Quantum Computing Seminar 1

YongHyun "Aeren" An

Samsung Research

August 12, 2024
August 26, 2024

Complex Numbers

Complex Numbers

Definition ($\mathbb{C}$)

- A **complex number** is a pair of real numbers (a, b)
- The set of complex numbers is denoted by $\mathbb{C}$
- For $(a, b) \in \mathbb{C}$, $\mathrm{Re}((a, b)) := a$ and $\mathrm{Im}((a, b)) := b$
- $(a, b) + (c, d) \mapsto (a + c, b + d) : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$
- $(a, b) \cdot (c, d) \mapsto (a \cdot c - b \cdot d, a \cdot d + b \cdot c) : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$

Complex Numbers

Definition ($\mathbb{C}$)

- A **complex number** is a pair of real numbers (a, b)
- The set of complex numbers is denoted by $\mathbb{C}$
- For $(a, b) \in \mathbb{C}$, $\mathrm{Re}((a, b)) := a$ and $\mathrm{Im}((a, b)) := b$
- $(a, b) + (c, d) \mapsto (a + c, b + d) : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$
- $(a, b) \cdot (c, d) \mapsto (a \cdot c - b \cdot d, a \cdot d + b \cdot c) : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$

By convention, $(0, 1)$ is denoted by the symbol $\imath$ and $(a, 0)$ is identified with a.
$(a, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + b \cdot \imath$

Complex Numbers

- $\mathfrak{i} \cdot \mathfrak{i} = -1$
- **Field Axioms**
  - **Associativity**
    for all $a, b, c \in \mathbb{C}$, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
  - **Existence of identity**
    for all $a \in \mathbb{C}$, $0 + a = a + 0 = a$ and $1 \cdot a = a \cdot 1 = a$.
  - **Existence of additive inverse**
    for all $a \in \mathbb{C}$, there exists $-a \in \mathbb{C}$ such that $a + -a = -a + a = 0$.
  - **Existence of multiplicative inverse**
    for all $a(\neq 0) \in \mathbb{C}$, there exists $a^{-1} \in \mathbb{C}$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
  - **Commutativity**
    for all $a, b \in \mathbb{C}$, $a + b = b + a$ and $a \cdot b = b \cdot a$.
  - **Distributivity**
    for all $a, b, c \in \mathbb{C}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Definition (conjugation)

The **(complex) conjugation** of $a \in \mathbb{C}$ is $\overline{a} := \mathrm{Re}(a) - \mathrm{Im}(a) \cdot \mathrm{i}$.

Complex Numbers

Definition (conjugation)

The **(complex) conjugation** of $a \in \mathbb{C}$ is $\overline{a} := \mathrm{Re}(a) - \mathrm{Im}(a) \cdot \mathrm{i}$.

Properties of conjugation

For all $a, b \in \mathbb{C}$,

- $\overline{\overline{a}} = a$
- $\overline{a + b} = \overline{a} + \overline{b}$
- $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$
- For a real coefficient monovariate/multivariate polynomial P, $\overline{P(a, b, c, \cdots)} = P(\overline{a}, \overline{b}, \overline{c}, \cdots)$

Complex Numbers

Definition (conjugate)

$a, b \in \mathbb{C}$ are said to be **conjugate** to each other, if they can't be distinguished by a real polynomial.
i.e. for all polynomial P with real coefficient, $P(a) = 0$ if and only if $P(b) = 0$

Theorem

$(a, b), (c, d) \in \mathbb{C}$ are conjugate to each other if and only if $(a, b) = (c, d)$ or $(a, b) = \overline{(c, d)}$.

Complex Numbers

Definition (size, argument)

Given $(a, b) \in \mathbb{C}$,

- **size/absolute value/magnitude** of (a, b) is $|(a, b)| := \sqrt{\overline{(a, b)} \cdot (a, b)} = \sqrt{a^2 + b^2}$, and
- **argument** of $(a, b)(\neq 0) \in \mathbb{C}$ is and $\arg(a, b) := \arctan b/a$

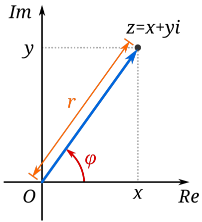

Figure: Complex number $z = x + y \cdot \mathrm{i}$ with size r and argument φ

Complex Numbers

Definition (exponentiation and polar form)

Given $\theta \in \mathbb{R}$, $e^{\theta \cdot \mathrm{i}} := \cos\theta + \sin\theta \cdot \mathrm{i}$

Complex Numbers

Definition (exponentiation and polar form)

