

Chapter 0: Brief definitions and basic concepts

As the future version of me might forgot everything we have over the summer, as I did for now, I will make a review again from the simple definition to recall the necessary information to tell you why we are here and how we are going to proceed.

This section serve as reference for definitions, notations, and theorems that we will use later. This section can be safely ignored if you are already familiar with the definitions and theorems.

But for the future self who might have no idea what I'm talking about, we will provided detailed definitions to you to understand the concepts.

0.1 Complex vector spaces

The main vector space we are interested in is \mathbb{C}^n ; therefore, all the linear operators we defined are from \mathbb{C}^n to \mathbb{C}^n .

Definition 1. We denote a vector in vector space as $|\psi\rangle = (z_1, \dots, z_n)$ (might also be infinite dimensional, and $z_i \in \mathbb{C}$).

Here ψ is just a label for the vector, and you don't need to worry about it too much. This is also called the ket, where the counterpart $\langle\psi|$ is called the bra, used to denote the vector dual to ψ ; such an element is a linear functional if you really want to know what that is.

Few additional notation will be introduced, in this document, we will follows the notation used in mathematics literature [axler2023linear]

- $\langle\psi|\varphi\rangle$ is the inner product between two vectors, and $\langle\psi|A|\varphi\rangle$ is the inner product between $A|\varphi\rangle$ and $\langle\psi|$, or equivalently $A^\dagger\langle\psi|$ and $|\varphi\rangle$.
- Given a complex matrix $A = \mathbb{C}^{n \times n}$,
 1. \bar{A} is the complex conjugate of A .

Example

$$A = \begin{bmatrix} 1+i & 2+i & 3+i \\ 4+i & 5+i & 6+i \\ 7+i & 8+i & 9+i \end{bmatrix}, \bar{A} = \begin{bmatrix} 1-i & 2-i & 3-i \\ 4-i & 5-i & 6-i \\ 7-i & 8-i & 9-i \end{bmatrix}$$

2. A^\top denotes the transpose of A .

Example

$$A = \begin{bmatrix} 1+i & 2+i & 3+i \\ 4+i & 5+i & 6+i \\ 7+i & 8+i & 9+i \end{bmatrix}, A^\top = \begin{bmatrix} 1+i & 4+i & 7+i \\ 2+i & 5+i & 8+i \\ 3+i & 6+i & 9+i \end{bmatrix}$$

3. $A^* = \overline{(A^\top)}$ denotes the complex conjugate transpose, referred to as the adjoint, or Hermitian conjugate of A .

Example

$$A = \begin{bmatrix} 1+i & 2+i & 3+i \\ 4+i & 5+i & 6+i \\ 7+i & 8+i & 9+i \end{bmatrix}, A^* = \begin{bmatrix} 1-i & 4-i & 7-i \\ 2-i & 5-i & 8-i \\ 3-i & 6-i & 9-i \end{bmatrix}$$

4. A is unitary if $A^*A = AA^* = I$.
 5. A is self-adjoint (hermitian in physics literature) if $A^* = A$.

Motivation of Tensor product

Recall from the traditional notation of product space of two vector spaces V and W , that is, $V \times W$, is the set of all ordered pairs $(|v\rangle, |w\rangle)$ where $|v\rangle \in V$ and $|w\rangle \in W$.

The space has dimension $\dim V + \dim W$.

We want to define a vector space with the notation of multiplication of two vectors from different vector spaces.

That is

$$\begin{aligned} (|v_1\rangle + |v_2\rangle) \otimes |w\rangle &= (|v_1\rangle \otimes |w\rangle) + (|v_2\rangle \otimes |w\rangle) \\ |v\rangle \otimes (|w_1\rangle + |w_2\rangle) &= (|v\rangle \otimes |w_1\rangle) + (|v\rangle \otimes |w_2\rangle) \end{aligned}$$

and enables scalar multiplication by

$$\lambda(|v\rangle \otimes |w\rangle) = (\lambda|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\lambda|w\rangle)$$

And we wish to build a way to associate the basis of V and W with the basis of $V \otimes W$. That makes the tensor product a vector space with dimension $\dim V \times \dim W$.

Definition 2. *Definition of linear functional*

A linear functional is a linear map from V to \mathbb{F} .

Note the difference between a linear functional and a linear map.

A generalized linear map is a function $f : V \rightarrow W$ satisfying the condition.

- $f(|u\rangle + |v\rangle) = f(|u\rangle) + f(|v\rangle)$
- $f(\lambda |v\rangle) = \lambda f(|v\rangle)$

Definition 3. A bilinear functional is a bilinear function $\beta : V \times W \rightarrow \mathbb{F}$ satisfying the condition that $|v\rangle \rightarrow \beta(|v\rangle, |w\rangle)$ is a linear functional for all $|w\rangle \in W$ and $|w\rangle \rightarrow \beta(|v\rangle, |w\rangle)$ is a linear functional for all $|v\rangle \in V$.

The vector space of all bilinear functionals is denoted by $\mathcal{B}(V, W)$.

Definition 4. Let V, W be two vector spaces.

Let V' and W' be the dual spaces of V and W , respectively, that is $V' = \{\psi : V \rightarrow \mathbb{F}\}$ and $W' = \{\phi : W \rightarrow \mathbb{F}\}$, ψ, ϕ are linear functionals.

The tensor product of vectors $v \in V$ and $w \in W$ is the bilinear functional defined by $\forall(\psi, \phi) \in V' \times W'$ given by the notation

$$(v \otimes w)(\psi, \phi) = \psi(v)\phi(w)$$

The tensor product of two vector spaces V and W is the vector space $\mathcal{B}(V', W')$

Notice that the basis of such vector space is the linear combination of the basis of V' and W' , that is, if $\{e_i\}$ is the basis of V' and $\{f_j\}$ is the basis of W' , then $\{e_i \otimes f_j\}$ is the basis of $\mathcal{B}(V', W')$.

That is, every element of $\mathcal{B}(V', W')$ can be written as a linear combination of the basis.

Since $\{e_i\}$ and $\{f_j\}$ are bases of V' and W' , respectively, then we can always find a set of linear functionals $\{\phi_i\}$ and $\{\psi_j\}$ such that $\phi_i(e_j) = \delta_{ij}$ and $\psi_j(f_i) = \delta_{ij}$.

Here $\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$ is the Kronecker delta.

$$V \otimes W = \left\{ \sum_{i=1}^n \sum_{j=1}^m a_{ij} \phi_i(v) \psi_j(w) : \phi_i \in V', \psi_j \in W' \right\}$$

Note that $\sum_{i=1}^n \sum_{j=1}^m a_{ij} \phi_i(v) \psi_j(w)$ is a bilinear functional that maps $V' \times W'$ to \mathbb{F} .

