

Quantum Computing

Lecture $|05\rangle$: Mathematical Structures

Paolo Zuliani

Dipartimento di Informatica
Università di Roma “La Sapienza”, Rome, Italy



SAPIENZA
UNIVERSITÀ DI ROMA

Agenda

- Groups
- Vector spaces
- Scalar products
- Dirac's notation
- Hilbert spaces
- Adjoint operators and projectors
- Spectral theorem
- The rules of Quantum Mechanics

Groups

The ‘bedrock’ of Quantum Mechanics are particular vector spaces (Hilbert spaces) that are built on top of groups.

Definition

A group is a non-empty set G with a “multiplication” operation that satisfies:

- 1 *associativity*: $a(bc) = (ab)c$;
- 2 there exists a *unit* element $1 \in G$ such that $\forall a \in G, a1 = 1a = a$;
- 3 $\forall a \in G$ there exists an *inverse* a^{-1} such that $aa^{-1} = a^{-1}a = 1$.

Groups

The ‘bedrock’ of Quantum Mechanics are particular vector spaces (Hilbert spaces) that are built on top of groups.

Definition

A group is a non-empty set G with a “multiplication” operation that satisfies:

- ① *associativity*: $a(bc) = (ab)c$;
- ② there exists a *unit* element $1 \in G$ such that $\forall a \in G, a1 = 1a = a$;
- ③ $\forall a \in G$ there exists an *inverse* a^{-1} such that $aa^{-1} = a^{-1}a = 1$.

In an *abelian* group multiplication is *commutative*, i.e., $\forall a, b \in G, ab = ba$.

Example: the set of reals \mathbb{R} with the usual multiplication is an abelian group.

Groups

The ‘bedrock’ of Quantum Mechanics are particular vector spaces (Hilbert spaces) that are built on top of groups.

Definition

A group is a non-empty set G with a “multiplication” operation that satisfies:

- ① *associativity*: $a(bc) = (ab)c$;
- ② there exists a *unit* element $1 \in G$ such that $\forall a \in G, a1 = 1a = a$;
- ③ $\forall a \in G$ there exists an *inverse* a^{-1} such that $aa^{-1} = a^{-1}a = 1$.

In an *abelian* group multiplication is *commutative*, i.e., $\forall a, b \in G, ab = ba$.

Example: the set of reals \mathbb{R} with the usual multiplication is an abelian group.

Example: the set of complex invertible square matrices with the row by column product is a group, although not abelian.

Complex Vector Spaces

Definition

A complex vector space is a set V with a vector “sum” denoted $u + v$ and a scalar “multiplication” denoted λv for $\lambda \in \mathbb{C}$ that make V an abelian group:

- ① *associativity*: $u + (v + w) = (u + v) + w$;
- ② *null vector* 0 (unit element for the group): $0 + v = v + 0$;
- ③ every element v has an *inverse element* $-v$, i.e., $v + (-v) = 0$;
- ④ $+$ is commutative.

Complex Vector Spaces

Definition

A complex vector space is a set V with a vector “sum” denoted $u + v$ and a scalar “multiplication” denoted λv for $\lambda \in \mathbb{C}$ that make V an abelian group:

- ① *associativity*: $u + (v + w) = (u + v) + w$;
- ② *null vector* 0 (unit element for the group): $0 + v = v + 0$;
- ③ every element v has an *inverse element* $-v$, i.e., $v + (-v) = 0$;
- ④ $+$ is commutative.

Scalar multiplication satisfies:

- ① $\alpha(u + v) = \alpha u + \alpha v$;
- ② $(\alpha + \beta)v = \alpha v + \beta v$;
- ③ $\alpha(\beta v) = (\alpha\beta)v$;
- ④ $1v = v$;
- ⑤ $0v = 0$. (Notation abuse: 0 is a scalar on the LHS and a vector on the RHS.)