Given $\theta \in \mathbb{R}$, $e^{\theta \cdot \mathrm{i}} := \cos\theta + \sin\theta \cdot \mathrm{i}$

This definition allows us to write $a = r \cdot e^{\theta \cdot \mathrm{i}}$ where $r = |a|$ and $\theta = \arg a$.
This is known as the **polar form**

Complex Numbers

Definition (exponentiation and polar form)

Given $\theta \in \mathbb{R}$, $e^{\theta \cdot \mathrm{i}} := \cos\theta + \sin\theta \cdot \mathrm{i}$

This definition allows us to write $a = r \cdot e^{\theta \cdot \mathrm{i}}$ where $r = |a|$ and $\theta = \arg a$.
This is known as the **polar form**

Theorem (multiplication in polar form)

$r_0 \cdot e^{\theta_0 \cdot \mathrm{i}} \cdot r_1 \cdot e^{\theta_1 \cdot \mathrm{i}} = (r_0 \cdot r_1) \cdot e^{(\theta_0 + \theta_1) \cdot \mathrm{i}}$

Complex Numbers

Definition (exponentiation and polar form)

Given $\theta \in \mathbb{R}$, $e^{\theta \cdot \mathrm{i}} := \cos \theta + \sin \theta \cdot \mathrm{i}$

This definition allows us to write $a = r \cdot e^{\theta \cdot \mathrm{i}}$ where $r = |a|$ and $\theta = \arg a$.
This is known as the **polar form**

Theorem (multiplication in polar form)

$r_0 \cdot e^{\theta_0 \cdot \mathrm{i}} \cdot r_1 \cdot e^{\theta_1 \cdot \mathrm{i}} = (r_0 \cdot r_1) \cdot e^{(\theta_0 + \theta_1) \cdot \mathrm{i}}$

Root of unity

- Given a positive integer n, equation $X^n = 1$ has exactly n complex roots: $e^{(2\pi k/n) \cdot \mathrm{i}}$ for each integer $0 \leq k < n$.
- Equivalently, $X^n - 1 = \prod_{k=0}^{n-1} (X - e^{(2\pi k/n) \cdot \mathrm{i}})$.

Linear Algebra

Linear Algebra

Definition (finite dimensional complex vector space)

An n-**dimensional complex vector space** is the set $\mathbb{C}^n$ together with the following operations.

- Vector addition
  $(a_1, \cdots, a_n) + (b_1, \cdots, b_n) \mapsto (a_1 + b_1, \cdots, a_n + b_n) : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^n$
- Scalar multiplication
  $c \cdot (a_1, \cdots, a_n) \mapsto (c \cdot a_1, \cdots, c \cdot a_n) : \mathbb{C} \times \mathbb{C}^n \to \mathbb{C}^n$
- Inner product
  $\langle (a_1, \cdots, a_n), (b_1, \cdots, b_n) \rangle \mapsto \overline{a_1} \cdot b_1 + \cdots + \overline{a_n} \cdot b_n : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$

Linear Algebra

Definition

- **Norm** of a vector $a = (a_1, \cdots, a_n) \in \mathbb{C}^n$ is $|a| := \sqrt{\langle a, a \rangle} = \sqrt{|a_1|^2 + \cdots + |a_n|^2}$.
- **Unit vector** is a vector of norm 1.
- Vectors $u, v \in \mathbb{C}^n$ are **orthogonal** if $\langle u, v \rangle = 0$.

Linear Algebra

Definition ($\mathbb{M}$)

Given a non-negative integer m and n, $\mathbb{M}_{m,n}$ is the set of functions $\{1, \cdots, m\} \times \{1, \cdots, n\} \to \mathbb{C}$.
An element A of $\mathbb{M}_{m,n}$, is called a **matrix** and we denote $A(i, j)$ by $A_{i,j}$.

Definition ($\mathbb{M}$)

Given a non-negative integer m and n, $\mathbb{M}_{m,n}$ is the set of functions $\{1, \cdots, m\} \times \{1, \cdots, n\} \to \mathbb{C}$.
An element A of $\mathbb{M}_{m,n}$, is called a **matrix** and we denote $A(i,j)$ by $A_{i,j}$.

Special matrices

- $I \in \mathbb{M}_{n,n}$ is the matrix with $I_{i,j} = [i = j]$.
- $O \in \mathbb{M}_{n,n}$ is the matrix with $I_{i,j} = 0$.

Definition ($\mathbb{M}$)

Given a non-negative integer m and n, $\mathbb{M}_{m,n}$ is the set of functions $\{1, \cdots, m\} \times \{1, \cdots, n\} \to \mathbb{C}$.
An element A of $\mathbb{M}_{m,n}$, is called a **matrix** and we denote $A(i,j)$ by $A_{i,j}$.

