ITIS 6260/8260 Quantum Computing

Lecture 0: Introduction to Hilbert space

Yongge Wang

UNC Charlotte, USA

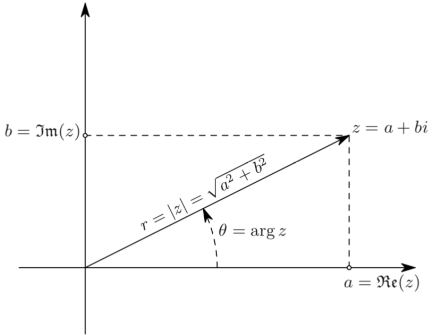
January 5, 2019

Outline

Outline

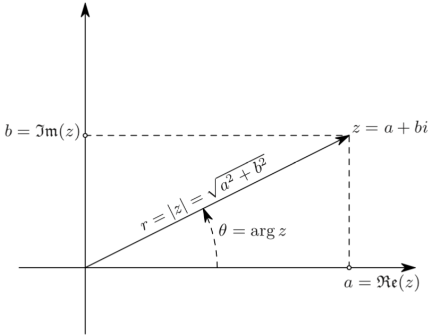
Complex numbers

- What is the solution for $x^2 + 1 = 0$?
- Assume a number i with $i^2 = -1$.
- A complex number is $a + bi$ where a and b are real numbers.



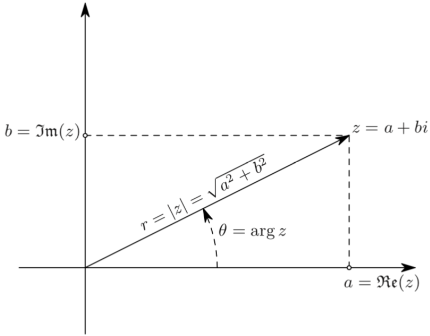
Complex numbers

- What is the solution for $x^2+1=0$?
- Assume a number i with $i^2=-1$.
- A complex number is $a+bi$ where a and b are real numbers.



Complex numbers

- What is the solution for $x^2 + 1 = 0$?
- Assume a number i with $i^2 = -1$.
- A complex number is $a + bi$ where a and b are real numbers.



Argument and Absolute Value

- For a complex number $z = a + bi$, the absolute value or modulus is

$$|z| = \sqrt{a^2 + b^2}$$

where |z| is the distance from (0,0) to the point z in the complex plane

- The angle θ is called the argument of the complex number z. Written as arg $z = \theta$.
- From trigonometry, a complex number $z = a + bi$ has the property

$$a = |z| \cos\theta \text{ and } b = |z| \sin\theta$$

That is,

$$z = |z|(\cos\theta + i\sin\theta)$$

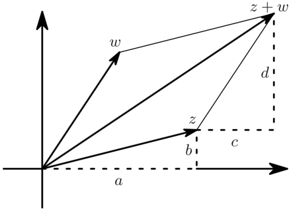
Argument and Absolute Value

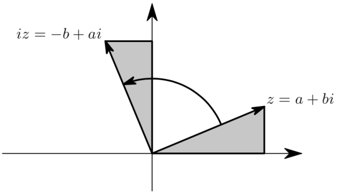
- For a complex number $z = a + bi$, the absolute value or modulus is
  $$|z| = \sqrt{a^2 + b^2}$$
  where |z| is the distance from (0,0) to the point z in the complex plane
- The angle θ is called the argument of the complex number z. Written as arg $z = \theta$.
- From trigonometry, a complex number $z = a + bi$ has the property
  $$a = |z| \cos \theta \text{ and } b = |z| \sin \theta$$
  That is,
  $$z = |z|(\cos \theta + i \sin \theta)$$

Argument and Absolute Value

- For a complex number $z = a + bi$, the absolute value or modulus is
$$|z| = \sqrt{a^2 + b^2}$$
where |z| is the distance from (0,0) to the point z in the complex plane
- The angle θ is called the argument of the complex number z. Written as $\arg z = \theta$.
- From trigonometry, a complex number $z = a + bi$ has the property
$$a = |z| \cos\theta \text{ and } b = |z| \sin\theta$$
That is,
$$z = |z|(\cos\theta + i \sin\theta)$$

Geometry of Arithmetic



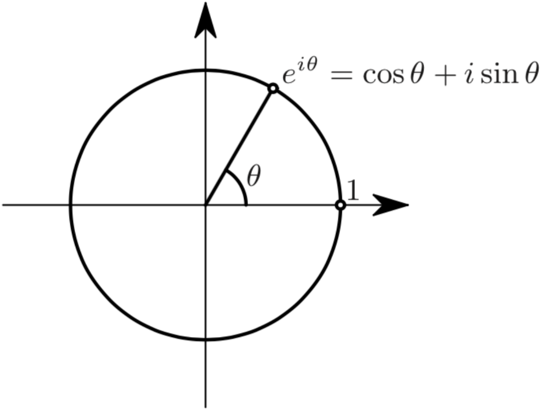


Additionof $z = a + bi$ and $w = c + di$ and Multiplication of $a + bi$ by i.