Complex Vector Spaces

Examples:

- the usual \mathbb{R}^3 space of classical (Newtonian) physics;
- the space $\mathbb{C}^n = \underbrace{\mathbb{C} \times \mathbb{C} \times \dots \times \mathbb{C}}_{n \text{ times}}$ of n -dimensional complex vectors with the “obvious” vector sum and scalar multiplication;
- the set of $n \times n$ complex matrices with the usual matrix sum and scalar multiplication of linear maps.

Linear Maps

Definition

A linear map between vector spaces V and W is a function $L : V \rightarrow W$ that satisfies:

$$L(\alpha u + \beta v) = \alpha L(u) + \beta L(v)$$

Linear Maps

Definition

A linear map between vector spaces V and W is a function $L : V \rightarrow W$ that satisfies:

$$L(\alpha u + \beta v) = \alpha L(u) + \beta L(v)$$

Note: the set of all linear maps $L : V \rightarrow W$ is itself a vector space with the “obvious” sum and scalar multiplication.

Linear Maps

Definition

A linear map between vector spaces V and W is a function $L : V \rightarrow W$ that satisfies:

$$L(\alpha u + \beta v) = \alpha L(u) + \beta L(v)$$

Note: the set of all linear maps $L : V \rightarrow W$ is itself a vector space with the “obvious” sum and scalar multiplication.

Definition

The dual of a complex vector space V (denoted V^*) is the set of all linear maps $L : V \rightarrow \mathbb{C}$.

Definition

Given a vector space V , a set $W \subset V$ is a linear subspace of V if sum and scalar multiplication are closed in W .

Definition

- Vectors $v_1, \dots, v_n \in V$ are linearly dependent if there are numbers $\alpha_1, \dots, \alpha_n$ (not all zero) such that

$$\sum_{i=1}^n \alpha_i v_i = 0$$

[otherwise they are said linearly independent];

Definition

- Vectors $v_1, \dots, v_n \in V$ are linearly dependent if there are numbers $\alpha_1, \dots, \alpha_n$ (not all zero) such that

$$\sum_{i=1}^n \alpha_i v_i = 0$$

[otherwise they are said linearly independent];

- A vector space is n -dimensional if it has a set of n linearly independent vectors, but no subset of $n + 1$ such vectors;

Definition

- Vectors $v_1, \dots, v_n \in V$ are linearly dependent if there are numbers $\alpha_1, \dots, \alpha_n$ (not all zero) such that

$$\sum_{i=1}^n \alpha_i v_i = 0$$

[otherwise they are said linearly independent];

- A vector space is n -dimensional if it has a set of n linearly independent vectors, but no subset of $n + 1$ such vectors;
- A set of n linearly independent vectors in a n -dimensional vector space V is called a basis set for V ;

Definition

- Vectors $v_1, \dots, v_n \in V$ are linearly dependent if there are numbers $\alpha_1, \dots, \alpha_n$ (not all zero) such that

$$\sum_{i=1}^n \alpha_i v_i = 0$$

[otherwise they are said linearly independent];

- A vector space is n -dimensional if it has a set of n linearly independent vectors, but no subset of $n + 1$ such vectors;
- A set of n linearly independent vectors in a n -dimensional vector space V is called a basis set for V ;
- Given $S \subset V$, the linear span $[S]$ of S is the set of all *finite* linear combinations of vectors of S .

Proposition

Given a vector space V and a basis set $S = \{e_1, \dots, e_n\}$ such that $[S] = V$, then any $v \in V$ can be written as:

$$v = \sum_{i=1}^n \alpha_i e_i$$

where the coefficients α_i 's are complex.

Proof: *[Exercise. Hint: start by noticing that the vectors $\{e_1, \dots, e_n, v\}$ are linearly dependent.]*

Proposition

Given a vector space V and a basis set $S = \{e_1, \dots, e_n\}$ such that $[S] = V$, then any $v \in V$ can be written as:

$$v = \sum_{i=1}^n \alpha_i e_i$$

where the coefficients α_i 's are complex.

Proof: *[Exercise. Hint: start by noticing that the vectors $\{e_1, \dots, e_n, v\}$ are linearly dependent.]*

Proposition

The coefficients α_i 's are unique (wrt to a basis set).

