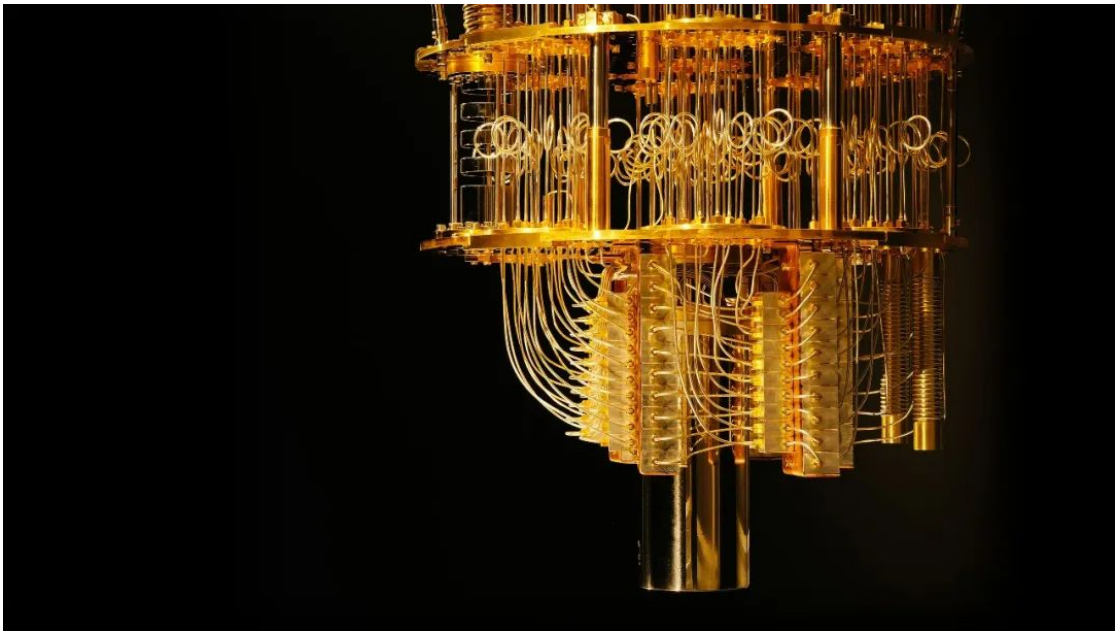
Lecture Notes for Quantum Computing

Chao Liang

cliang@whu.edu.cn

National Engineering Research Centre for Multimedia Software (NERCMS)

School of Computer Science, Wuhan University



Spring, 2024

(Last updated on March 5, 2024)

Contents

1 Introduction and Complex Number

1.1 Introduction to Quantum Computing

1.1.1 A Brief History

Quantum Mechanics as a branch of physics began with a set of scientific discoveries in the late 19th Century and has been in active development ever since. Most people will point to the 1980s as the start of physicists actively looking at computing with quantum systems[1]:

- **1982:** History of quantum computing starts with Richard Feynman lectures on the potential advantages of computing with quantum systems.
- **1985:** David Deutsch publishes the idea of a "universal quantum computer".
- **1994:** Peter Shor presents an algorithm that can efficiently find the factors of large numbers, significantly outperforming the best classical algorithm and theoretically putting the underpinning of modern encryption at risk (referred to now as Shors algorithm).
- **1996:** Lov Grover presents an algorithm for quantum computers that would be more efficient for searching databases (referred to now as Groves search algorithm).
- **1996:** Seth Lloyd proposes a quantum algorithm which can simulate quantum-mechanical systems.
- **1999:** D-Wave Systems founded by Geordie Rose.
- **2000:** Eddie Farhi at MIT develops idea for adiabatic quantum computing.
- **2001:** IBM and Stanford University publish the first implementation of Shors algorithm, factoring 15 into its prime factors on a 7-qubit processor.
- **2010:** D-Wave One: first commercial quantum computer released (annealer).
- **2016:** IBM makes quantum computing available on IBM Cloud.
- **2019:** Google claims the achievement of quantum supremacy. Quantum Supremacy was termed by John Preskill in 2012 to describe when quantum systems could perform tasks surpassing those in the classical world.

A more complete history comes from the quantumpedia[2], where the development of quantum computing is divided into five distinct periods (Figure 1.1):

[1] https://thequantuminsider.com/2020/05/26/history-of-quantum-computing/
[2] https://quantumpedia.uk/a-brief-history-of-quantum-computing-e0bbd05893d0

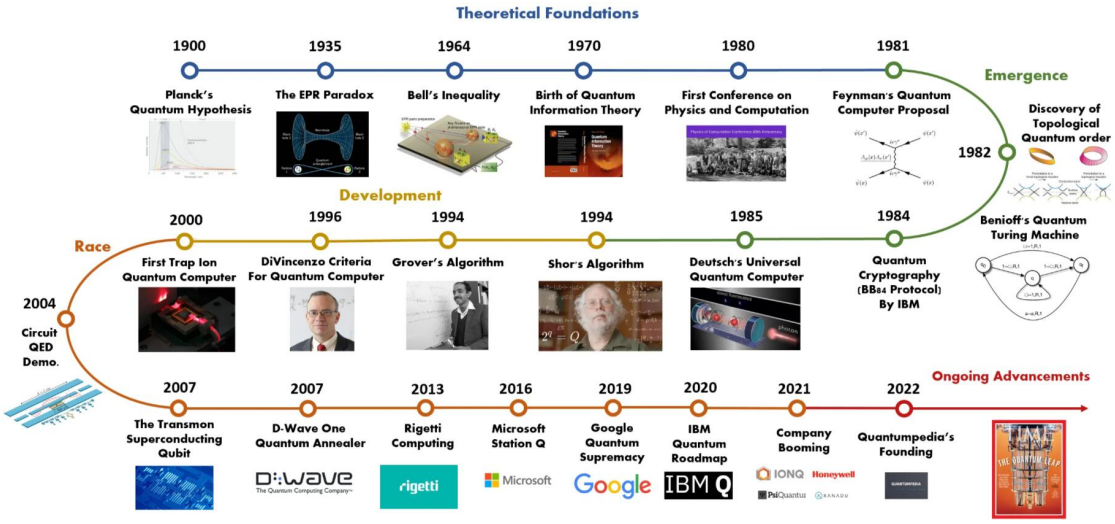


Figure 1.1: A Brief History of Quantum Computing (Copyright: Quantumpedia)

- **1900–1980:** The Theoretical Foundations of Quantum Computing.
- **1980–1994:** The Emergence of Quantum Computing.
- **1994–2000:** The Development of Quantum Algorithms.
- **2000–2021:** The Race to Build Quantum Computers.
- **2021–present:** Ongoing Advancements.