This enables basis-free construction of vector spaces with proper multiplication and scalar multiplication.

Examples of tensor product for vectors

Let $V = \mathbb{C}^2, W = \mathbb{C}^3$, choose bases $\{|0\rangle, |1\rangle\} \subset V, \{|0\rangle, |1\rangle, |2\rangle\} \subset W$.

$$v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = v_1 |0\rangle + v_2 |1\rangle \in V, w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = w_1 |0\rangle + w_2 |1\rangle + w_3 |2\rangle \in W$$

Then the tensor product $v \otimes w$ is given by

$$v \otimes w = \begin{pmatrix} v_1 w_1 & v_1 w_2 & v_1 w_3 \\ v_2 w_1 & v_2 w_2 & v_2 w_3 \end{pmatrix} \in \mathbb{C}^6$$

Examples of tensor product for vector spaces

Let $V = \mathbb{C}^2, W = \mathbb{C}^3$, choose bases $\{|0\rangle, |1\rangle\} \subset V, \{|0\rangle, |1\rangle, |2\rangle\} \subset W$.

Then a basis of the tensor product is

$$\{|00\rangle, |01\rangle, |02\rangle, |10\rangle, |11\rangle, |12\rangle\},$$

where $|ij\rangle := |i\rangle \otimes |j\rangle$.

An example element of $V \otimes W$ is

$$|\psi\rangle = 2|0\rangle \otimes |1\rangle + (1+i)|1\rangle \otimes |0\rangle - i|1\rangle \otimes |2\rangle.$$

With respect to the ordered basis

$$(|00\rangle, |01\rangle, |02\rangle, |10\rangle, |11\rangle, |12\rangle),$$

this tensor corresponds to the coordinate vector

$$|\psi\rangle \longleftrightarrow \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1+i \\ 0 \\ -i \end{pmatrix} \in \mathbb{C}^6.$$

Using the canonical identification

$$\mathbb{C}^2 \otimes \mathbb{C}^3 \cong \mathbb{C}^{2 \times 3},$$

where

$$|i\rangle \otimes |j\rangle \mapsto E_{ij},$$

the same tensor is represented by the matrix

$$|\psi\rangle \longleftrightarrow \begin{pmatrix} 0 & 2 & 0 \\ 1+i & 0 & -i \end{pmatrix}.$$

Definition 5. The vector space defined by the tensor product is equipped with the unique inner product $\langle v \otimes w, u \otimes x \rangle_{V \otimes W} : V \otimes W \times V \otimes W \rightarrow \mathbb{F}$ defined by

$$\langle v \otimes w, u \otimes x \rangle = \langle v, u \rangle_V \langle w, x \rangle_W$$

In practice, we ignore the subscript of the vector space and just write $\langle v \otimes w, u \otimes x \rangle = \langle v, u \rangle \langle w, x \rangle$.
Partial trace

Definition 6. Let T be a linear operator on \mathcal{H} , (e_1, e_2, \dots, e_n) be a basis of \mathcal{H} and $(\epsilon_1, \epsilon_2, \dots, \epsilon_n)$ be a basis of dual space \mathcal{H}^* . Then the trace of T is defined by

$$\text{Tr}(T) = \sum_{i=1}^n \epsilon_i(T(e_i)) = \sum_{i=1}^n \langle e_i, T(e_i) \rangle$$

This is equivalent to the sum of the diagonal elements of T .

Definition 7. Let T be a linear operator on $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$, where \mathcal{A} and \mathcal{B} are finite-dimensional Hilbert spaces.

An operator T on $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$ can be written as

$$T = \sum_{i=1}^n a_i A_i \otimes B_i$$

where A_i is a linear operator on \mathcal{A} and B_i is a linear operator on \mathcal{B} .

The \mathcal{B} -partial trace of T ($\text{Tr}_{\mathcal{B}}(T) : \mathcal{L}(\mathcal{A} \otimes \mathcal{B}) \rightarrow \mathcal{L}(\mathcal{A})$) is the linear operator on \mathcal{A} defined by

$$\text{Tr}_{\mathcal{B}}(T) = \sum_{i=1}^n a_i \text{Tr}(B_i) A_i$$

Or we can define the map $L_v : \mathcal{A} \rightarrow \mathcal{A} \otimes \mathcal{B}$ by

$$L_v(u) = u \otimes v$$

Note that $\langle u, L_v^*(u') \otimes v' \rangle = \langle u, u' \rangle \langle v, v' \rangle = \langle u \otimes v, u' \otimes v' \rangle = \langle L_v(u), u' \otimes v' \rangle$.

Therefore, $L_v^* \sum_j u_j \otimes v_j = \sum_j \langle v, v_j \rangle u_j$.

Then the partial trace of T can also be defined by

Let $\{v_j\}$ be a set of orthonormal basis of \mathcal{B} .

$$\text{Tr}_{\mathcal{B}}(T) = \sum_j L_{v_j}^*(T) L_{v_j}$$

Definition 8. Let T be a linear operator on $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$, where \mathcal{A} and \mathcal{B} are finite-dimensional Hilbert spaces.

Let ρ be a state on \mathcal{B} consisting of orthonormal basis $\{v_j\}$ and eigenvalue $\{\lambda_j\}$.

The partial trace of T with respect to ρ is the linear operator on \mathcal{A} defined by

$$\text{Tr}_{\mathcal{A}}(T) = \sum_j \lambda_j L_{v_j}^*(T) L_{v_j}$$

This introduces a new model in mathematics explaining quantum mechanics: the non-commutative probability theory.

0.2 Non-commutative probability theory

The non-commutative probability theory is a branch of generalized probability theory that studies the probability of events in non-commutative algebras.

There are several main components of the generalized probability theory; let's see how we can formulate them, comparing with the classical probability theory.

First, we define the Hilbert space in case one did not make the step from the linear algebra courses like me.

Definition 9. *Hilbert space:*

A Hilbert space is a complete inner product space.

That is, a vector space equipped with an inner product, with the induced metric defined by the norm of the inner product, we have a metric space, which is complete. Reminds that complete mean that every Cauchy sequence, the sequence such that for any $\epsilon > 0$, there exists an N such that for all $m, n \geq N$, we have $|x_m - x_n| < \epsilon$, converges to a limit.

As a side note we will use later, we also defined the Borel measure on a space, here we use the following definition specialized for the space (manifolds) we are interested in.