Proof: *[Exercise]*

Scalar (Inner) Products

Definition

A scalar product over a vector space V is a function that maps $v, w \in V$ to a complex $\langle v, w \rangle$ such that

$$\textcircled{1} \quad \langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle$$

Scalar (Inner) Products

Definition

A scalar product over a vector space V is a function that maps $v, w \in V$ to a complex $\langle v, w \rangle$ such that

- ① $\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle$
- ② $\langle u, v \rangle^* = \langle v, u \rangle$

Scalar (Inner) Products

Definition

A scalar product over a vector space V is a function that maps $v, w \in V$ to a complex $\langle v, w \rangle$ such that

- ❶ $\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle$
- ❷ $\langle u, v \rangle^* = \langle v, u \rangle$
- ❸ $\langle u, u \rangle \geq 0$ and $\langle u, u \rangle = 0$ iff $u = 0$.

Scalar (Inner) Products

Definition

A scalar product over a vector space V is a function that maps $v, w \in V$ to a complex $\langle v, w \rangle$ such that

- ① $\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle$
- ② $\langle u, v \rangle^* = \langle v, u \rangle$
- ③ $\langle u, u \rangle \geq 0$ and $\langle u, u \rangle = 0$ iff $u = 0$.

Proposition

$$\langle \alpha u + \beta v, w \rangle = \alpha^* \langle u, w \rangle + \beta^* \langle v, w \rangle$$

Proof: *[Exercise]*

Scalar (Inner) Products

Definition

Given two vectors $u = (u_1 \dots u_n) \in \mathbb{C}^n$ and $v = (v_1 \dots v_n) \in \mathbb{C}^n$ we define the scalar product:

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

Scalar (Inner) Products

Definition

Given two vectors $u = (u_1 \dots u_n) \in \mathbb{C}^n$ and $v = (v_1 \dots v_n) \in \mathbb{C}^n$ we define the scalar product:

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

Note: $\langle u, v \rangle$ can be written as the product of an $1 \times n$ matrix (row vector) and a $n \times 1$ matrix (column vector)

$$\langle u, v \rangle = (u_1^* \dots u_n^*) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

The Dirac Notation

After Paul Dirac (1902-1984; Nobel Prize in Physics).

The Dirac Notation

After Paul Dirac (1902-1984; Nobel Prize in Physics).

$\langle u, v \rangle = \langle u | v \rangle$ is the “braket” made by the “bra” $\langle u |$ and the “ket” $|v\rangle$.

The ket $|v\rangle$ is just a regular vector $v \in V$.

The Dirac Notation

After Paul Dirac (1902-1984; Nobel Prize in Physics).

$\langle u, v \rangle = \langle u|v \rangle$ is the “braket” made by the “bra” $\langle u|$ and the “ket” $|v\rangle$.

The ket $|v\rangle$ is just a regular vector $v \in V$.

The bra $\langle u|$ is a *map* from V to $\mathbb{C}!!$ (The bra is actually an element of V^* .)

$$\langle u|v \rangle = (u_1^* \dots u_n^*) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Thus $\langle u| = (u_1^* \dots u_n^*)$ and $|v\rangle = (v_1 \dots v_n)^T$.

Schwarz's Inequality

Theorem (Schwarz's Inequality)

For any two vectors u, v of a complex vector space it holds that:

$$|\langle u|v\rangle| \leq \sqrt{\langle u|u\rangle \langle v|v\rangle}$$

where equality holds iff u, v are linearly dependent.

Schwarz's Inequality

Theorem (Schwarz's Inequality)

For any two vectors u, v of a complex vector space it holds that:

$$|\langle u|v \rangle| \leq \sqrt{\langle u|u \rangle \langle v|v \rangle}$$

where equality holds iff u, v are linearly dependent.

Definition

The norm of vector u is $\|u\| = \sqrt{\langle u|u \rangle}$.