1.1.2 Prof. Andrew Chi-Chih Yao's Talk in Micius Salon

Prof. Yao gave a talk entitled "The Advent of Quantum Computing" in Micius Salon in 2018[3]. Here are some key points:

- Two key topics: (1) what is the nature of quantum computer?; and (2) where does quantum computer gets its power from?
- The particle-wave duality plays the starting role in making it possible for us to do quantum computing faster than classic computing under certain circumstances
- Richard Feynman's question: can quantum physics be simulated efficiently? Answer: unlikely by a classic computer, but hopefully by a quantum computer.
- The comparison of classic computer and quantum computers (Figure 1.2). Classic computers manipulate classic bits $0110\cdots$ with Boolean operations in $\{0,1\}^n$, while quantum computers manipulate quantum bits $|0101\cdots\rangle$ with "rotations" in $\mathbb{C}^{2^n}$

[3] https://www.bilibili.com/video/BV1Ct411Z7BQ/?spm_id_from=333.337.search-card.all.click&vd_source=322773747f9aa504da745054e83290e9

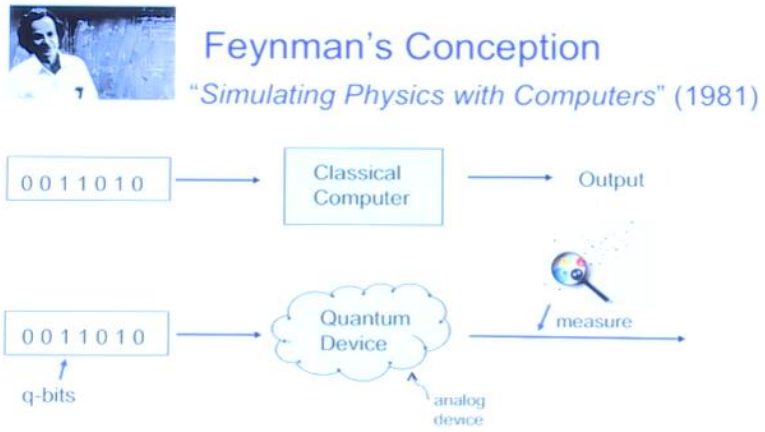


Figure 1.2: The comparison of classic and quantum computers.

- The **parallel superposition** is brought by the fact that each quantum bit represents not a single state, but a "probabilistic distribution" of states as shown in Figure 1.3[4].

(a) Schrodinger's cat (b) Monkey King's 72 changes (c) Naruto's shadow clone jutsu

Figure 1.3: Some examples of parallel superposition.

- Parallelism could speed up computational tasks by parallel search.

1.2 Complex Numbers

The original motivation for the introduction of complex numbers was seeking solutions of polynomial equations. Here is the simplest example:

$$x^2 + 1 = 0 \tag{1.1}$$

Obviously, we cannot find its solution in the set of real numbers. To solve this problem, Mathematics introduces following definitions.

The fundamental reason we review complex numbers first in this course is that physics has recognized that quantum mechanics must be complex in nature[5] (Figure 1.4).

[4] Strictly speaking, Figure 1.3a is more accurate than the other two because states in quantum computing are mutually exclusive rather than similar to each other.

[5] https://physics.aps.org/articles/v15/7

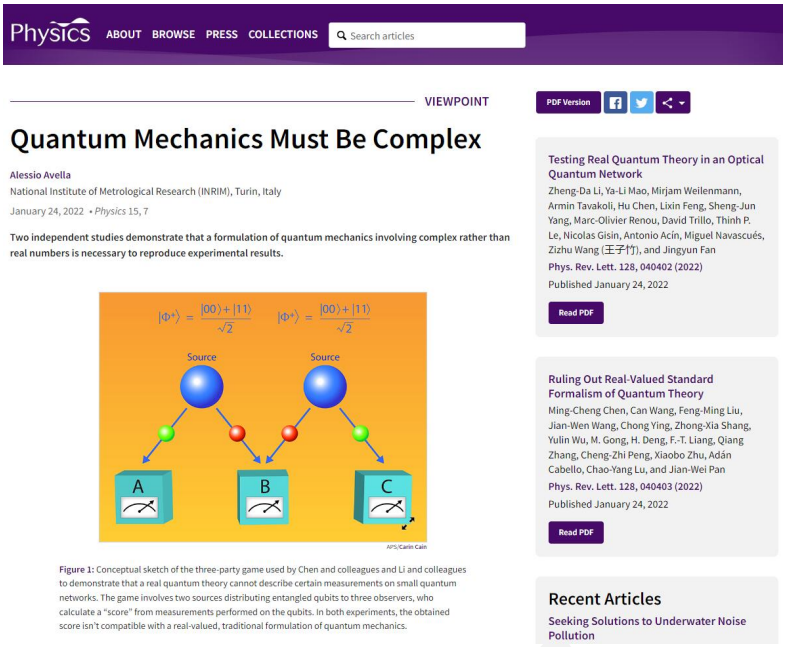


Figure 1.4: Quantum mechanics must be complex (source: APS)

1.2.1 Definitions

Definition 1.1 (Imaginary Number). *An imaginary number is a real number multiplied by the imaginary unit i, which is defined by its property $i^2 = 1$ or $i = \sqrt{-1}$.*

Definition 1.2 (Complex Number). *A complex number is a hybrid entity which adds a real number with an imaginary number, for instance,*

$$c = a + b \times i = a + bi \tag{1.2}$$

where a, b are two real numbers, a is called the real part of c, whereas b is its imaginary part. The set of all complex numbers will be denoted as $\mathbb{C}$. When the $\times$ is understood, we shall omit it.