Definition 10. *Borel measure:*

Let X be a topological space, then a Borel measure $\mu : \mathcal{B}(X) \rightarrow [0, \infty]$ on X is a measure on the Borel σ -algebra of X $\mathcal{B}(X)$ satisfying the following properties:

1. $X \in \mathcal{B}$.
2. *Close under complement: If $A \subseteq X$, then $\mu(A^c) = \mu(X) - \mu(A)$*
3. *Close under countable unions; If E_1, E_2, \dots are disjoint sets, then $\mu(\bigcup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i)$*

In later sections, we will use Lebesgue measure, and Haar measure for various circumstances, their detailed definition may be introduced in later sections.

Example

To introduce an example of Hilbert space we use when studying quantum mechanics, we need to introduce a common inner product used in \mathbb{C}^n .

Proposition 11. *The Hermitian inner product on the complex vector space \mathbb{C}^n makes it a Hilbert space.*

Proof. We first verify that the Hermitian inner product

$$\langle u, v \rangle = \sum_{i=1}^n \bar{u}_i v_i$$

on \mathbb{C}^n satisfies the axioms of an inner product:

1. **Conjugate symmetry:** For all $u, v \in \mathbb{C}^n$,

$$\langle u, v \rangle = \sum_{i=1}^n \bar{u}_i v_i = \overline{\sum_{i=1}^n v_i u_i} = \overline{\langle v, u \rangle}.$$

2. **Linearity:** For any $u, v, w \in \mathbb{C}^n$ and scalars $a, b \in \mathbb{C}$, we have

$$\langle u, av + bw \rangle = \sum_{i=1}^n \bar{u}_i(av_i + bw_i) = a\langle u, v \rangle + b\langle u, w \rangle.$$

3. **Positive definiteness:** For every $u = (u_1, u_2, \dots, u_n) \in \mathbb{C}^n$, let $u_j = a_j + b_j i$, where $a_j, b_j \in \mathbb{R}$.

$$\langle u, u \rangle = \sum_{j=1}^n \bar{u}_j u_j = \sum_{i=1}^n (a_i^2 + b_i^2) \geq 0,$$

with equality if and only if $u = 0$.

Therefore, the Hermitian inner product is an inner product.

Next, we show that \mathbb{C}^n is complete with respect to the norm induced by this inner product:

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

Since \mathbb{C}^n is finite-dimensional, every Cauchy sequence (with respect to any norm) converges in \mathbb{C}^n . This is a standard result in finite-dimensional normed spaces, which implies that \mathbb{C}^n is indeed complete.

Therefore, since the Hermitian inner product fulfills the inner product axioms and \mathbb{C}^n is complete, the complex vector space \mathbb{C}^n with the Hermitian inner product is a Hilbert space. \square

Another classical example of Hilbert space is $L^2(\Omega, \mathcal{F}, P)$, where (Ω, \mathcal{F}, P) is a measure space (Ω is a set, \mathcal{F} is a σ -algebra on Ω , and P is a measure on \mathcal{F}). The L^2 space is the space of all function on Ω that is

1. **square integrable:** square integrable functions are the functions $f : \Omega \rightarrow \mathbb{C}$ such that

$$\int_{\Omega} |f(\omega)|^2 dP(\omega) < \infty$$

with inner product defined by

$$\langle f, g \rangle = \int_{\Omega} \overline{f(\omega)} g(\omega) dP(\omega)$$

2. **complex-valued:** functions are complex-valued measurable. $f = u + vi$ is complex-valued if u and v are real-valued measurable.

Example

Proposition 12. $L^2(\Omega, \mathcal{F}, P)$ is a Hilbert space.

Proof. We check the two conditions of the Hilbert space:

- **Completeness:** Let (f_n) be a Cauchy sequence in $L^2(\Omega, \mathcal{F}, P)$. Then for any $\epsilon > 0$, there exists an N such that for all $m, n \geq N$, we have

$$\int_{\Omega} |f_m(\omega) - f_n(\omega)|^2 dP(\omega) < \epsilon^2$$

This means that (f_n) is a Cauchy sequence in the norm of $L^2(\Omega, \mathcal{F}, P)$.

- Inner product: The inner product is defined by

$$\langle f, g \rangle = \int_{\Omega} \overline{f(\omega)} g(\omega) dP(\omega)$$

This is a well-defined inner product on $L^2(\Omega, \mathcal{F}, P)$. We can check the properties of the inner product:

- Linearity:

$$\langle af + bg, h \rangle = a\langle f, h \rangle + b\langle g, h \rangle$$

- Conjugate symmetry:

$$\langle f, g \rangle = \overline{\langle g, f \rangle}$$

- Positive definiteness:

$$\langle f, f \rangle \geq 0$$

□

Let \mathcal{H} be a Hilbert space. \mathcal{H} consists of complex-valued functions on a finite set $\Omega = \{1, 2, \dots, n\}$, and the functions (e_1, e_2, \dots, e_n) form an orthonormal basis of \mathcal{H} . (We use Dirac notation $|k\rangle$ to denote the basis vector e_k [parthasarathy1992quantum].)

As an analog to the classical probability space $(\Omega, \mathcal{F}, \mu)$, which consists of a sample space Ω and a probability measure μ on the state space \mathcal{F} , the non-commutative probability space $(\mathcal{H}, \mathcal{P}, \rho)$ consists of a Hilbert space \mathcal{H} and a state ρ on the space of all orthogonal projections \mathcal{P} .

The detailed definition of the non-commutative probability space is given below:

Definition 13. *Non-commutative probability space:*

A non-commutative probability space is a pair $(\mathcal{B}(\mathcal{H}), \mathcal{P})$, where $\mathcal{B}(\mathcal{H})$ is the set of all **bounded** linear operators on \mathcal{H} .

A linear operator on \mathcal{H} is **bounded** if for all u such that $\|u\| \leq 1$, we have $\|Au\| \leq M$ for some $M > 0$.

\mathcal{P} is the set of all orthogonal projections on $\mathcal{B}(\mathcal{H})$.

The set $\mathcal{P} = \{P \in \mathcal{B}(\mathcal{H}) : P^* = P = P^2\}$ is the set of all orthogonal projections on $\mathcal{B}(\mathcal{H})$.

Recall from classical probability theory, we call the initial probability distribution for possible outcomes in the classical probability theory as our *state*, similarly, we need to define the *state* in the non-commutative probability theory.

Definition 14. *Non-commutative probability state:*

Given a non-commutative probability space $(\mathcal{B}(\mathcal{H}), \mathcal{P})$,

A state is a unit vector $|\psi\rangle$ in the Hilbert space \mathcal{H} , such that $\langle \psi | \psi \rangle = 1$.

