}$ is an eigenvector of $\mathbb{1}_{AB}$ with eigenvalue +1, and of \mathbb{F}_{AB} with eigenvalue -1.

A first contact with representations

Symmetric subspace

$\text{Sym}^2(\mathbb{C}^2) := \text{span}(|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB})$ contains three copies of the 1-dimensional **trivial representation** of S_2 .

Each $|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}$ spans one copy, and both group elements $e, (12) \in S_2$ act trivially on each of them.

Antisymmetric subspace

$\Lambda^2(\mathbb{C}^2) := \text{span}(|\Psi^-\rangle)$ is the 1-dimensional **sign representation** of S_2 .

The identity e still acts trivially, transposition (12) acts by multiplying with -1 .

Decomposition of representation space:

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \text{Sym}^2(\mathbb{C}^2) \oplus \Lambda^2(\mathbb{C}^2),$$

$$\mathbb{1}_{AB} \cong \begin{pmatrix} 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \\ \cdot & \cdot & 1 \end{pmatrix} = \mathbb{1}_{\text{Sym}^2(\mathbb{C}^2)} \oplus \mathbb{1}_{\Lambda^2(\mathbb{C}^2)} \quad \mathbb{F}_{AB} \cong \begin{pmatrix} 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \\ \cdot & \cdot & -1 \end{pmatrix} = \mathbb{1}_{\text{Sym}^2(\mathbb{C}^2)} \oplus (-1)\mathbb{1}_{\Lambda^2(\mathbb{C}^2)}$$

PPT criterion: Necessary, but not sufficient

Unfortunately, the PPT criterion is only a *necessary* criterion for separability.

In small dimensions ($|A| \cdot |B| \leq 6$) it is also sufficient [HHH96], but in higher dimensions there are indeed “bound entangled states” that are PPT *and* entangled [Hor97; HHH98].

There are many necessary (but not sufficient) criteria for separability. Another well-known one is the “reduction criterion” $\rho_{AB} \leq \rho_A \otimes \mathbb{1}_B$ [HH99].

It is NP-hard to decide whether a given mixed state is separable [Gur03]. However, for pure states there is an efficiently checkable separability criterion based on the singular value decomposition.

Schmidt decomposition

Let $|\psi\rangle_{AB}$ be a pure bipartite quantum state. Then there are sets of orthonormal vectors $\{|e_i\rangle_A\}_{i=1}^r$ and $\{|f_j\rangle_B\}_{j=1}^r$ and strictly positive real numbers $(\lambda_i)_{i=1}^r$ such that

$$|\psi\rangle_{AB} = \sum_{i=1}^r \sqrt{\lambda_i} |e_i\rangle_A \otimes |f_i\rangle_B.$$

The *Schmidt coefficients* $(\lambda_i)_{i=1}^r$ satisfy $\sum_{i=1}^r \lambda_i = 1$, and are unique up to reordering. The integer r is called the *Schmidt rank* of $|\psi\rangle_{AB}$.

The state $|\psi\rangle_{AB}$ is entangled iff $r > 1$. The marginals of $|\psi\rangle_{AB}$ are given by

$$\rho_A = \text{tr}_B \psi_{AB} = \sum_{i=1}^r \lambda_i |e_i\rangle\langle e_i|_A \qquad \rho_B = \text{tr}_A \psi_{AB} = \sum_{i=1}^r \lambda_i |f_i\rangle\langle f_i|_B.$$

These are spectral decompositions, that is, ρ_A and ρ_B have the same spectrum given by the Schmidt coefficients, and the *Schmidt vectors* $\{|e_i\rangle_A\}$ and $\{|f_j\rangle_B\}$ can be completed to eigenbases of ρ_A and ρ_B , respectively.

Mixedness vs. purity

Mixed state: uncertainty of the true preparation of the quantum system.

If mixed state ρ_{AB} is realized by pure-state ensemble $(p_i, |\psi_i\rangle\langle\psi_i|)_i$ as $\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, then system is found in pure state ψ_i with probability p_i .

The *open systems* formulation of quantum mechanics provides a *purified* picture in which the uncertainty of system preparation corresponds to the system being entangled with an inaccessible environment.

Formally:

Purification

Let ρ_A be a mixed quantum state. Any state $|\psi\rangle_{AR} \in \mathcal{H}_A \otimes \mathcal{H}_R$ satisfying

$$\text{tr}_R \psi_{AR} = \rho_A,$$

where \mathcal{H}_R is some auxiliary Hilbert space, is called a *purification* of ρ_A .