Proposition 1 (Fundamental Theorem of Algebra). *Every polynomial equation of one variable with complex coefficients has a complex solution.*

1.2.2 The Algebra of Complex Numbers

Definition 1.3 (Ordered Pair Representation). *Ordered pair representation defines a complex number as an ordered pair of reals:*

$$c = a + b \mapsto (a, b) \tag{1.3}$$

Hence, ordinary real numbers can be identified with pairs $(a, 0)$

$$a \mapsto (a, b) \tag{1.4}$$

whereas imaginary numbers can be identified with pairs $(0, b)$. In particular,

$$i \mapsto (0, 1) \tag{1.5}$$

The four **arithmetic operations** between two complex numbers can be expressed as:

- Addition:
$$c_1 + c_2 = (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \tag{1.6}$$
- Subtraction:
$$c_1 - c_2 = (a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2) \tag{1.7}$$
- Multiplication:
$$c_1 \times c_2 = (a_1, b_1) \times (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1) \tag{1.8}$$
- Subdivision:
$$\frac{c_1}{c_2} = \frac{(a_1, b_1)}{(a_2, b_2)} = \left(\frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2}, \frac{a_2 b_1 - a_1 b_2}{a_2^2 + b_2^2} \right) \tag{1.9}$$

With the addition and multiplication operations, we can re-write a complex number as

$$c = a + bi = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \times (0, 1) \tag{1.10}$$

and from the denominator in the quotient formula in Eq.(1.9), we can define the **modulus** of a complex number as:

$$|c| = |a + bi| = +\sqrt{a^2 + b^2} \tag{1.11}$$

which has two useful properties:

- Property 1: $\forall c_1, c_2 \in \mathbb{C}, |c_1||c_2| = |c_1 c_2|$.
- Property 2: $\forall c_1, c_2 \in \mathbb{C}, |c_1 + c_2| \leq |c_1| + |c_2|$.

where the second property is also called triangular inequality of modulus operation.

Based on the above basic operations, it is easy to verify that complex numbers have the following **algebraic properties**:

- Addition has an identity called **additive identity**: $(0, 0)$, such that
$$\forall c \in \mathbb{C}, c + (0, 0) = c \tag{1.12}$$
- Multiplication has an identity called **multiplicative identity**: $(1, 0)$, such that
$$\forall c \in \mathbb{C}, c \times (1, 0) = (1, 0) \times c = c \tag{1.13}$$

- Both addition and multiplication are commutative:

$$\begin{cases} c_1 + c_2 = c_2 + c_1 \\ c_1 \times c_2 = c_2 \times c_1 \end{cases} \tag{1.14}$$

- Both addition and multiplication are associative:

$$\begin{cases} (c_1 + c_2) + c_3 = c_1 + (c_2 + c_3) \\ (c_1 \times c_2) \times c_3 = c_1 \times (c_2 \times c_3) \end{cases} \tag{1.15}$$

- Multiplication distributes with respect to addition:

$$c_1 \times (c_2 + c_3) = c_1 \times c_2 + c_1 \times c_3 \tag{1.16}$$

- Subtraction is defined everywhere.
- Division is defined everywhere except when the divisor is zero.

Besides basic arithmetic operations and modulus operation, complex numbers have a unique operation called **conjugation**. If $c = a + bi$ is an arbitrary complex number, then the conjugate of c is $\overline{c} = a - bi$. Two numbers related by conjugation are said to be **complex conjugates** of each other. The conjugation operation has several basic properties:

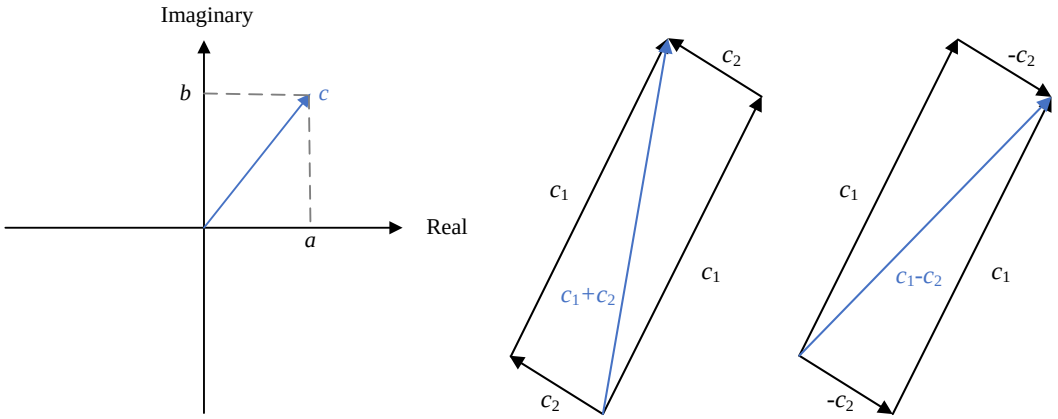
- Property 1: Conjugate respects addition $\overline{c_1 + c_2} = \overline{c_1} + \overline{c_2}$.
- Property 2: Conjugate respects multiplication $\overline{c_1 \times c_2} = \overline{c_1} \times \overline{c_2}$.
- Property 3: Conjugate $c \mapsto \overline{c}$ is bijective.
- Property 4: The modulus squared of a complex number is obtained by multiplying the number with its conjugate $c \times \overline{c} = |c|^2$.

1.2.3 The Geometry of Complex Numbers

Definition 1.4 (**Complex Plane** or **Argand Plane**). *The complex plane is the plane formed by the complex numbers, with a Cartesian coordinate system such that the horizontal x-axis, called the real axis, is formed by the real numbers, and the vertical y-axis, called the imaginary axis, is formed by the imaginary numbers.*

In the complex plane (Figure 1.5a), we can easily find that the modulus is nothing more than the length of the vector. Indeed, the length of a vector, via Pythagoras theorem, is the square root of the sum of the squares of its edges, which is precisely the modulus, as defined in the previous section.

Next comes addition: vectors can be added using the so-called **parallelogram rule** illustrated by Figure 1.5b. In words, draw the parallelogram whose parallel edges are the two vectors to be added; their sum is the diagonal.



(a) Complex plane (b) Addition (c) Subtraction

Figure 1.5: The complex plane (a) and parallelogram rule for (b) addition and (c) subtraction.

Subtraction too has a clear geometric meaning: subtracting c_2 from c_1 is the same as adding the negation of c_2, i.e., $-c_2$, to c_1 (Figure 1.5c).

To give a simple geometrical meaning to multiplication, we need to develop yet another characterization of complex numbers.