Every state uniquely defines a map $\rho : \mathcal{P} \rightarrow [0, 1]$, $\rho(P) = \langle \psi | P | \psi \rangle$ (commonly named as density operator) such that:

- $\rho(O) = 0$, where O is the zero projection, and $\rho(I) = 1$, where I is the identity projection.

- If P_1, P_2, \dots, P_n are pairwise disjoint orthogonal projections, then $\rho(P_1 + P_2 + \dots + P_n) = \sum_{i=1}^n \rho(P_i)$.

Note that the pure states are the density operators that can be represented by a unit vector $|\psi\rangle$ in the Hilbert space \mathcal{H} , whereas mixed states are the density operators that cannot be represented by a unit vector in the Hilbert space \mathcal{H} .

If $(|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle)$ is an orthonormal basis of \mathcal{H} consisting of eigenvectors of ρ , for the eigenvalues p_1, p_2, \dots, p_n , then $p_j \geq 0$ and $\sum_{j=1}^n p_j = 1$.

We can write ρ as

$$\rho = \sum_{j=1}^n p_j |\psi_j\rangle \langle \psi_j|$$

(Under basis $|\psi_j\rangle$, it is a diagonal matrix with p_j on the diagonal.)

The counterpart of the random variable in the non-commutative probability theory is called an observable, which is a Hermitian operator on \mathcal{H} (for all ψ, ϕ in the domain of A , we have $\langle A\psi, \phi \rangle = \langle \psi, A\phi \rangle$). This kind of operator ensures that our outcome interpreted as probability is a real number).

Definition 15. *Observable:*

Let $\mathcal{B}(\mathbb{R})$ be the set of all Borel sets on \mathbb{R} .

An (real-valued) observable (random variable) on the Hilbert space \mathcal{H} , denoted by A , is a projection-valued map (measure) $P_A : \mathcal{B}(\mathbb{R}) \rightarrow \mathcal{P}(\mathcal{H})$.

Satisfies the following properties:

- $P_A(\emptyset) = O$ (the zero projection)
- $P_A(\mathbb{R}) = I$ (the identity projection)
- For any sequence $A_1, A_2, \dots, A_n \in \mathcal{B}(\mathbb{R})$, the following holds:
 - $P_A(\bigcup_{i=1}^n A_i) = \bigvee_{i=1}^n P_A(A_i)$
 - $P_A(\bigcap_{i=1}^n A_i) = \bigwedge_{i=1}^n P_A(A_i)$
 - $P_A(A^c) = I - P_A(A), \forall A \in \mathcal{B}(\mathbb{R})$

If A is an observable determined by the map $P_A : \mathcal{B}(\mathbb{R}) \rightarrow \mathcal{P}(\mathcal{H})$, P_A is a spectral measure (a complete additive orthogonal projection valued measure on $\mathcal{B}(\mathbb{R})$). And every spectral measure can be represented by an observable. **[parthasarathy2005mathematical]**

Proposition 16. *If A_j are mutually disjoint (that is $P_A(A_i)P_A(A_j) = P_A(A_j)P_A(A_i) = O$ for $i \neq j$), then $P_A(\bigcup_{j=1}^n A_j) = \sum_{j=1}^n P_A(A_j)$*

Definition 17. *Probability of a random variable:*

Let A be a real-valued observable on a Hilbert space \mathcal{H} . ρ be a state. The probability of observing the outcome $E \in \mathcal{B}(\mathbb{R})$ is given by:

$$\mu(E) = \text{Tr}(\rho P_A(E))$$

Restriction of a quantum state to a commutative subalgebra defines an ordinary probability measure.

Example

Let

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The eigenvalues of Z are $+1$ and -1 , with corresponding normalized eigenvectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The spectral projections are

$$P_Z(\{1\}) = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_Z(\{-1\}) = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

The associated projection-valued measure P_Z satisfies

$$P_Z(\{1, -1\}) = I, \quad P_Z(\emptyset) = 0.$$

Let

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The normalized eigenvectors of X are

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

with eigenvalues $+1$ and -1 , respectively.

The corresponding spectral projections are

$$P_X(\{1\}) = |+\rangle\langle +| = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

$$P_X(\{-1\}) = |-\rangle\langle -| = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

Compute

$$P_Z(\{1\})P_X(\{1\}) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

On the other hand,

$$P_X(\{1\})P_Z(\{1\}) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

Since

$$P_Z(\{1\})P_X(\{1\}) \neq P_X(\{1\})P_Z(\{1\}),$$

the projections do not commute.

Let ρ be a density operator on \mathbb{C}^2 , i.e.

$$\rho \geq 0, \quad \text{Tr}(\rho) = 1.$$

For a pure state $|\psi\rangle$, one has

$$\rho = |\psi\rangle\langle\psi|.$$

The probability that a measurement associated with a PVM P yields an outcome in a Borel set $A \in \mathcal{B}$ is

$$\mathbb{P}(A) = \text{Tr}(\rho P(A)).$$

For example, let

$$\rho = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then

$$\text{Tr}(\rho P_Z(\{1\})) = 1, \quad \text{Tr}(\rho P_X(\{1\})) = \frac{1}{2}.$$

Definition 18. *Definition of measurement:*

A measurement (observation) of a system prepared in a given state produces an outcome x , x is a physical event that is a subset of the set of all possible outcomes. For each x , we associate a measurement operator M_x on \mathcal{H} .

Given the initial state (pure state, unit vector) u , the probability of measurement outcome x is given by:

$$p(x) = \|M_x u\|^2$$

Note that to make sense of this definition, the collection of measurement operators $\{M_x\}$ must satisfy the completeness requirement:

$$1 = \sum_{x \in X} p(x) = \sum_{x \in X} \|M_x u\|^2 = \sum_{x \in X} \langle M_x u, M_x u \rangle = \langle u, (\sum_{x \in X} M_x^* M_x) u \rangle$$

So $\sum_{x \in X} M_x^ M_x = I$.*

Here is Table 1 summarizing the analog of classical probability theory and non-commutative (*quantum*) probability theory [**Feres**]:

Table 1: Analog of classical probability theory and non-commutative (*quantum*) probability theory