Purifications exist and are equivalent

Let ρ_A be a mixed quantum state.

- (i) There exists a purification of ρ_A on $\mathcal{H}_A \otimes \mathcal{H}_R$ with $\dim \mathcal{H}_R \geq \text{rank } \rho_A$.
- (ii) Any two purifications are isometrically equivalent: Let $|\psi\rangle_{AR_1}$ and $|\varphi\rangle_{AR_2}$ be two purifications of ρ_A , and without loss of generality assume $\dim \mathcal{H}_{R_1} \leq \dim \mathcal{H}_{R_2}$. Then there exists an isometry $V: \mathcal{H}_{R_1} \rightarrow \mathcal{H}_{R_2}$ such that

$$|\varphi\rangle_{AR_2} = (\mathbb{1}_A \otimes V) |\psi\rangle_{AR_1}.$$

Proof.

(i) Consider a spectral decomposition $\rho_A = \sum_{i=1}^n \lambda_i |v_i\rangle\langle v_i|_A$, where $\lambda_i > 0$ such that $r = \text{rank } \rho_A$. Take $\mathcal{H}_R = \mathbb{C}^r$ with orthonormal basis $\{|w_i\rangle_R\}_{i=1}^r$, then

$|\psi\rangle_{AR} := \sum_{i=1}^r \sqrt{\lambda_i} |v_i\rangle_A \otimes |w_i\rangle_R$ is the desired purification.

(ii) This follows from Schmidt decomposition. □

Distance measures

Approximations are quantified using measures of how close quantum states are.

Here we focus on two such measures: trace norm and fidelity.

First, we define a useful norm on operators.

Definition (Trace norm)

The *trace norm* of a linear operator $X \in \mathcal{L}(\mathcal{H})$ is

$$\|X\|_1 = \operatorname{tr}\sqrt{X^\dagger X} = \sum_{i=1}^d s_i(X),$$

where $d = \dim\mathcal{H}$ and $s_i(X)$ are the singular values of X .

This defines a norm (in the usual sense) on $\mathcal{L}(\mathcal{H})$.

Special case when X is Hermitian with real eigenvalues λ_i :

$$\|X\|_1 = \sum_{i=1}^d |\lambda_i|.$$

Trace distance

The trace distance is defined as the metric obtained from the trace norm:

Trace distance

Let ρ and σ be quantum states on \mathcal{H} . Then their *trace distance* is defined as

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

The factor $\frac{1}{2}$ is for normalization, ensuring that $0 \leq D(\rho, \sigma) \leq 1$.

There is a useful variational characterization of the trace norm:

Variational characterization of trace norm

$$\|X\|_1 = \max\{|\operatorname{tr}(XU)| : U \text{ unitary}\}.$$

Proved in the exercises.

Properties of the trace distance

- (i) $D(\cdot, \cdot)$ is a metric: non-negative, symmetric and satisfying the triangle inequality.
- (ii) $0 \leq D(\rho, \sigma) \leq 1$ and $D(\rho, \sigma) = 0$ iff $\rho = \sigma$.
With $\text{supp}X := (\ker X)^\perp$, we also have $D(\rho, \sigma) = 1$ iff $\text{supp}\rho \perp \text{supp}\sigma$.
- (iii) $D(\rho, \sigma) = \sup\{\text{tr}[P(\rho - \sigma)] : P \geq 0 \text{ and } \mathbb{1} - P \geq 0\}$.
- (iv) Data-processing:

$$D(\rho, \sigma) = D(U\rho U^\dagger, U\sigma U^\dagger) \text{ for all unitaries } U;$$

$$D(\rho_A, \sigma_A) \leq D(\rho_{AB}, \sigma_{AB}).$$

- (v) $D(\rho, \sigma)$ is related to the maximum success probability $p_{\text{succ}}(\rho, \sigma)$ of distinguishing between ρ and σ (Holevo-Helstrom theorem):

$$p_{\text{succ}}(\rho, \sigma) = \frac{1}{2} (1 + D(\rho, \sigma)).$$

Another important distance measure (though not a metric in the mathematical sense) is the fidelity:

Fidelity

The fidelity $F(\rho, \sigma)$ of quantum states ρ and σ is defined as

$$F(\rho, \sigma) = \left\| \sqrt{\rho} \sqrt{\sigma} \right\|_1 = \text{tr}(\sigma^{1/2} \rho \sigma^{1/2})^{1/2}.$$

The origin of fidelity lies in the transition probability

$$\text{Prob}(\psi \rightarrow \phi) := |\langle \psi | \phi \rangle|^2$$

of a quantum system to go from a state $|\psi\rangle$ to a state $|\phi\rangle$.