Definition 1.5 (**Polar Coordinate System**). *The polar coordinate system is a two-dimensional coordinate system in which each point on a plane is determined by a distance ρ from a reference point and an angle θ from a reference direction.*

Similar to the previous **Cartesian representation** (a, b), the **polar representation** (ρ, θ) is capable to uniquely determine a complex number because these two representations can be mutually converted:

$$(a, b) \mapsto (\rho, \theta) \tag{1.17}$$

where ρ is the modulus

$$\rho = \sqrt{a^2 + b^2} \tag{1.18}$$

and θ is also easy, via trigonometry

$$\theta = \tan^{-1}\left(\frac{b}{a}\right) \tag{1.19}$$

$$(\rho, \theta) \mapsto (a, b) \tag{1.20}$$

where a is the real part

$$a = \rho \cos(\theta) \tag{1.21}$$

and b is the imaginary part

$$b = \rho \sin(\theta) \tag{1.22}$$

In physics and engineering, angle θ is also known as **phase** and distance ρ is also known as **magnitude**. Hence, we have another definition of a complex number

Definition 1.6 (Complex Number). *A complex number is a magnitude and a phase.*

We are now ready for multiplication: given two complex numbers in polar coordinates, $c_1 = (\rho_1, \theta_1)$ and $c_2 = (\rho_2, \theta_2)$, their product can be obtained by simply multiplying their magnitude and adding their phase:

$$c_1 \times c_2 = (\rho_1, \theta_1) \times (\rho_2, \theta_2) = (\rho_1 \rho_2, \theta_1 + \theta_2) \tag{1.23}$$

Now that we are armed with a geometric way of looking at multiplication, we can tackle division as well. After all, division is nothing more than the inverse operation of multiplication:

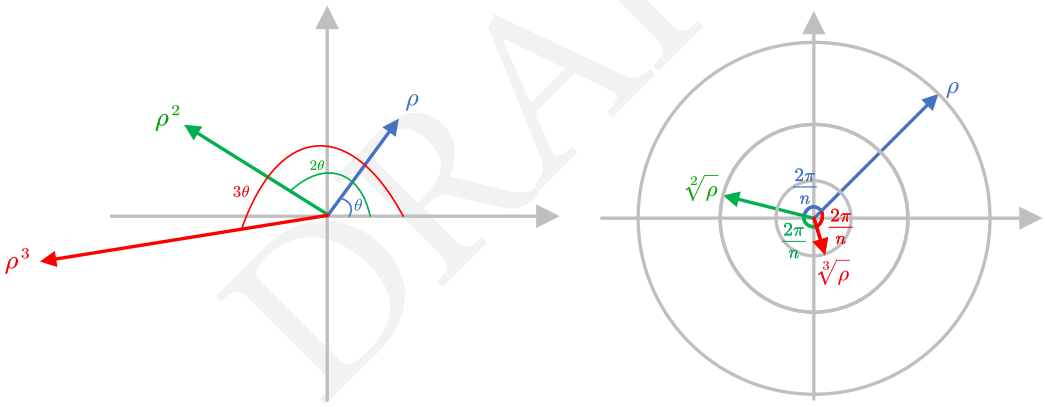
$$\frac{c_1}{c_2} = \left(\frac{\rho_1}{\rho_2}, \theta_1 - \theta_2 \right) \tag{1.24}$$

On this basis, we can further derive fast n-order power (Figure 1.6a) and root (Figure 1.6b) calculations about a complex number $c = (\rho, \theta)$

$$c^n = (\rho^n, n\theta) \tag{1.25}$$

and

$$c^{\frac{1}{n}} = \left(\rho^{\frac{1}{n}}, \frac{1}{n}(\theta + k2\pi) \right), \text{ where } k = 0, 1, \cdots, n-1 \tag{1.26}$$



(a) The n-order Powers (b) The n-order roots

Figure 1.6: The n-order powers (a) and roots (b) of a complex number.

2 Complex Vector Space

2.1 Complex Vector Space

Definition 2.1 (Complex Vector Space). *A complex vector space is a nonempty set $\mathbb{V}$, whose elements we shall call vectors, with three operations*

- *Addition:* $+: \mathbb{V} \times \mathbb{V} \to \mathbb{V}$
- *Negation:* $-: \mathbb{V} \to \mathbb{V}$
- *Scalar multiplication:* $\cdot: \mathbb{C} \times \mathbb{V} \to \mathbb{V}$

and a distinguished element called the ***zero vector*** $\mathbf{0} \in \mathbb{V}$ *in the set. These operations and zero must satisfy the following properties:* $\forall \boldsymbol{v}, \boldsymbol{w}, \boldsymbol{x} \in \mathbb{V}$ *and for all* $c, c_1, c_2 \in \mathbb{C}$,

i. *Commutativity of addition:* $\boldsymbol{v} + \boldsymbol{w} = \boldsymbol{w} + \boldsymbol{v}$,
ii. *Associativity of addition:* $(\boldsymbol{v} + \boldsymbol{w}) + \boldsymbol{x} = \boldsymbol{v} + (\boldsymbol{w} + \boldsymbol{x})$,
iii. *Additive identity:* $\boldsymbol{v} + \mathbf{0} = \boldsymbol{v} = \mathbf{0} + \boldsymbol{v}$,
iv. *Additive inverse:* $\boldsymbol{v} + (-\boldsymbol{v}) = \mathbf{0} = (-\boldsymbol{v}) + \boldsymbol{v}$,
v. *Multiplication identity:* $1 \cdot \boldsymbol{v} = \boldsymbol{v}$,
vi. *Scalar multiplication distributes over addition:* $c \cdot (\boldsymbol{v} + \boldsymbol{w}) = c \cdot \boldsymbol{v} + c \cdot \boldsymbol{w}$,
vii. *Scalar multiplication distributes over complex addition:* $(c_1 + c_2) \cdot \boldsymbol{v} = c_1 \cdot \boldsymbol{v} + c_2 \cdot \boldsymbol{v}$,

Example 2.1: $\mathbb{C}^n$

$\mathbb{C}^n$, the set of vectors of length n with complex entries, is a complex vector space.

Example 2.2: $\mathbb{C}^{m \times n}$

$\mathbb{C}^{m \times n}$, the set of all m-by-n matrices (two-dimensional arrays) with complex entries, is a complex vector space.