Classical probability	Non-commutative probability
Sample space Ω , cardinality $ \Omega = n$, example: $\Omega = \{0, 1\}$	Complex Hilbert space \mathcal{H} , dimension $\dim \mathcal{H} = n$, example: $\mathcal{H} = \mathbb{C}^2$
Common algebra of \mathbb{C} valued functions	Algebra of bounded operators $\mathcal{B}(\mathcal{H})$
$f \mapsto \bar{f}$ complex conjugation	$P \mapsto P^*$ adjoint
Events: indicator functions of sets	Projections: space of orthogonal projections $\mathcal{P} \subseteq \mathcal{B}(\mathcal{H})$
functions f such that $f^2 = f = \bar{f}$	orthogonal projections P such that $P^* = P = P^2$
\mathbb{R} -valued functions $f = \bar{f}$	self-adjoint operators $A = A^*$
$\mathbb{I}_{f^{-1}(\{\lambda\})}$ is the indicator function of the set $f^{-1}(\{\lambda\})$	$P(\lambda)$ is the orthogonal projection to eigenspace
$f = \sum_{\lambda \in \text{Range}(f)} \lambda \mathbb{I}_{f^{-1}(\{\lambda\})}$	$A = \sum_{\lambda \in \text{sp}(A)} \lambda P(\lambda)$
Probability measure μ on Ω	Density operator ρ on \mathcal{H}
Delta measure δ_ω	Pure state $\rho = \psi\rangle\langle\psi $
μ is non-negative measure and $\sum_{i=1}^n \mu(\{i\}) = 1$	ρ is positive semi-definite and $\text{Tr}(\rho) = 1$
Expected value of random variable f is $\mathbb{E}_\mu(f) = \sum_{i=1}^n f(i)\mu(\{i\})$	Expected value of operator A is $\mathbb{E}_\rho(A) = \text{Tr}(\rho A)$
Variance of random variable f is $\text{Var}_\mu(f) = \sum_{i=1}^n (f(i) - \mathbb{E}_\mu(f))^2 \mu(\{i\})$	Variance of operator A is $\text{Var}_\rho(A) = \text{Tr}(\rho A^2) - \text{Tr}(\rho A)^2$
Covariance of random variables f and g is $\text{Cov}_\mu(f, g) = \sum_{i=1}^n (f(i) - \mathbb{E}_\mu(f))(g(i) - \mathbb{E}_\mu(g))\mu(\{i\})$	Covariance of operators A and B is $\text{Cov}_\rho(A, B) = \text{Tr}(\rho A \circ B) - \text{Tr}(\rho A) \text{Tr}(\rho B)$
Composite system is given by Cartesian product of the sample spaces $\Omega_1 \times \Omega_2$	Composite system is given by tensor product of the Hilbert spaces $\mathcal{H}_1 \otimes \mathcal{H}_2$
Product measure $\mu_1 \times \mu_2$ on $\Omega_1 \times \Omega_2$	Tensor product of space $\rho_1 \otimes \rho_2$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$
Marginal distribution $\pi_* v$	Partial trace $\text{Tr}_2(\rho)$

0.3 Manifolds

In this section, we will introduce some basic definitions and theorems used in manifold theory that are relevant to our study. Assuming no prior knowledge of manifold theory but basic topology understanding. We will provide brief definitions and explanations for each term. From the most abstract Manifold definition to the Riemannian manifolds and related theorems.

0.3.1 Manifolds

Definition 19. *An m -manifold is a Topological space X that is*

1. *Hausdorff: every distinct two points in X can be separated by two disjoint open sets.*

2. *Second countable: X has countable basis.*
3. *Every point p has an open neighborhood $p \in U$ that is homeomorphic to an open subset of \mathbb{R}^m .*

Example

Let $X = \mathbb{R}$ and $\mathcal{B} = \{(a, b) | a, b \in \mathbb{R}, a < b\}$ (collection of all open intervals with rational endpoints).

Since the rational numbers are countable, so \mathcal{B} is countable.

So \mathbb{R} is second countable.

Likewise, \mathbb{R}^n is also second countable.

Example

1-manifold is a curve and 2-manifold is a surface.

Theorem 20. *Whitney's Embedding Theorem:*

If X is a compact m -manifold, then X can be imbedded in \mathbb{R}^n for some n .

This proof is from topology course, and use additional one lemma:

Lemma 21. *Let $\{U_i\}_{i=1}^n$ be a finite open cover of a normal space X (Every pair of closed sets in X can be separated by two open sets in X).*

Then there exists a partition of unity dominated by $\{U_i\}_{i=1}^n$.

Proof. Since X is a m compact manifold, $\forall x \in X$, there is an open neighborhood U_x of x such that U_x is homeomorphic to \mathbb{R}^m . That means there exists $\varphi_i : U_x \rightarrow \varphi(U_x) \subseteq \mathbb{R}^m$.

Where $\{U_x\}_{x \in X}$ is an open cover of X . Since X is compact, there is a finite subcover $\bigcup_{i=1}^k U_{x_i} = X$.

Apply the existence of a finite partition of unity, we can find a partition of unity dominated by $\{U_{x_i}\}_{i=1}^k$. With family of functions $\phi_i : \mathbb{R}^d \rightarrow [0, 1]$.

Define $h_i : X \rightarrow \mathbb{R}^m$ by

$$h_i(x) = \begin{cases} \phi_i(x)\varphi_i(x) & \text{if } x = x_i \\ 0 & \text{otherwise} \end{cases}$$

We claim that h_i is continuous using pasting lemma.

On U_i , $h_i = \phi_i\varphi_i$ is product of two continuous functions therefore continuous.

On $X - \text{supp}(\phi_i)$, $h_i = 0$ is continuous.

By pasting lemma, h_i is continuous.

Define

$$F : X \rightarrow (\mathbb{R}^m \times \mathbb{R})^n$$

where $x \mapsto (h_1(x), \varphi_1(x), h_2(x), \varphi_2(x), \dots, h_n(x), \varphi_n(x))$

We want to show that F is imbedding map.

1. F is continuous

since it is a product of continuous functions.

2. F is injective

that is, if $F(x_1) = F(x_2)$, then $x_1 = x_2$.

By partition of unity, we have,

$$h_1(x_1) = h_1(x_2), h_2(x_1) = h_2(x_2), \dots, h_n(x_1) = h_n(x_2).$$

$$\text{And } \varphi_1(x_1) = \varphi_1(x_2), \varphi_2(x_1) = \varphi_2(x_2), \dots, \varphi_n(x_1) = \varphi_n(x_2).$$

Because $\sum_{i=1}^n \varphi_i(x_1) = 1$, therefore there exists $\varphi_i(x_1) = \varphi_i(x_2) > 0$.

Therefore $x_1, x_2 \in \text{supp}(\phi_i) \subseteq U_i$.

By definition of h , $h_i(x_1) = h_i(x_2)$, $\varphi_i(x_1)\phi_i(x_1) = \varphi_i(x_2)\phi_i(x_2)$.

Using cancellation, $\phi_i(x_1) = \phi_i(x_2)$.

Therefore $x_1 = x_2$ since $\phi_i(x_1) = \phi_i(x_2)$ is a homeomorphism.