Special matrices

- $I \in \mathbb{M}_{n,n}$ is the matrix with $I_{i,j} = [i = j]$.
- $O \in \mathbb{M}_{n,n}$ is the matrix with $I_{i,j} = 0$.

Definition (inverse matrix)

A matrix $A \in \mathbb{M}_{n,n}$ is **invertible**, if there exists a matrix $B \in \mathbb{M}_{n,n}$ with $A \cdot B = I$. We write $B = A^{-1}$.

Operations on matrix

- Matrix-matrix multiplication: $\cdot : \mathbb{M}_{m,n} \times \mathbb{M}_{n,k} \to \mathbb{M}_{m,k}$
  $(A \cdot B)_{i,k} = \sum_{j=1}^{n} A_{i,j} \cdot B_{j,k}$
- Matrix-scalar multiplication $\cdot : \mathbb{M}_{m,n} \times \mathbb{C}^n \to \mathbb{C}^m$
  $(A \cdot v)_i = \sum_{j=1}^{n} A_{i,j} \cdot v_j$
- Conjugate transposition $\circ^H = \mathbb{M}_{m,n} \to \mathbb{M}_{n,m}$
  $(A^H)_{i,j} = \overline{A_{j,i}}$

Linear Algebra

We identify $v \in \mathbb{C}^n$ with a matrix $A \in \mathbb{M}_{n,1}$ where $A_{i,1} = v_i$.

We identify $v \in \mathbb{C}^n$ with a matrix $A \in \mathbb{M}_{n,1}$ where $A_{i,1} = v_i$.

Definition (unitary matrix)

A matrix $A \in \mathbb{M}_{n,n}$ is **unitary** if $A^H \cdot A = I$.

Linear Algebra

We identify $v \in \mathbb{C}^n$ with a matrix $A \in \mathbb{M}_{n,1}$ where $A_{i,1} = v_i$.

Definition (unitary matrix)

A matrix $A \in \mathbb{M}_{n,n}$ is **unitary** if $A^H \cdot A = I$.

Theorem

- A matrix $A \in \mathbb{M}_{n,n}$ is unitary if and only if each column vector of A is a unit vector that is pairwise orthogonal.
- A matrix $A \in \mathbb{M}_{n,n}$ is unitary if and only if for all $u, v \in \mathbb{C}^n$, $\langle A \cdot u, A \cdot v \rangle = \langle u, v \rangle$.
- Given a unitary matrix $A \in \mathbb{M}_{n,n}$ and $v \in \mathbb{C}^n$, $|A \cdot v| = |v|$.
- The product of two unitary matrices is unitary.

Linear Algebra

Definition (Kronecker product)

$\otimes : \mathbb{M}_{m,n} \times \mathbb{M}_{p,q} \to \mathbb{M}_{m \cdot p, n \cdot q}$
$(A \otimes B)_{p \cdot (i-1)+k, q \cdot (j-1)+l} = A_{i,j} \cdot B_{k,l}$

$$A \otimes B = \begin{bmatrix} A_{1,1} \cdot B & \cdots & A_{1,n} \cdot B \\ \vdots & \ddots & \vdots \\ A_{m,1} \cdot B & \cdots & A_{m,n} \cdot B \end{bmatrix}$$

Linear Algebra

The followings hold for matrices A, B, C with suitable size, scalar $k \in \mathbb{C}$, and vectors u, v.

1. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$
2. $A \otimes O = O \otimes A = O$
3. $A \otimes (B + C) = A \otimes B + A \otimes C$
4. $(A + B) \otimes C = A \otimes C + B \otimes C$
5. $(k \cdot A) \otimes B = A \otimes (k \cdot B) = k \cdot (A \otimes B)$
6. $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$
7. $(A \otimes B)^H = A^H \otimes B^H$
8. $A \otimes B$ is invertible if and only if A and B are both invertible, in which case $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.
9. $|u \otimes v| = |u| \cdot |v|$
10. If A and B are unitary, so is $A \otimes B$.

Linear Algebra

Definition (Dirac notation / bra-ket notation)

Let n be a fixed integer, and let $v_i \in \mathbb{C}^n$ with $v_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ (single 1 at the i-th entry).

- **Ket**: we identify v_i with $|i\rangle$.
- **Bra**: we identify v_i^H with $\langle i|$.
- $|i, j\rangle := |i\rangle \otimes |j\rangle$
- $\langle i, j| := \langle i| \otimes \langle j|$

The End