2.1.1 Unary Operations

Three **unary operations** for $\forall \mathbf{A} \in \mathbb{C}^{m\times n}$

- Transpose:
$$\mathbf{A}^\top \in \mathbb{C}^{n\times m} \text{ such that } \mathbf{A}^\top(j,k) = \mathbf{A}^\top(k,j) \tag{2.1}$$
- Conjugate:
$$\overline{\mathbf{A}} \in \mathbb{C}^{m\times n} \text{ such that } \overline{\mathbf{A}}(j,k) = \overline{\mathbf{A}(j,k)} \tag{2.2}$$
- Ajoint:
$$\mathbf{A}^\dagger \in \mathbb{C}^{n\times m} \text{ such that } \mathbf{A}^\dagger(j,k) = \overline{\mathbf{A}(k,j)} \tag{2.3}$$

Property 1 (Properties of transpose)**.** $\forall c \in \mathbb{C}$ *and* $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{m\times n}$

- *Transpose is idempotent:*
$$(\mathbf{A}^\top)^\top = \mathbf{A} \tag{2.4}$$
- *Transpose respects addition:*
$$(\mathbf{A}+\mathbf{B})^\top = \mathbf{A}^\top + \mathbf{B}^\top \tag{2.5}$$
- *Transpose respects scalar multiplication:*
$$(c\cdot\mathbf{A})^\top = c\cdot\mathbf{A}^\top \tag{2.6}$$

Property 2 (Properties of conjugate)**.** $\forall c \in \mathbb{C}$ *and* $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{m\times n}$

- *Conjugate is idempotent:*
$$\overline{\overline{\mathbf{A}}} = \mathbf{A} \tag{2.7}$$
- *Conjugate respects addition:*
$$\overline{\mathbf{A}+\mathbf{B}} = \overline{\mathbf{A}} + \overline{\mathbf{B}} \tag{2.8}$$
- *Conjugate respects scalar multiplication:*
$$\overline{c\cdot\mathbf{A}} = \overline{c}\cdot\overline{\mathbf{A}} \tag{2.9}$$

Property 3 (Properties of adjoint)**.** $\forall c \in \mathbb{C}$ *and* $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{m\times n}$

- *Adjoint is idempotent:*
$$(\mathbf{A}^\dagger)^\dagger = \mathbf{A} \tag{2.10}$$
- *Adjoint respects addition:*
$$(\mathbf{A}+\mathbf{B})^\dagger = \mathbf{A}^\dagger + \mathbf{B}^\dagger \tag{2.11}$$
- *Conjugate respects scalar multiplication:*
$$(c\cdot\mathbf{A})^\dagger = \overline{c}\cdot\mathbf{A}^\dagger \tag{2.12}$$

2.1.2 Matrix Multiplication

Property 4 (Properties of matrix multiplication). *$\forall \mathbf{A} \in \mathbb{C}^{m\times n}, \mathbf{B} \in \mathbb{C}^{n\times p}, \mathbf{C} \in \mathbb{C}^{n\times p}$, and $\mathbf{D} \in \mathbb{C}^{p\times q}$,*

- *Matrix multiplication distributes over addition:*

$$\mathbf{A} \times (\mathbf{B} + \mathbf{C}) = (\mathbf{A} \times \mathbf{B}) + (\mathbf{A} \times \mathbf{C}) \tag{2.13}$$

$$(\mathbf{B} + \mathbf{C}) \times \mathbf{D} = (\mathbf{B} \times \mathbf{D}) + (\mathbf{C} \times \mathbf{D}) \tag{2.14}$$

- *Matrix multiplication respect scalar multiplication:*

$$c \cdot (\mathbf{A} \times \mathbf{B}) = (c \cdot \mathbf{A}) \times \mathbf{B} = \mathbf{A} \times (c \cdot \mathbf{B}) \tag{2.15}$$

- *Matrix multiplication relates to the transpose:*

$$(\mathbf{A} \times \mathbf{B})^\top = \mathbf{B}^\top \times \mathbf{A}^\top \tag{2.16}$$

- *Matrix multiplication respects to the conjugate:*

$$\overline{\mathbf{A} \times \mathbf{B}} = \overline{\mathbf{A}} \times \overline{\mathbf{B}} \tag{2.17}$$

- *Matrix multiplication relates to the adjoint:*

$$(\mathbf{A} \times \mathbf{B})^\dagger = \mathbf{B}^\dagger \times \mathbf{A}^\dagger \tag{2.18}$$

The physical explanation. The elements of $\mathbb{C}^n$ are the ways of describing the states of a quantum system. Some suitable elements of $\mathbb{C}^{nn}$ will correspond to the changes that occur to the states of a quantum system. Given a state $\boldsymbol{x} \in \mathbb{C}^n$ and a matrix $\mathbf{A} \in \mathbb{C}^{n\times n}$, we shall form another state of the system $\mathbf{A} \times \boldsymbol{x}$ which is an element of $\mathbb{C}^n$. Formally, $\times$ in this case is a function $\times : \mathbb{C}^{n\times n} \times \mathbb{C}^n \to \mathbb{C}^n$. We say that the algebra of matrices "**acts**" on the vectors to yield new vectors.

2.1.3 Linear Map

Definition 2.2 (Linear Map). *A linear map from $\mathbb{V}$ to $\mathbb{V}'$ is a function $f : \mathbb{V} \to \mathbb{V}', \forall \boldsymbol{v}, \boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{V}$, and $c \in \mathbb{C}$ where*

- *f respects the addition:*

$$f(\boldsymbol{v}_1 + \boldsymbol{v}_2) = f(\boldsymbol{v}_1) + f(\boldsymbol{v}_2) \tag{2.19}$$

- *f respects the scalar multiplication:*

$$f(c \cdot \boldsymbol{v}) = c \cdot f(\boldsymbol{v}) \tag{2.20}$$

The physical explanation. We shall call any linear map from a complex vector space to itself an **operator**. If $F : \mathbb{C}^n \to \mathbb{C}^n$ is an operator on $\mathbb{C}^n$ and $\mathbf{A}$ is an n-by-n matrix such that for all $\boldsymbol{v}$ we have $F(\boldsymbol{v}) = \mathbf{A} \times \boldsymbol{v}$, then we say that F is **represented** by $\mathbf{A}$. Several different matrices might represent the same operator.

2.2 Basis and Dimension

2.2.1 Basis

Definition 2.3 (Linear Combination). *Let $\mathbb{V}$ be a complex (real) vector space. $\boldsymbol{v} \in \mathbb{V}$ is a linear combination of the vectors $\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{n-1}$ in $\mathbb{V}$ if $\mathbf{v}$ can be written as*

$$\boldsymbol{v} = c_0 \cdot \boldsymbol{v}_0 + c_1 \cdot \boldsymbol{v}_1 + \cdots + c_{n-1} \cdot \boldsymbol{v}_{n-1} \tag{2.21}$$

for some $c_0, c_1, \cdots, c_{n-1}$ in $\mathbb{C}(\mathbb{R})$.