In this proof, φ ensures the imbedding is properly defined on the open sets

3. F is a homeomorphism.

Note that if $f : X \rightarrow Y$ is continuous and X is compact, Y is Hausdorff, then f is a closed map.

$F : X \rightarrow F(X)$ is a bijective map from a compact space to a Hausdorff space, therefore F is a closed map.

Since F is continuous, then $F^{-1}(C)$ where C is a closed set in $F(X)$, $F^{-1}(C)$ is closed in X .

Therefore F is a homeomorphism.

□

0.3.2 Smooth manifolds and Lie groups

This section is adopted from [lee·introduction·2012]

Definition 22. Let $U \subseteq \mathbb{R}^n$ and $f : U \rightarrow \mathbb{R}^n$ be a map.

For any $a = (a_1, \dots, a_n) \in U$, $j \in \{1, \dots, n\}$, the j -th partial derivative of F at a is defined as

$$\begin{aligned} \frac{\partial f}{\partial x_j}(a) &= \lim_{h \rightarrow 0} \frac{f(a_1, \dots, a_j + h, \dots, a_n) - f(a_1, \dots, a_j, \dots, a_n)}{h} \\ &= \lim_{h \rightarrow 0} \frac{f(a + he_j) - f(a)}{h} \end{aligned}$$

Definition 23. Let $U \subseteq \mathbb{R}^n$ and $f : U \rightarrow \mathbb{R}^n$ be a map.

If for any $j \in \{1, \dots, n\}$, the j -th partial derivative of f is continuous at a , then f is continuously differentiable at a .

If $\forall a \in U$, $\frac{\partial f}{\partial x_j}$ exists and is continuous at a , then f is continuously differentiable on U . or C^1 map. (Note that C^0 map is just a continuous map.)

Definition 24. A function $f : U \rightarrow \mathbb{R}^n$ is smooth if it is of class C^k for every $k \geq 0$ on U . Such function is called a diffeomorphism if it is also a **bijection** and its **inverse is also smooth**.

Definition 25. Let M be a smooth manifold. A **chart** is a pair (U, φ) where $U \subseteq M$ is an open subset and $\varphi : U \rightarrow \hat{U} \subseteq \mathbb{R}^n$ is a homeomorphism (a continuous bijection map and its inverse is also continuous).

If $p \in U$ and $\varphi(p) = 0$, then we say that p is the origin of the chart (U, φ) .

For $p \in U$, we note that the continuous function $\varphi(p) = (x_1(p), \dots, x_n(p))$ gives a vector in \mathbb{R}^n . The $(x_1(p), \dots, x_n(p))$ is called the **local coordinates** of p in the chart (U, φ) .

Definition 26. Let M be a smooth manifold. An **atlas** is a collection of charts $\mathcal{A} = \{(U_\alpha, \phi_\alpha)\}_{\alpha \in I}$ such that $M = \bigcup_{\alpha \in I} U_\alpha$.

An atlas is said to be **smooth** if the transition maps $\phi_\alpha \circ \phi_\beta^{-1} : \phi_\beta(U_\alpha \cap U_\beta) \rightarrow \phi_\alpha(U_\alpha \cap U_\beta)$ are smooth for all $\alpha, \beta \in I$.

Definition 27. A smooth manifold is a pair (M, \mathcal{A}) where M is a topological manifold and \mathcal{A} is a smooth atlas.

Definition 28. Let M and N be smooth manifolds, and $f : M \rightarrow N$ be a smooth map. For each $p \in M$, the **differential** of f at p is the linear map

$$df_p : T_p M \rightarrow T_{f(p)} N$$

Definition 29. A smooth map $f : M \rightarrow N$ is a **smooth submersion** if for each $p \in M$, the differential $F : M \rightarrow N$ is surjective.

Or equivalently $\text{rank}(F) = \dim N$ for each $p \in M$.

Here are some additional propositions that will be helpful for our study in later sections:

This one is from [lee'introduction'2012] Theorem 4.26

Theorem 30. Let M and N be smooth manifolds and $\pi : M \rightarrow N$ is a smooth map. Then π is a smooth submersion if and only if every point of M is in the image of a smooth local section of π (a local section of π is a map $\sigma : U \rightarrow M$ defined on some open subset $U \subseteq N$ with $\pi \circ \sigma = \text{Id}_U$).

0.3.3 Riemannian manifolds

Definition 31. Let M be a smooth manifold. A **Riemannian metric** on M is a smooth covariant tensor field $g \in \mathcal{T}^2(M)$ such that for each $p \in M$, g_p is an inner product on $T_p M$.

$g_p(v, v) \geq 0$ for each $p \in M$ and each $v \in T_p M$. equality holds if and only if $v = 0$.

Definition 32. Suppose (\tilde{M}, \tilde{g}) and (M, g) are smooth Riemannian manifolds, and $\pi : \tilde{M} \rightarrow M$ is a smooth submersion. Then π is said to be a **Riemannian submersion** if for each $x \in \tilde{M}$, the differential $d\pi_x : \tilde{g}_x \rightarrow g_{\pi(x)}$ restricts to a linear isometry from H_x onto $T_{\pi(x)} M$.

In other words, $\tilde{g}_x(v, w) = g_{\pi(x)}(d\pi_x(v), d\pi_x(w))$ whenever $v, w \in H_x$.

Theorem 33. Let (\tilde{M}, \tilde{g}) be a Riemannian manifold, let $\pi : \tilde{M} \rightarrow M$ be a surjective smooth submersion, and let G be a group acting on \tilde{M} . If the **action** is

1. *isometric*: the map $x \mapsto \varphi \cdot x$ is an isometry for each $\varphi \in G$.
2. *vertical*: every element $\varphi \in G$ takes each fiber to itself, that is $\pi(\varphi \cdot p) = \pi(p)$ for all $p \in \tilde{M}$.
3. *transitive on fibers*: for each $p, q \in \tilde{M}$ such that $\pi(p) = \pi(q)$, there exists $\varphi \in G$ such that $\varphi \cdot p = q$.

Then there is a unique Riemannian metric on M such that π is a Riemannian submersion.

Proof. For each $p \in \tilde{M}$, let

$$V_p := \ker(d\pi_p) \subseteq T_p\tilde{M}$$

be the vertical space, and let

$$H_p := V_p^{\perp_{\tilde{g}}}$$

be its \tilde{g} -orthogonal complement. Since π is a surjective smooth submersion, each $d\pi_p : T_p\tilde{M} \rightarrow T_{\pi(p)}M$ is surjective, so

$$T_p\tilde{M} = V_p \oplus H_p,$$

and therefore the restriction

$$d\pi_p|_{H_p} : H_p \rightarrow T_{\pi(p)}M$$

is a linear isomorphism.