The Complex Exponential Function: e^{a+bi}

Consider Euler's definition of $e^{i\theta} = \cos\theta + i\sin\theta$. It is easy to verify Euler's famous formula

$$e^{\pi i} + 1 = 0$$



The Complex Exponential Function: why $e^{i\theta} = \cos\theta + i\sin\theta$?

- Reason 1: We haven't defined $e^{i\theta}$ before and we can do anything we like.
- Reason 2 (not a proof): Substitute $i\theta$ in Taylor series for e^x:

$$
\begin{aligned}
e^{i\theta} &= 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \cdots \\
&= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + \cdots \\
&= 1 - \theta^2/2! + \theta^4/4! - \cdots + i(\theta - \theta^3/3! + \theta^5/5! - \cdots) \\
&= \cos\theta + i\sin\theta
\end{aligned}
$$

The Complex Exponential Function: why $e^{i\theta} = \cos\theta + i\sin\theta$?

- Reason 1: We haven't defined $e^{i\theta}$ before and we can do anything we like.
- Reason 2 (not a proof): Substitute $i\theta$ in Taylor series for e^x:

$$\begin{aligned} e^{i\theta} &= 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \cdots \\ &= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + \cdots \\ &= 1 - \theta^2/2! + \theta^4/4! - \cdots + i(\theta - \theta^3/3! + \theta^5/5! - \cdots) \\ &= \cos\theta + i\sin\theta \end{aligned}$$

Definition

- A Hilbert space H is a complex inner product space that is also a complete metric space with respect to the distance function induced by the inner product.

Vector space

- closure under addition: $\mathbf{v} + \mathbf{w}$ is a vector
- has a zero: $\mathbf{v} + \mathbf{0} = \mathbf{v}$
- closure under scalar multiplication: $c\mathbf{v}$ is a vector
- inverse: for each $\mathbf{v}$, these exists $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
- associative: $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$

Vector space

- closure under addition: $\mathbf{v} + \mathbf{w}$ is a vector
- has a zero: $\mathbf{v} + \mathbf{0} = \mathbf{v}$
- closure under scalar multiplication: $c\mathbf{v}$ is a vector
- inverse: for each $\mathbf{v}$, these exists $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
- associative: $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$

Vector space

- closure under addition: $\mathbf{v}+\mathbf{w}$ is a vector
- has a zero: $\mathbf{v}+\mathbf{0}=\mathbf{v}$
- closure under scalar multiplication: $c\mathbf{v}$ is a vector
- inverse: for each $\mathbf{v}$, these exists $-\mathbf{v}$ such that $\mathbf{v}+(-\mathbf{v})=\mathbf{0}$
- associative: $(\mathbf{u}+\mathbf{v})+\mathbf{w}=\mathbf{u}+(\mathbf{v}+\mathbf{w})$

Vector space

- closure under addition: $\mathbf{v} + \mathbf{w}$ is a vector
- has a zero: $\mathbf{v} + \mathbf{0} = \mathbf{v}$
- closure under scalar multiplication: $c\mathbf{v}$ is a vector
- inverse: for each $\mathbf{v}$, these exists $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
- associative: $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$

Vector space

- closure under addition: $\mathbf{v} + \mathbf{w}$ is a vector
- has a zero: $\mathbf{v} + \mathbf{0} = \mathbf{v}$
- closure under scalar multiplication: $c\mathbf{v}$ is a vector
- inverse: for each $\mathbf{v}$, these exists $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
- associative: $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$

The C^{2^n} vector space

- For a discrete quantum system with 2^n possible states (of n qubits), we will be interested in the space C^{2^n} of 2^n-tuples of complex numbers
- It is easy to verify that C^{2^n} is a vector space

The C^{2^n} vector space

- For a discrete quantum system with 2^n possible states (of n qubits), we will be interested in the space C^{2^n} of 2^n-tuples of complex numbers
- It is easy to verify that C^{2^n} is a vector space