Definition 2.4 (Linearly independent). *A set $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{n-1}\}$ of vectors in $\mathbb{V}$ is called linearly independent if*

$$\mathbf{0} = c_0 \cdot \boldsymbol{v}_0 + c_1 \cdot \boldsymbol{v}_1 + \cdots + c_{n-1} \cdot \boldsymbol{v}_{n-1} \tag{2.22}$$

implies that $c_0 = c_1 = \cdots = c_{n-1} = 0$. This means that the only way that a linear combination of the vectors can be the zero vector is if all the c_j are zero.

Corollary 1. *For any $\boldsymbol{v}_{i|i=0,1,\cdots,n-1}$, cannot be written as a combination of the others $\{\boldsymbol{v}_j\}_{j=0,j\neq i}^{n-1}$*

Corollary 2. *For any $\mathbf{0} \neq \boldsymbol{v} \in \mathbb{V}$, unique coefficients $\{c_i\}_{i=0}^{n-1}$*

Definition 2.5 (Basis). *A set $\mathcal{B} = \{\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{n-1}\} \subseteq \mathbb{V}$ of vectors is called a basis of a (complex) vector space $\mathbb{V}$ if both*

- $\forall \boldsymbol{v} \in \mathbb{V}, \boldsymbol{v} = c_0 \cdot \boldsymbol{v}_0 + c_1 \cdot \boldsymbol{v}_1 + \cdots + c_{n-1} \cdot \boldsymbol{v}_{n-1}$
- $\{\boldsymbol{v}_i | \boldsymbol{v}_0 \in \mathbb{V}\}_{i=0}^{n-1}$ *is linearly independent*

2.2.2 Dimension

Definition 2.6 (Dimension). *The dimension of a (complex) vector space is the number of elements in a basis of the vector space.*

Definition 2.7 (Transition Matrix). *A change of basis matrix or a transition matrix from basis $\mathcal{B}$ to basis $\mathcal{D}$ is a matrix $\mathbf{M}_{\mathcal{D}\leftarrow\mathcal{B}}$ such that their coefficients satisfy*

$$\boldsymbol{v}_{\mathcal{D}} = \mathbf{M}_{\mathcal{D}\leftarrow\mathcal{B}} \times \boldsymbol{v}_{\mathcal{B}} \tag{2.23}$$

In other words, $\mathbf{M}_{\mathcal{D}\leftarrow\mathcal{B}}$ is a way of getting the coefficients with respect to one basis from the coefficients with respect to another basis.

Remark. *Utilities of Transition Matrix*

- *Operator re-representation in a new basis*

$$\mathbf{A}_{\mathcal{D}} = \mathbf{M}_{\mathcal{D}\leftarrow\mathcal{B}}^{-1} \times \mathbf{A}_{\mathcal{B}} \times \mathbf{M}_{\mathcal{D}\leftarrow\mathcal{B}} \tag{2.24}$$

- *State re-representation in a new basis*

$$\boldsymbol{v}_{\mathcal{D}} = \mathbf{M}_{\mathcal{D}\leftarrow\mathcal{B}} \times \boldsymbol{v}_{\mathcal{B}} \tag{2.25}$$

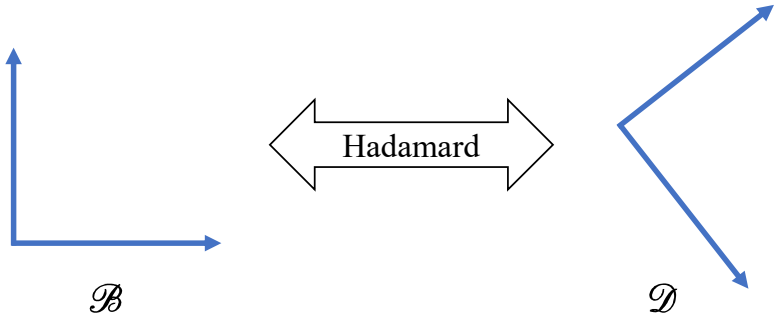


Figure 2.1: The Hardamard matrix for basis transition

Example 2.3: Hadamard Matrix

In $\mathbb{R}^2$, the transition matrix from the canonical basis

$$\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}\right\} \tag{2.26}$$

to this other basis

$$\left\{\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}, \begin{bmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{bmatrix}\right\} \tag{2.27}$$

is the Hadamard matrix:

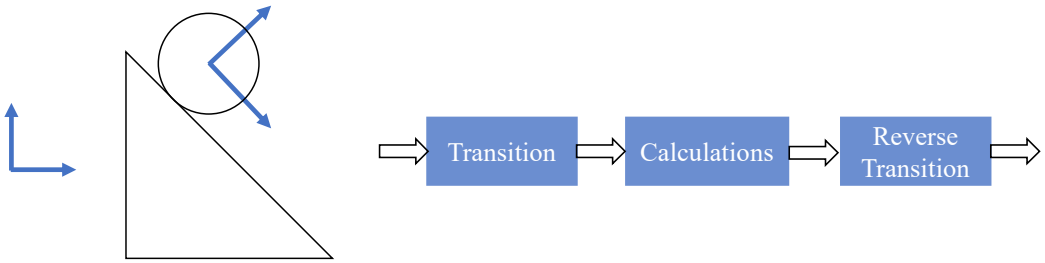
$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix} \tag{2.28}$$

as shown in Figure 2.1.

The motivation to change basis. In physics, we are often faced with a problem in which it is easier to calculate something in a noncanonical basis. For example, consider a ball rolling down a ramp as depicted in Figure 2.2a.

The ball will not be moving in the direction of the canonical basis. Rather it will be rolling downward in the direction of +45, 45 basis. Suppose we wish to calculate when this ball will reach the bottom of the ramp or what is the speed of the ball. To do this, we change the problem from one in the canonical basis to one in the other basis. In this other basis, the motion is easier to deal with. Once we have completed the calculations, we change our results into the more understandable canonical basis and produce the desired answer. We might envision this as the flowchart shown in Figure 2.2b.

Throughout this course, we shall go from one basis to another basis, perform some calculations, and finally revert to the original basis. The Hadamard matrix will frequently be the means by which we change the basis.



(a) A ball rolling down a ramp

(b) Problem-solving flowchart

Figure 2.2: Basis transition example (a) and flowchart (b).