We first show that the group action preserves the horizontal distribution. Fix $\varphi \in G$. Since the action is vertical, we have

$$\pi(\varphi \cdot x) = \pi(x) \quad \text{for all } x \in \tilde{M}.$$

Differentiating at p gives

$$d\pi_{\varphi \cdot p} \circ d\varphi_p = d\pi_p.$$

Hence if $v \in V_p = \ker(d\pi_p)$, then

$$d\pi_{\varphi \cdot p}(d\varphi_p v) = d\pi_p(v) = 0,$$

so $d\varphi_p(V_p) \subseteq V_{\varphi \cdot p}$. Since φ acts isometrically, $d\varphi_p$ is a linear isometry, and thus it preserves orthogonal complements. Therefore

$$d\varphi_p(H_p) = H_{\varphi \cdot p}.$$

We now define a metric on M . Let $m \in M$, and choose any $p \in \pi^{-1}(m)$. For $u, v \in T_m M$, let $\tilde{u}, \tilde{v} \in H_p$ be the unique horizontal lifts satisfying

$$d\pi_p(\tilde{u}) = u, \quad d\pi_p(\tilde{v}) = v.$$

Define

$$g_m(u, v) := \tilde{g}_p(\tilde{u}, \tilde{v}).$$

This is a symmetric bilinear form on $T_m M$, and it is positive definite because \tilde{g}_p is positive definite on H_p and $d\pi_p|_{H_p}$ is an isomorphism.

It remains to show that this definition is independent of the choice of p in the fiber. Suppose $p, q \in \pi^{-1}(m)$. By transitivity of the action on fibers, there exists $\varphi \in G$ such that $\varphi \cdot p = q$. Let $\tilde{u}_p, \tilde{v}_p \in H_p$ be the horizontal lifts of u, v at p , and define

$$\tilde{u}_q := d\varphi_p(\tilde{u}_p), \quad \tilde{v}_q := d\varphi_p(\tilde{v}_p).$$

By the previous paragraph, $\tilde{u}_q, \tilde{v}_q \in H_q$. Moreover,

$$d\pi_q(\tilde{u}_q) = d\pi_q(d\varphi_p\tilde{u}_p) = d\pi_p(\tilde{u}_p) = u,$$

and similarly $d\pi_q(\tilde{v}_q) = v$. Thus \tilde{u}_q, \tilde{v}_q are exactly the horizontal lifts of u, v at q . Since φ is an isometry,

$$\tilde{g}_q(\tilde{u}_q, \tilde{v}_q) = \tilde{g}_q(d\varphi_p\tilde{u}_p, d\varphi_p\tilde{v}_p) = \tilde{g}_p(\tilde{u}_p, \tilde{v}_p).$$

Therefore $g_m(u, v)$ is independent of the chosen point $p \in \pi^{-1}(m)$, so g is well defined on M .

Next we prove that g is smooth. Let $m_0 \in M$. Since π is a smooth submersion, there exists an open neighborhood $U \subseteq M$ of m_0 and a smooth local section

$$s : U \rightarrow \tilde{M} \quad \text{such that} \quad \pi \circ s = \text{id}_U.$$

Over $s(U)$, the vertical bundle $V = \ker d\pi$ is a smooth subbundle of $T\tilde{M}$, and hence so is its orthogonal complement $H = V^\perp$. For each $x \in U$, the restriction

$$d\pi_{s(x)}|_{H_{s(x)}} : H_{s(x)} \rightarrow T_x M$$

is a linear isomorphism, and these isomorphisms depend smoothly on x . Thus they define a smooth vector bundle isomorphism

$$d\pi|_H : H|_{s(U)} \rightarrow TU,$$

whose inverse is also smooth.

If X, Y are smooth vector fields on U , define their horizontal lifts along s by

$$X_x^H := (d\pi_{s(x)}|_{H_{s(x)}})^{-1}(X_x), \quad Y_x^H := (d\pi_{s(x)}|_{H_{s(x)}})^{-1}(Y_x).$$

Then X^H and Y^H are smooth vector fields along $s(U)$, and by construction,

$$g(X, Y)(x) = \tilde{g}_{s(x)}(X_x^H, Y_x^H).$$

Since the right-hand side depends smoothly on x , it follows that g is a smooth Riemannian metric on M .

By construction, for every $p \in \tilde{M}$ and every $\tilde{u}, \tilde{v} \in H_p$,

$$g_{\pi(p)}(d\pi_p\tilde{u}, d\pi_p\tilde{v}) = \tilde{g}_p(\tilde{u}, \tilde{v}).$$

Thus $d\pi_p : H_p \rightarrow T_{\pi(p)}M$ is an isometry for every p , so $\pi : (\tilde{M}, \tilde{g}) \rightarrow (M, g)$ is a Riemannian submersion.

Finally, uniqueness is immediate. Indeed, if g' is another Riemannian metric on M such that $\pi : (M, \tilde{g}) \rightarrow (M, g')$ is a Riemannian submersion, then for any $m \in M$, any $p \in \pi^{-1}(m)$, and any $u, v \in T_m M$, letting $\tilde{u}, \tilde{v} \in H_p$ denote the horizontal lifts of u, v , we must have

$$g'_m(u, v) = \tilde{g}_p(\tilde{u}, \tilde{v}) = g_m(u, v).$$

Hence $g' = g$.

Therefore there exists a unique Riemannian metric on M such that π is a Riemannian submersion. \square

0.3.4 Hopf fibration

There are some remaining steps for showing how the metric on Sphere induces the metric on complex projective space, now we will just drop the conclusion here so that we can continue our discussion:

- Every nonzero vector can be normalized, so each pure state has a representative on the unit sphere

$$S^{2n+1} \subset \mathbb{C}^{n+1}.$$

- Two unit vectors represent the same pure state exactly when they differ by a phase:

$$z \sim e^{i\theta} z.$$

- Therefore

$$\mathbb{C}P^n = S^{2n+1}/S^1.$$

The quotient map

$$p : S^{2n+1} \rightarrow \mathbb{C}P^n, \quad p(z) = [z] = \{\lambda z : \lambda \in \mathbb{C}^\times\},$$

is the **Hopf fibration**.

The geometric picture is

$$S^{2n+1} \xrightarrow{\text{Hopf fibration}} \mathbb{C}P^n, \quad \text{round metric} \rightsquigarrow \text{Fubini–Study metric}.$$

The sphere $S^{2n+1} \subset \mathbb{C}^{n+1}$ has the **round metric**

$$g_{\text{round}} = \sum_{j=0}^n (dx_j^2 + dy_j^2)|_{S^{2n+1}},$$

induced from the Euclidean metric on \mathbb{R}^{2n+2} .