Theorem (Triangular Inequality)

For any two vectors u, v of a complex vector space it holds that:

$$\|u + v\| \leq \|u\| + \|v\|$$

Orthogonal Vectors

Definition

Two vectors u, v of a complex vector space are orthogonal if $\langle u|v \rangle = 0$.

Orthogonal Vectors

Definition

Two vectors u, v of a complex vector space are orthogonal if $\langle u|v \rangle = 0$.

Definition

The vectors set $\{u_1, \dots, u_m\}$ is orthonormal if $\langle u_i|u_j \rangle = \delta_{ij}$ for all $i, j \in \{1, \dots, m\}$.

The Kronecker delta is defined as $\delta_{ij} = 1$ if $i = j$ and 0 otherwise.

Orthonormal Bases

Let $\{e_1, \dots, e_n\}$ be an orthonormal basis for an n -dimensional vector space V . We know that for any $u \in V$ we can write

$$u = \sum_{i=1}^n \alpha_i e_i.$$

How to compute the α_i 's?

Orthonormal Bases

Let $\{e_1, \dots, e_n\}$ be an orthonormal basis for an n -dimensional vector space V . We know that for any $u \in V$ we can write

$$u = \sum_{i=1}^n \alpha_i e_i.$$

How to compute the α_i 's?

$$\langle e_j | u \rangle =$$

Orthonormal Bases

Let $\{e_1, \dots, e_n\}$ be an orthonormal basis for an n -dimensional vector space V . We know that for any $u \in V$ we can write

$$u = \sum_{i=1}^n \alpha_i e_i.$$

How to compute the α_i 's?

$$\langle e_j | u \rangle = \langle e_j | \sum_{i=1}^n \alpha_i e_i \rangle$$

Orthonormal Bases

Let $\{e_1, \dots, e_n\}$ be an orthonormal basis for an n -dimensional vector space V . We know that for any $u \in V$ we can write

$$u = \sum_{i=1}^n \alpha_i e_i.$$

How to compute the α_i 's?

$$\langle e_j | u \rangle = \langle e_j | \sum_{i=1}^n \alpha_i e_i \rangle = \sum_{i=1}^n \alpha_i \langle e_j | e_i \rangle =$$

Orthonormal Bases

Let $\{e_1, \dots, e_n\}$ be an orthonormal basis for an n -dimensional vector space V . We know that for any $u \in V$ we can write

$$u = \sum_{i=1}^n \alpha_i e_i.$$

How to compute the α_i 's?

$$\langle e_j | u \rangle = \langle e_j | \sum_{i=1}^n \alpha_i e_i \rangle = \sum_{i=1}^n \alpha_i \langle e_j | e_i \rangle = \sum_{i=1}^n \alpha_i \delta_{ji} = \alpha_j.$$

Orthonormal Bases

Let $\{e_1, \dots, e_n\}$ be an orthonormal basis for an n -dimensional vector space V . We know that for any $u \in V$ we can write

$$u = \sum_{i=1}^n \alpha_i e_i.$$

How to compute the α_i 's?

$$\langle e_j | u \rangle = \langle e_j | \sum_{i=1}^n \alpha_i e_i \rangle = \sum_{i=1}^n \alpha_i \langle e_j | e_i \rangle = \sum_{i=1}^n \alpha_i \delta_{ji} = \alpha_j.$$

In Dirac notation:

$$|u\rangle = \sum_{i=1}^n |e_i\rangle \langle e_i | u \rangle \quad \Rightarrow \quad \langle v | u \rangle = \sum_{i=1}^n \langle v | e_i \rangle \langle e_i | u \rangle$$

Hilbert Spaces (almost)

After David Hilbert (mathematician; 1862-1943).

Definition

A vector sequence $v_m \in V$ converges strongly to $v \in V$ (denoted $v_m \rightarrow v$) if $\lim_{m \rightarrow \infty} \|v - v_m\| = 0$

Hilbert Spaces (almost)

After David Hilbert (mathematician; 1862-1943).