By item (v) in the proposition below, $F(\psi, \phi)^2 = \text{Prob}(\psi \rightarrow \phi)$ for pure states $|\psi\rangle, |\phi\rangle$.

Properties of the fidelity

- (i) $0 \leq F(\rho, \sigma) \leq 1$ and $F(\rho, \sigma) = 1$ iff $\rho = \sigma$, while $F(\rho, \sigma) = 0$ iff $\text{supp} \rho \perp \text{supp} \sigma$.
- (ii) $F(\rho, \sigma) = F(\sigma, \rho)$.
- (iii) $F(\rho, \sigma) = F(U\rho U^\dagger, U\sigma U^\dagger)$ for all unitaries U , and $F(\rho_{AB}, \sigma_{AB}) \leq F(\rho_A, \sigma_A)$.
- (iv) $F(\cdot, \cdot)$ is jointly concave: For quantum states ρ_i, σ_i and a probability distribution $(p_i)_i$,

$$F\left(\sum_i p_i \rho_i, \sum_i p_i \sigma_i\right) \geq \sum_i p_i F(\rho_i, \sigma_i).$$

- (v) For pure states $|\psi\rangle$ and $|\phi\rangle$ we have $F(\psi, \phi) = |\langle \psi | \phi \rangle|$.
- (vi) Uhlmann's theorem:

$$F(\rho, \sigma) = \max\{|\langle \psi^\rho | \phi^\sigma \rangle|\}$$

where the maximization is over purifications $|\psi^\rho\rangle, |\phi^\sigma\rangle$ of ρ, σ , respectively.

Relating trace distance and fidelity

Fuchs-van de Graaf inequalities

For any two quantum states ρ and σ ,

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}.$$

Easy to check for pure states: Write $|\phi\rangle = \cos\theta|\psi\rangle + \sin\theta|\psi^\perp\rangle$, then $F(\psi, \phi) = \cos\theta$ and

$$2D(\psi, \phi) = \left\| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \right\|_1 = 2|\sin\theta| = 2\sqrt{1 - \cos^2\theta} = 2\sqrt{1 - F(\psi, \phi)^2}.$$

This can be extended to mixed states, see [Wil16] for a full proof.

References

- [Bru17] Časlav Brukner. **“On the Quantum Measurement Problem”**. *Quantum [Un]Speakables II: Half a Century of Bell’s Theorem*. Ed. by Reinhold Bertlmann and Anton Zeilinger. Cham: Springer International Publishing, 2017, pp. 95–117. arXiv: 1507.05255 [quant-ph].
- [Gur03] Leonid Gurvits. **“Classical Deterministic Complexity of Edmonds’ Problem and Quantum Entanglement”**. *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*. STOC ’03. San Diego, CA, USA: Association for Computing Machinery, 2003, pp. 10–19. arXiv: quant-ph/0303055.
- [HH99] Michał Horodecki and Paweł Horodecki. **“Reduction criterion of separability and limits for a class of distillation protocols”**. *Physical Review A* 59.6 (June 1999), pp. 4206–4216. quant-ph: quant-ph/9708015.
- [HHH96] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. **“Separability of mixed states: necessary and sufficient conditions”**. *Physics Letters A* 223.1 (1996), pp. 1–8. arXiv: quant-ph/9605038.

- [HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. “**Mixed-State Entanglement and Distillation: Is there a “Bound” Entanglement in Nature?**” *Physical Review Letters* 80 (24 June 1998), pp. 5239–5242. arXiv: quant-ph/9801069.
- [Hor97] Paweł Horodecki. “**Separability criterion and inseparable mixed states with positive partial transposition**”. *Physics Letters A* 232.5 (1997), pp. 333–339. arXiv: quant-ph/9703004.
- [Wil16] Mark M. Wilde. **Quantum information theory**. 2nd ed. Cambridge University Press, 2016. arXiv: 1106.1445 [quant-ph].