In homogeneous coordinates $[z] \in \mathbb{C}P^n$, the **Fubini–Study metric** is

$$g_{FS} = \frac{\langle dz, dz \rangle \langle z, z \rangle - |\langle z, dz \rangle|^2}{\langle z, z \rangle^2},$$

0.4 Quantum physics and terminologies

In this section, we will introduce some terminologies and theorems used in quantum physics that are relevant to our study. Assuming no prior knowledge of quantum physics, we will provide brief definitions and explanations for each term.

One might ask, what is the fundamental difference between a quantum system and a classical system, and why can we not directly apply those theorems in classical computers to a quantum computer? It turns out that quantum error-correcting codes are hard due to the following definitions and features for quantum computing.

Definition 34. *All quantum operations can be constructed by composing four kinds of transformations: (adapted from Chapter 10 of [Bengtsson·Zyczkowski·2017])*

1. *Unitary operations.* $U(\cdot)$ for any quantum state. It is possible to apply a non-unitary operation for an open quantum system, but that is usually not the focus for quantum computing and usually leads to non-recoverable loss of information that we wish to obtain.
2. *Extend the system.* Given a quantum state $\rho \in \mathcal{H}^N$, we can extend it to a larger quantum system by "entangle" (For this report, you don't need to worry for how quantum entanglement works) it with some new states $\sigma \in \mathcal{H}^K$ (The space where the new state dwells is usually called ancilla system) and get $\rho' = \rho \otimes \sigma \in \mathcal{H}^N \otimes \mathcal{K}$.
3. *Partial trace.* Given a quantum state $\rho \in \mathcal{H}^N$ and some reference state $\sigma \in \mathcal{H}^K$, we can trace out some subsystems and get a new state $\rho' \in \mathcal{H}^{N-K}$.
4. *Selective measurement.* Given a quantum state, we measure it and get a classical bit; unlike the classical case, the measurement is a probabilistic operation. (More specifically, this is some projection to a reference state corresponding to a classical bit output. For this report, you don't need to worry about how such a result is obtained and how the reference state is constructed.)

$U(n)$ is the group of all $n \times n$ **unitary matrices** over \mathbb{C} ,

$$U(n) = \{A \in \mathbb{C}^{n \times n} : A^*A = AA^* = I_n\}$$

The uniqueness of such measurement came from the lemma below [Elizabeth·book]

Lemma 35. *Let $(U(n), \|\cdot\|, \mu)$ be a metric measure space where $\|\cdot\|$ is the Hilbert-Schmidt norm and μ is the measure function.*

The Haar measure on $U(n)$ is the unique probability measure that is invariant under the action of $U(n)$ on itself.

That is, fixing $B \in U(n)$, $\forall A \in U(n)$, $\mu(A \cdot B) = \mu(B \cdot A) = \mu(B)$.

The Haar measure is the unique probability measure that is invariant under the action of $U(n)$ on itself.

A finite-dimensional quantum system is modeled by a complex Hilbert space (a complete inner product space)

$$\mathcal{H} \cong \mathbb{C}^{n+1}.$$

A **pure state** is represented by a unit vector

$$\psi \in \mathcal{H}, \quad \|\psi\| = 1.$$

A **mixed state** is represented by a density matrix

$$\rho = \sum_{j=1}^n p_j |\psi_j\rangle\langle\psi_j|, \quad \sum_{j=1}^n p_j = 1, \quad p_j \geq 0.$$

Some key comparisons between pure states and mixed states:

Pure states describe maximal information; mixed states describe probabilistic mixtures or partial information.

Pure states form a curved geometric space; mixed states form a convex set inside the space of matrices.

Pure states live in the complex projective space.

- Two nonzero vectors that differ by a nonzero complex scalar represent the same physical state:

$$\psi \sim \lambda\psi, \quad \lambda \in \mathbb{C}^\times.$$

- In particular, multiplying by a phase $e^{i\theta}$ does not change any physical predictions.
- Therefore the physical pure state is not a single vector, but the *complex line* spanned by that vector.

Hence the space of pure states (denoted by $\mathcal{P}(\mathcal{H})$) is

$$\mathcal{P}(\mathcal{H}) = (\mathcal{H} \setminus \{0\})/\mathbb{C}^\times.$$

After choosing a basis $\mathcal{H} \cong \mathbb{C}^{n+1}$, this becomes

$$\mathcal{P}(\mathcal{H}) \cong \mathbb{C}P^n.$$

Proposition 36. *Proposition of indistinguishability:*

Suppose that we have two systems $u_1, u_2 \in \mathcal{H}_1$, the two states are distinguishable if and only if they are orthogonal.

Proof. Ways to distinguish the two states:

1. Set $X = \{0, 1, 2\}$ and $M_i = |u_i\rangle\langle u_i|$, $M_0 = I - M_1 - M_2$
2. Then $\{M_0, M_1, M_2\}$ is a complete collection of measurement operators on \mathcal{H} .
3. Suppose the prepared state is u_1 , then $p(1) = \|M_1 u_1\|^2 = \|u_1\|^2 = 1$, $p(2) = \|M_2 u_1\|^2 = 0$, $p(0) = \|M_0 u_1\|^2 = 0$.

If they are not orthogonal, then there is no choice of measurement operators to perfectly distinguish the two states.

□

Intuitively, if the two states are not orthogonal, then for any measurement (projection) there exists non-zero probability of getting the same outcome for both states.

0.4.1 Random quantum states

First, we need to define what is a random state in a bipartite system.

Definition 37. *Pure state:*

A random pure state φ is any random variable distributed according to the unitarily invariant probability measure on the pure states $\mathcal{P}(A)$ of the system A , denoted by $\varphi \in_R \mathcal{P}(A)$.

It is trivial that for the space of pure state, we can easily apply the Haar measure as the unitarily invariant probability measure since the space of pure state is S^n for some n . However, for the case of mixed states, that is a bit complicated and we need to use partial tracing to defined the rank- s random states.

Definition 38. *Rank- s random state.*

For a system A and an integer $s \geq 1$, consider the distribution onn the mixed states $\mathcal{S}(A)$ of A induced by the partial trace over the second factor form the uniform distribution on pure states of $A \otimes \mathbb{C}^s$. Any random variable ρ distributed as such will be called a rank- s random states; denoted as $\rho \in_R \mathcal{S}_s(A)$. And $\mathcal{P}(A) = \mathcal{S}_1(A)$.