Definition

A vector sequence $v_m \in V$ converges strongly to $v \in V$ (denoted $v_m \rightarrow v$) if $\lim_{m \rightarrow \infty} \|v - v_m\| = 0$

Proposition

If $(v_m \rightarrow v)$ then:

- 1 If $(v_m \rightarrow v)$ then $\lim_{m \rightarrow \infty} \|v_m\| = \|v\|$ (this is weak convergence; the converse holds in finite-dimensional spaces.)
- 2 $\langle u | v \rangle = \lim_{m \rightarrow \infty} \langle u | v_m \rangle$ (scalar products are continuous)

Hilbert Spaces (almost)

Definition

A vector sequence $v_i \in V$ is a Cauchy sequence if for any $\epsilon > 0$ there exists n_ϵ such that $\forall n, m > n_\epsilon \quad \|v_n - v_m\| < \epsilon$.

Hilbert Spaces (almost)

Definition

A vector sequence $v_i \in V$ is a Cauchy sequence if for any $\epsilon > 0$ there exists n_ϵ such that $\forall n, m > n_\epsilon \ \|v_n - v_m\| < \epsilon$.

Definition

A Hilbert space is a *complete* scalar product space, *i.e.*, every Cauchy sequence converges strongly to an element in the space.

Hilbert Spaces (almost)

Definition

A vector sequence $v_i \in V$ is a Cauchy sequence if for any $\epsilon > 0$ there exists n_ϵ such that $\forall n, m > n_\epsilon \ \|v_n - v_m\| < \epsilon$.

Definition

A Hilbert space is a *complete* scalar product space, *i.e.*, every Cauchy sequence converges strongly to an element in the space.

Proposition

Finite-dimensional vector spaces are always complete.

Quantum mechanics is developed over Hilbert spaces with *countable* bases. However, for quantum computing we need finite-dimensional Hilbert spaces only.

Linear Operators

Definition

Let \mathcal{H} be a Hilbert space.

- A linear operator A is a linear function $A : \mathcal{H} \rightarrow \mathcal{H}$;
- Operator sum: $\forall v \in \mathcal{H} \quad (A + B)v = Av + Bv$;
- Operator product: $\forall v \in \mathcal{H} \quad (AB)v = A(Bv)$.

Linear Operators

Definition

Let \mathcal{H} be a Hilbert space.

- A linear operator A is a linear function $A : \mathcal{H} \rightarrow \mathcal{H}$;
- Operator sum: $\forall v \in \mathcal{H} \quad (A + B)v = Av + Bv$;
- Operator product: $\forall v \in \mathcal{H} \quad (AB)v = A(Bv)$.

Definition

The adjoint of an operator A is the operator A^\dagger defined by:

$$\forall u, v \in \mathcal{H} \quad \langle u | A^\dagger v \rangle = \langle Au | v \rangle$$

Definition

An operator A is self-adjoint (or Hermitian) if $A = A^\dagger$.

If A is self-adjoint then $\langle u | Av \rangle = \langle Au | v \rangle = \langle v | Au \rangle^*$.

Linear Operators

Definition

A unitary operator U is a linear operator that satisfies $UU^\dagger = U^\dagger U = I$, where I is the identity operator.

Linear Operators

Definition

A unitary operator U is a linear operator that satisfies $UU^\dagger = U^\dagger U = I$, where I is the identity operator.

An *equivalent* definition is:

Definition

A unitary operator U is a linear operator that satisfies

- ① U is surjective; and
- ② $\forall x, y \in \mathcal{H} \quad \langle Ux | Uy \rangle = \langle x | y \rangle$ (or equivalently, $\forall x \in \mathcal{H} \quad \|Ux\| = \|x\|$)

Linear Operators

Definition

A unitary operator U is a linear operator that satisfies $UU^\dagger = U^\dagger U = I$, where I is the identity operator.