Inner product

- A method to combine two vectors to get a complex number
- Let $\mathbf{u} = (u_1, \cdots, u_n), \mathbf{v} = (v_1, \cdots, v_n) \in C^n$
- The inner product $\mathbf{u} \cdot \mathbf{v} = u_1^* v_1 + \cdots + u_n^* v_n$ where $z^* = a - bi$ is the complex conjugate of $z = a + bi$

Inner product

- A method to combine two vectors to get a complex number
- Let $\mathbf{u} = (u_1, \cdots, u_n), \mathbf{v} = (v_1, \cdots, v_n) \in C^n$
- The inner product $\mathbf{u} \cdot \mathbf{v} = u_1^* v_1 + \cdots + u_n^* v_n$ where $z^* = a - bi$ is the complex conjugate of $z = a + bi$

Inner product

- A method to combine two vectors to get a complex number
- Let $\mathbf{u} = (u_1, \cdots, u_n), \mathbf{v} = (v_1, \cdots, v_n) \in C^n$
- The inner product $\mathbf{u} \cdot \mathbf{v} = u_1^* v_1 + \cdots + u_n^* v_n$ where $z^* = a - bi$ is the complex conjugate of $z = a + bi$

Quangum notations

- $|\psi\rangle \in C^{2^n}$: a vector (a ket) represents a possible state of the discrete quantum system (of n qubits)
- $\langle\psi|$: dual vector (bra) of $|\psi\rangle$ (that is, a row vector)
- $\langle\psi|\phi\rangle = |\psi\rangle \cdot |\phi\rangle$: inner product of two vectors
- $|\psi\rangle \otimes |\phi\rangle$: tensor product (a $2^n \times 2^n$ vector)
- $\langle\psi|A|\phi\rangle$: inner product of $|\psi\rangle$ and $A|\phi\rangle$

Quangum notations

- $|\psi\rangle \in C^{2^n}$: a vector (a ket) represents a possible state of the discrete quantum system (of n qubits)
- $\langle\psi|$: dual vector (bra) of $|\psi\rangle$ (that is, a row vector)
- $\langle\psi|\phi\rangle = |\psi\rangle \cdot |\phi\rangle$: inner product of two vectors
- $|\psi\rangle \otimes |\phi\rangle$: tensor product (a $2^n \times 2^n$ vector)
- $\langle\psi|A|\phi\rangle$: inner product of $|\psi\rangle$ and $A|\phi\rangle$

Quangum notations

- $|\psi\rangle \in C^{2^n}$: a vector (a ket) represents a possible state of the discrete quantum system (of n qubits)
- $\langle\psi|$: dual vector (bra) of $|\psi\rangle$ (that is, a row vector)
- $\langle\psi|\phi\rangle = |\psi\rangle \cdot |\phi\rangle$: inner product of two vectors
- $|\psi\rangle \otimes |\phi\rangle$: tensor product (a $2^n \times 2^n$ vector)
- $\langle\psi|A|\phi\rangle$: inner product of $|\psi\rangle$ and $A|\phi\rangle$

Quangum notations

- $|\psi\rangle \in C^{2^n}$: a vector (a ket) represents a possible state of the discrete quantum system (of n qubits)
- $\langle\psi|$: dual vector (bra) of $|\psi\rangle$ (that is, a row vector)
- $\langle\psi|\phi\rangle = |\psi\rangle \cdot |\phi\rangle$: inner product of two vectors
- $|\psi\rangle \otimes |\phi\rangle$: tensor product (a $2^n \times 2^n$ vector)
- $\langle\psi|A|\phi\rangle$: inner product of $|\psi\rangle$ and $A|\phi\rangle$

Quangum notations

- $|\psi\rangle \in C^{2^n}$: a vector (a ket) represents a possible state of the discrete quantum system (of n qubits)
- $\langle\psi|$: dual vector (bra) of $|\psi\rangle$ (that is, a row vector)
- $\langle\psi|\phi\rangle = |\psi\rangle \cdot |\phi\rangle$: inner product of two vectors
- $|\psi\rangle \otimes |\phi\rangle$: tensor product (a $2^n \times 2^n$ vector)
- $\langle\psi|A|\phi\rangle$: inner product of $|\psi\rangle$ and $A|\phi\rangle$

Independence

- $V = \{|v_1\rangle, \cdots, |v_n\rangle\}$ is a spanning set if each vector $|v\rangle$ can be written as a linear combination of V: $v = \sum_{j=1}^{n} a_i |v_j\rangle$.
- Linear independence: a set of vectors $V = \{|v_1\rangle, \cdots, |v_n\rangle\}$ is linear independent if there does not exist non-zero a_j such that $0 = \sum_{j=1}^{n} a_i |v_j\rangle$
- a linearly independent spanning set is a basis