2.3 Inner Product and Hilbert Space

2.3.1 Inner Product

Definition 2.8 (Inner Product). *An inner product (also called a dot product or scalar product) on a complex vector space $\mathbb{V}$ is a function*

$$\langle \cdot, \cdot \rangle : \mathbb{V} \times \mathbb{V} \to \mathbb{C} \tag{2.29}$$

that satisfies the following conditions for all $\boldsymbol{v}$, $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, and $\boldsymbol{v}_3$ in $\mathbb{V}$ and for $a, c \in \mathbb{C}$:

i. Nondegenerate:

$$\langle \boldsymbol{v}, \boldsymbol{v} \rangle \geq 0 \text{ and } \langle \boldsymbol{v}, \boldsymbol{v} \rangle \Leftrightarrow \boldsymbol{v} = \boldsymbol{0} \tag{2.30}$$

ii. Respects addition:

$$\langle \boldsymbol{v}_1 + \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_3 \rangle + \langle \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle \tag{2.31}$$

$$\langle \boldsymbol{v}_1, \boldsymbol{v}_2 + \boldsymbol{v}_3 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle + \langle \boldsymbol{v}_1, \boldsymbol{v}_3 \rangle \tag{2.32}$$

iii. Respects scalar multiplication:

$$\langle c \cdot \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \overline{c} \times \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle \tag{2.33}$$

$$\langle \boldsymbol{v}_1, c \cdot \boldsymbol{v}_2 \rangle = c \times \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle \tag{2.34}$$

iv. Skew symmetric:

$$\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \overline{\langle \boldsymbol{v}_2, \boldsymbol{v}_1 \rangle} \tag{2.35}$$

Definition 2.9 (Inner Product Space). *A vector space with an inner space.*

Example 2.4: Inner product in $\mathbb{R}^n$

$\mathbb{R}^n$: The inner product is given as

$$\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \boldsymbol{v}_1^\top \times \boldsymbol{v}_2 \tag{2.36}$$

Example 2.5: Inner product in $\mathbb{C}^n$

$\mathbb{C}^n$: The inner product is given as

$$\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \boldsymbol{v}_1^\dagger \times \boldsymbol{v}_2 \tag{2.37}$$

Example 2.6: Inner product in $\mathbb{R}^{n\times n}$

$\mathbb{R}^{n\times n}$ has an inner product given for matrices $\mathbf{A}, \mathbf{B} \in \mathbb{R}^{n\times n}$ as

$$\langle \mathbf{A}, \mathbf{B} \rangle = \mathrm{Tr}(\mathbf{A}^\top \times \mathbf{B}) \tag{2.38}$$

where the **trace** of a square matrix $\mathbf{C}$ is given as the sum of the diagonal elements. That is,

$$\mathrm{Tr}(C) = \sum_{i=0}^{n-1} C[i,i] \tag{2.39}$$

Example 2.7: Inner product in $\mathbb{C}^{n\times n}$

$\mathbb{C}^{n\times n}$ has an inner product given for matrices $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{n\times n}$ as

$$\langle \mathbf{A}, \mathbf{B} \rangle = \mathrm{Tr}(\mathbf{A}^\dagger \times \mathbf{B}) \tag{2.40}$$

Definition 2.10 (Norm). *Norm is a unary function derived from inner product*

$$|\cdot| : \mathbb{V} \to \mathbb{R} \tag{2.41}$$

defined as $|\boldsymbol{v}| = \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}$*, which has the following properties*

- *Norm is nondegenerate:*
$$|\boldsymbol{v}| > 0 \text{ if } \boldsymbol{v} \neq \mathbf{0} \text{ and } |\mathbf{0}| = 0 \tag{2.42}$$
- *Norm satisfies the triangular inequality:*
$$|\boldsymbol{v} + \boldsymbol{w}| \leq |\boldsymbol{v}| + |\boldsymbol{w}| \tag{2.43}$$
- *Norm respects scalar multiplication:*
$$|c \cdot \boldsymbol{v}| = |c| \cdot |\boldsymbol{v}| \tag{2.44}$$

Definition 2.11 (Distance). *Distance is a binary function defined based on norm*

$$d(\cdot,\cdot) : \mathbb{V} \times \mathbb{V} \to \mathbb{R} \tag{2.45}$$

defined as $d(\boldsymbol{v}_1, \boldsymbol{v}_2) = |\boldsymbol{v}_1 - \boldsymbol{v}_2| = \sqrt{\langle \boldsymbol{v}_1 - \boldsymbol{v}_2, \boldsymbol{v}_1 - \boldsymbol{v}_2 \rangle}$*, which has the following properties*

- *Distance is nondegenerate:*

$$d(\boldsymbol{v}, \boldsymbol{w}) > 0 \text{ if } \boldsymbol{v} \neq \boldsymbol{w} \text{ and } d(\boldsymbol{v}, \boldsymbol{w}) = 0 \iff \boldsymbol{v} = \boldsymbol{w} \tag{2.46}$$

- *Distance satisfies the triangular inequality:*

$$d(\boldsymbol{u}, \boldsymbol{v}) \leq d(\boldsymbol{u}, \boldsymbol{w}) + d(\boldsymbol{w}, \boldsymbol{v}) \tag{2.47}$$

- *Distance is symmetric:*

$$d(\boldsymbol{u}, \boldsymbol{v}) = d(\boldsymbol{v}, \boldsymbol{u}) \tag{2.48}$$

Definition 2.12 (Orthonormal Basis). *A basis* $\mathcal{B} = \{\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{n-1}\}$ *for an inner space*

$$\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \tag{2.49}$$

with the following property

- *For* $\forall \boldsymbol{v} \in \mathbb{V}$ *and any orthonormal basis* $\{\boldsymbol{e}_i\}_{i=0}^{n-1}$ *we have*

$$\boldsymbol{v} = \sum_{i=0}^{n-1} \langle \boldsymbol{e}_i, \boldsymbol{v} \rangle \boldsymbol{e}_i \tag{2.50}$$

Note: inner product defines geometry in the vector space (Figure 2.3).