An *equivalent* definition is:

Definition

A unitary operator U is a linear operator that satisfies

- 1 U is surjective; and
- 2 $\forall x, y \in \mathcal{H} \quad \langle Ux | Uy \rangle = \langle x | y \rangle$ (or equivalently, $\forall x \in \mathcal{H} \quad \|Ux\| = \|x\|$)

Note: The linearity assumption in either definition is not needed: if U satisfies $UU^\dagger = U^\dagger U = I$ then U must be linear [Exercise].

Eigenvectors and eigenvalues for operators are defined as usual.

Definition

An eigenvalue λ of an operator A is d -fold degenerate if there are d linearly independent eigenvectors u_1, \dots, u_d associated to λ .

Note that for any $\alpha_i \in \mathbb{C}$ we have $A(\sum_{i=1}^d \alpha_i u_i) = \lambda(\sum_{i=1}^d \alpha_i u_i)$.

Linear Operators

Eigenvectors and eigenvalues for operators are defined as usual.

Definition

An eigenvalue λ of an operator A is d -fold degenerate if there are d linearly independent eigenvectors u_1, \dots, u_d associated to λ .

Note that for any $\alpha_i \in \mathbb{C}$ we have $A(\sum_{i=1}^d \alpha_i u_i) = \lambda(\sum_{i=1}^d \alpha_i u_i)$.

Definition

The eigenvectors of a given eigenvalue form a linear subspace (the eigenspace).

Linear Operators: Dirac Notation

$$\langle u|Av\rangle = \langle u|A|v\rangle = \begin{cases} (\langle u|A)|v\rangle \\ \langle u|(A|v\rangle) \end{cases}$$

We can think that A right-multiplies the bra $\langle u|$ or left-multiplies the ket $|v\rangle$.

$$\langle u|Av\rangle = \langle u|A|v\rangle = \begin{cases} (\langle u|A)|v\rangle \\ \langle u|(A|v\rangle) \end{cases}$$

We can think that A right-multiplies the bra $\langle u|$ or left-multiplies the ket $|v\rangle$.

If λ is a non-degenerate eigenvalue of A we write $A|\lambda\rangle = \lambda|\lambda\rangle$.

We have that $\langle\lambda|A^\dagger = \lambda^*\langle\lambda|$. [Exercise]

Proposition

Any linear operator A on a scalar product vector space with an orthonormal basis e_i 's can be represented in matrix form by:

$$A_{ij} = \langle e_i | A e_j \rangle \quad A_{ij}^\dagger = A_{ji}^*$$

Linear Operators as Matrices

Proposition

Any linear operator A on a scalar product vector space with an orthonormal basis e_i 's can be represented in matrix form by:

$$A_{ij} = \langle e_i | A e_j \rangle \quad A_{ij}^\dagger = A_{ji}^*$$

Note that $\langle u | v \rangle w = \langle u | v \rangle |w\rangle = (|w\rangle \langle u|) |v\rangle$.

Linear Operators as Matrices

Proposition

Any linear operator A on a scalar product vector space with an orthonormal basis e_i 's can be represented in matrix form by:

$$A_{ij} = \langle e_i | A e_j \rangle \quad A_{ij}^\dagger = A_{ji}^*$$

Note that $\langle u | v \rangle w = \langle u | v \rangle |w\rangle = (|w\rangle \langle u|) |v\rangle$.

Now, considering an orthonormal basis e_i we have $|v\rangle = \sum_i |e_i\rangle \langle e_i | v \rangle$, and hence

$$I = \sum_i |e_i\rangle \langle e_i| \quad (\text{resolution of identity})$$

Proposition

For operators A, B and complex λ , we have:

$$(AB)^\dagger = B^\dagger A^\dagger$$

$$(\lambda A)^\dagger = \lambda^* A^\dagger$$

$$(A^\dagger)^\dagger = A$$

Definition

A linear subspace W of a Hilbert space \mathcal{H} is topologically closed if any sequence of vectors in W converges in W .

Projectors

Definition

A linear subspace W of a Hilbert space \mathcal{H} is topologically closed if any sequence of vectors in W converges in W .