Independence

- $V = \{|v_1\rangle, \cdots, |v_n\rangle\}$ is a spanning set if each vector $|v\rangle$ can be written as a linear combination of V: $v = \sum_{j=1}^{n} a_i |v_j\rangle$.
- Linear independence: a set of vectors $V = \{|v_1\rangle, \cdots, |v_n\rangle\}$ is linear independent if there does not exist non-zero a_j such that $0 = \sum_{j=1}^{n} a_i |v_j\rangle$
- a linearly independent spanning set is a basis

Independence

- $V = \{|v_1\rangle, \cdots, |v_n\rangle\}$ is a spanning set if each vector $|v\rangle$ can be written as a linear combination of V: $v = \sum_{j=1}^{n} a_i |v_j\rangle$.
- Linear independence: a set of vectors $V = \{|v_1\rangle, \cdots, |v_n\rangle\}$ is linear independent if there does not exist non-zero a_j such that $0 = \sum_{j=1}^{n} a_i |v_j\rangle$
- a linearly independent spanning set is a basis

More on inner product

- Orthonogality: $|u\rangle$ and $|v\rangle$ are orthogonal if $\langle u|v\rangle = 0$
- Norm: $\||v\rangle\| = \sqrt{\langle v|v\rangle}$
- Orthonormal basis: a basis $\{|v_1\rangle, \cdots, |v_n\rangle\}$ such that $\langle v_i|v_j\rangle = \delta_{ij}$ where $\delta_{ij} = 0$ if $i \neq j$ and 1 otherwise.

More on inner product

- Orthonogality: $|u\rangle$ and $|v\rangle$ are orthogonal if $\langle u|v\rangle = 0$
- Norm: $\||v\rangle\| = \sqrt{\langle v|v\rangle}$
- Orthonormal basis: a basis $\{|v_1\rangle, \cdots, |v_n\rangle\}$ such that $\langle v_i|v_j\rangle = \delta_{ij}$ where $\delta_{ij} = 0$ if $i \neq j$ and 1 otherwise.

More on inner product

- Orthonogality: $|u\rangle$ and $|v\rangle$ are orthogonal if $\langle u|v\rangle = 0$
- Norm: $\||v\rangle\| = \sqrt{\langle v|v\rangle}$
- Orthonormal basis: a basis $\{|v_1\rangle, \cdots, |v_n\rangle\}$ such that $\langle v_i|v_j\rangle = \delta_{ij}$ where $\delta_{ij} = 0$ if $i \neq j$ and 1 otherwise.

Linear operator

- A linear operator is a matrix A that maps a vector space to another vector space
- The new vector space is spanned by: $A|v_1\rangle, \cdots, A|v_n\rangle$ (this is not necessarily a basis)

Linear operator

- A linear operator is a matrix A that maps a vector space to another vector space
- The new vector space is spanned by: $A|v_1\rangle, \cdots, A|v_n\rangle$ (this is not necessarily a basis)

The Postulates of Quantum Mechanics

- Postulate 1: A phyiscal system is equivalent to the Hilbert space
- Postulate 2: evolution of a closed physical system is equivalent to a unitry transformation
- Postulate 3: measurements of a physical system is equivalent to measurement operators
- Postulate 4: composite physical systems is equivalent of tensor product of component systems

The Postulates of Quantum Mechanics

- Postulate 1: A phyiscal system is equivalent to the Hilbert space
- Postulate 2: evolution of a closed physical system is equivalent to a unitry transformation
- Postulate 3: measurements of a physical system is equivalent to measurement operators
- Postulate 4: composite physical systems is equivalent of tensor product of component systems

The Postulates of Quantum Mechanics

- Postulate 1: A phyiscal system is equivalent to the Hilbert space
- Postulate 2: evolution of a closed physical system is equivalent to a unitry transformation
- Postulate 3: measurements of a physical system is equivalent to measurement operators
- Postulate 4: composite physical systems is equivalent of tensor product of component systems

The Postulates of Quantum Mechanics

- Postulate 1: A phyiscal system is equivalent to the Hilbert space
- Postulate 2: evolution of a closed physical system is equivalent to a unitry transformation
- Postulate 3: measurements of a physical system is equivalent to measurement operators
- Postulate 4: composite physical systems is equivalent of tensor product of component systems

Q&A

Q&A?