Definition

Two linear subspaces $V, W \subset \mathcal{H}$ are orthogonal if every vector of V is orthogonal to every vector of W .

The orthogonal complement of V is $V^\perp = \{u \in \mathcal{H} \text{ s.t. } \forall v \in V, \langle u|v \rangle = 0\}$

Proposition

If \mathcal{H} is finite-dimensional, then $(V^\perp)^\perp = V$.

Projectors

Given a closed subspace $W \subset \mathcal{H}$, we would like to write any $v \in \mathcal{H}$ as $v_W + v_{W^\perp}$, where $v_W \in W$ and $v_{W^\perp} \in W^\perp$.

Definition

Let f_i be an orthonormal basis for W . Define:

$$v_W = \sum_i \langle f_i | v \rangle f_i \quad v_{W^\perp} = v - v_W$$

Projectors

Given a closed subspace $W \subset \mathcal{H}$, we would like to write any $v \in \mathcal{H}$ as $v_W + v_{W^\perp}$, where $v_W \in W$ and $v_{W^\perp} \in W^\perp$.

Definition

Let f_i be an orthonormal basis for W . Define:

$$v_W = \sum_i \langle f_i | v \rangle f_i \quad v_{W^\perp} = v - v_W$$

Exercise: show that v_W does not depend on the choice of basis f_i .

Projectors

Given a closed subspace $W \subset \mathcal{H}$, we would like to write any $v \in \mathcal{H}$ as $v_W + v_{W^\perp}$, where $v_W \in W$ and $v_{W^\perp} \in W^\perp$.

Definition

Let f_i be an orthonormal basis for W . Define:

$$v_W = \sum_i \langle f_i | v \rangle f_i \quad v_{W^\perp} = v - v_W$$

Exercise: show that v_W does not depend on the choice of basis f_i .

Definition

The map $P_W : \mathcal{H} \rightarrow W$ defined as $P_W v = v_W$ is the projection operator on W .

The projector on the orthogonal complement of W is $P_{W^\perp} = I - P_W$.

Proposition

$$v \in W \quad \text{iff} \quad P_W v = v$$

$$v \in W^\perp \quad \text{iff} \quad P_W v = 0$$

Thus P_W has only two eigenvalues: 0 and 1 (in general degenerate).

In addition, we have that $P_W^2 = P_W$ and $P_W^\dagger = P_W$. (We could use these two conditions to define a projector.)

Definition

Two projectors P, Q are orthogonal if $PQ = QP = 0$ (the two subspaces are \perp).

If $P \perp Q$ then $P + Q$ is also a projector. (Exercise)

Given a family P_i of projectors such that $P_i P_j = \delta_{ij}$, then

$$I = \sum_i P_i \quad (\text{resolution of identity})$$

Theorem

- ① *The eigenvalues of a self-adjoint operator are real numbers.*
- ② *The eigenvalues of a unitary operator are complex numbers of modulus 1.*
- ③ *Eigenvectors (of self-adjoint and unitary operators) associated to different eigenvalues are orthogonal.*

Theorem

- ① *The eigenvalues of a self-adjoint operator are real numbers.*
- ② *The eigenvalues of a unitary operator are complex numbers of modulus 1.*
- ③ *Eigenvectors (of self-adjoint and unitary operators) associated to different eigenvalues are orthogonal.*

What's special about self-adjoint operators and unitary operators?

Theorem

- 1 The eigenvalues of a self-adjoint operator are real numbers.
- 2 The eigenvalues of a unitary operator are complex numbers of modulus 1.
- 3 Eigenvectors (of self-adjoint and unitary operators) associated to different eigenvalues are orthogonal.

What's special about self-adjoint operators and unitary operators?

Definition

An operator A is normal if it satisfies $A^\dagger A = AA^\dagger$.

Clearly, both self-adjoint and unitary operators are normal.

Theorem (Spectral Theorem for finite-dimensional Hilbert Spaces)

The set of all eigenvectors u_{ij} of a normal operator is an orthonormal basis for \mathcal{H} , i.e., for any $v \in \mathcal{H}$:

$$v = \sum_{i=1}^m \sum_{j=1}^{d_i} \alpha_{ij} u_{ij}$$

where $\alpha_{ij} = \langle u_{ij} | v \rangle$.

Note that $\dim \mathcal{H} = \sum_{i=1}^m d_i$.

Spectral Theory: Dirac Notation

$$v = \sum_{i=1}^m \sum_{j=1}^{d_i} \alpha_{ij} u_{ij} \quad \text{where} \quad \alpha_{ij} = \langle u_{ij} | v \rangle$$

In Dirac notation:

$$|v\rangle = \sum_{i=1}^m \sum_{j=1}^{d_i} \langle \lambda_{ij} | v \rangle |\lambda_{ij}\rangle$$

Spectral Theory: Dirac Notation

$$v = \sum_{i=1}^m \sum_{j=1}^{d_i} \alpha_{ij} u_{ij} \quad \text{where} \quad \alpha_{ij} = \langle u_{ij} | v \rangle$$

In Dirac notation:

$$|v\rangle = \sum_{i=1}^m \sum_{j=1}^{d_i} \langle \lambda_{ij} | v \rangle |\lambda_{ij}\rangle$$

Exercise: prove that $A = \sum_{i=1}^m \lambda_i P_i$, where P_i is the projector of the eigenspace of λ_i .

The Rules of Quantum Mechanics

Rule 1: The state space of Quantum Mechanics is a Hilbert space \mathcal{H} (the “physical” state of a system is a complex vector).

The Rules of Quantum Mechanics

Rule 1: The state space of Quantum Mechanics is a Hilbert space \mathcal{H} (the “physical” state of a system is a complex vector).

Rule 2: Observables are represented mathematically by self-adjoint operators on \mathcal{H} .

The Rules of Quantum Mechanics

Rule 1: The state space of Quantum Mechanics is a Hilbert space \mathcal{H} (the “physical” state of a system is a complex vector).

Rule 2: Observables are represented mathematically by self-adjoint operators on \mathcal{H} .

Rule 3: Given an observable A and a state $v \in \mathcal{H}$, then the *expected result* of measuring A is

$$\langle v | Av \rangle$$

(results are probabilistic).

The Rules of Quantum Mechanics

Rule 1: The state space of Quantum Mechanics is a Hilbert space \mathcal{H} (the “physical” state of a system is a complex vector).

Rule 2: Observables are represented mathematically by self-adjoint operators on \mathcal{H} .

Rule 3: Given an observable A and a state $v \in \mathcal{H}$, then the *expected result* of measuring A is

$$\langle v | Av \rangle$$

(results are probabilistic).

Rule 4: A closed system evolves through time according to the Schrödinger equation:

$$i\hbar \frac{dv(t)}{dt} = Hv(t)$$

where H is the system *Hamiltonian* (a self-adjoint operator describing the total energy of the system).

Rule 3 is equivalent to:

Rule 3': Given an observable A and a state $\nu \in \mathcal{H}$:

- ① The only possible results of measuring A are one of its eigenvalues
- ② The probability of measuring eigenvalue λ in state ν is:

$$\text{Prob}(A = \lambda; \nu) = \langle \nu | P_\lambda \nu \rangle$$

Tensor Products

Definition

The tensor product of two n -dimensional vectors u, v is the n^2 -dimensional vector $w = u \otimes v$ defined by:

$$w_i = u_j \otimes v_i \text{ mod } n$$

Definition

The scalar product of tensor vectors is defined by:

$$\langle u \otimes v | w \otimes z \rangle = \langle u | w \rangle \langle v | z \rangle$$

Definition

The tensor product of operators (or matrices) A, B is defined by:

$$(A \otimes B)u \otimes v = Au \otimes Bv$$

Proposition

For suitably sized matrices (or operators) L, M, N , and P , we have that:

$$(M \cdot N) \otimes (L \cdot P) = (M \otimes L) \cdot (N \otimes P)$$