2.3.2 Hilbert Space

Definition 2.13 (Cauchy Sequence). *Within an inner product space* $\mathbb{V}$*,* $\langle \cdot, \cdot \rangle$ *(with the derived norm and a distance function), a sequence of vectors* $\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots$ *is called a Cauchy sequence if* $\forall \epsilon > 0$*, there exists an* $N_0 \in \mathbb{N}$ *such that for all* $m, n \geq N_0, d(\boldsymbol{v}_m, \boldsymbol{v}_n) \leq \epsilon$*.*

Definition 2.14 (Complete). *For any Cauchy sequence* $\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots$*, it is complete if there exist a* $\overline{\boldsymbol{v}} \in \mathbb{V}$*, such that* $\lim_{n \to \infty} d(\boldsymbol{v}_n - \overline{\boldsymbol{v}}) = 0$*.*

Definition 2.15 (Hilbert Space). *A Hilbert space is a complex inner space that is complete.*

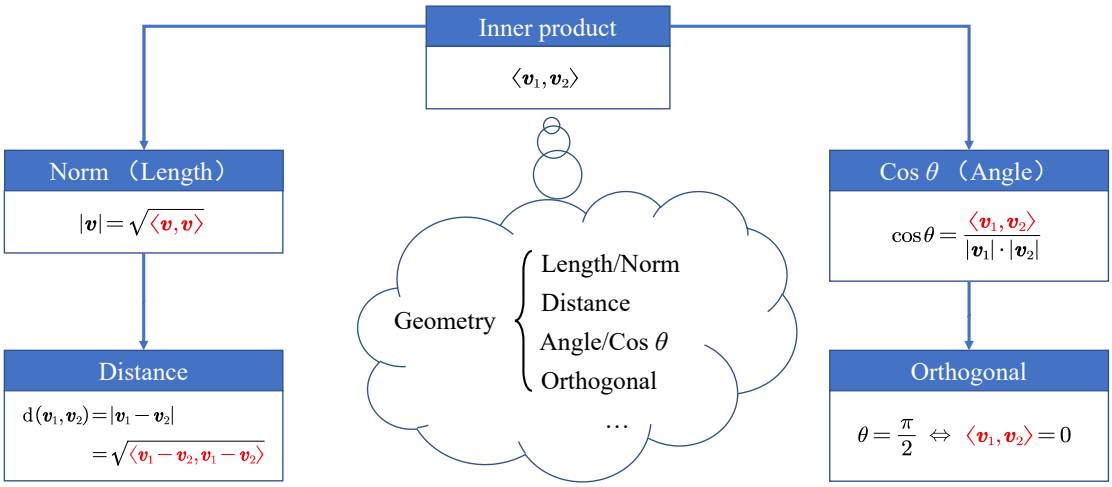


Figure 2.3: Inner product lays the geometric foundation in the vector space.

2.4 Eigenvalue and Eigenvector

Definition 2.16 (Eigenvalue and Eigenvector). *For a matrix* $\mathbf{A} \in \mathbb{C}^{n\times n}$*, if there is a number* $c \in \mathbb{C}$ *and a vector* $0 \neq \boldsymbol{v} \in \mathbb{C}^n$ *such that*

$$\mathbf{A}\boldsymbol{v} = c \cdot \boldsymbol{v} \tag{2.51}$$

then c *is called an eigenvalue of* $\mathbf{A}$ *and* $\boldsymbol{v}$ *is called an eigenvector of* $\mathbf{A}$ *associate with* c*.*

2.5 Hermitian and Unitary Matrices

2.5.1 Hermitian Matrix

Definition 2.17 (Hermitian). *An n-by-n matrix* $\mathbf{A}$ *is called hermitian if* $\mathbf{A}^\dagger = \mathbf{A}$*. In other words,* $A[j,k] = \overline{A[k,j]}$*.*

Definition 2.18 (Self-adjoint). *If* $\mathbf{A}$ *is a hermitian matrix then the operator that it represents is called self-adjoint.*

Proposition 2. *if* $\mathbf{A} \in \mathbb{C}^{n\times n}$ *is Hermitian,* $\forall \boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$ *we have*

$$\langle \mathbf{A}\boldsymbol{v}, \boldsymbol{w} \rangle = \langle \boldsymbol{v}, \mathbf{A}\boldsymbol{w} \rangle \tag{2.52}$$

Proof.

$$\begin{aligned}
\langle \mathbf{A}\boldsymbol{v}, \boldsymbol{w}\rangle &= (\mathbf{A}\boldsymbol{v})^\dagger \times \boldsymbol{w} && \% \text{ definition of inner product} && (2.53)\\
&= \boldsymbol{v}^\dagger \times \mathbf{A}^\dagger \times \boldsymbol{w} && \% \text{ multiplication relates to the adjoint} && (2.54)\\
&= \boldsymbol{v}^\dagger \times \mathbf{A} \times \boldsymbol{w} && \% \text{ definition of Hermitian matrices} && (2.55)\\
&= \boldsymbol{v}^\dagger \times (\mathbf{A}\boldsymbol{w}) && \% \text{ multiplication is associative} && (2.56)\\
&= \langle \boldsymbol{v}, \mathbf{A}\boldsymbol{w}\rangle && \% \text{ definition of inner product} && (2.57)
\end{aligned}$$

□

Proposition 3. *For a Hermitian matrix, its all eigenvalues are real.*

Proof. Let $\mathbf{A} \in \mathbb{C}^{n\times n}$ be a Hermitian matrix with an eigenvalue $c \in \mathbb{C}$ and an eigenvector $\boldsymbol{v} \in \mathbb{C}^n$

$$\begin{aligned}
c\langle \boldsymbol{v}, \boldsymbol{v}\rangle &= \langle \boldsymbol{v}, c\boldsymbol{v}\rangle && \% \text{ inner product respects scalar multiplication} && (2.58)\\
&= \langle \boldsymbol{v}, \mathbf{A}\boldsymbol{v}\rangle && \% \text{ definition of eigenvalue and eigenvector} && (2.59)\\
&= \langle \mathbf{A}\boldsymbol{v}, \boldsymbol{v}\rangle && \% \text{ see Proposition 2} && (2.60)\\
&= \langle c\boldsymbol{v}, \boldsymbol{v}\rangle && \% \text{ definition of eigenvalue and eigenvector} && (2.61)\\
&= \bar{c}\langle \boldsymbol{v}, \boldsymbol{v}\rangle && \% \text{ inner product respects scalar multiplication} && (2.62)\\
& && && (2.63)
\end{aligned}$$

□

Proposition 4. *For a Hermitian matrix, distinct eigenvectors that have distinct eigenvalues are orthogonal*

Proof. Let $\mathbf{A} \in \mathbb{C}^{n\times n}$ be a Hermitian matrix with two distinct eigenvectors $\boldsymbol{v}_1 \neq \boldsymbol{v}_2 \in \mathbb{C}^n$ and their related eigenvalues $c_1, c_2 \in \mathbb{C}$

$$\begin{aligned}
c_2\langle \boldsymbol{v}_1, \boldsymbol{v}_2\rangle &= \langle \boldsymbol{v}_1, c_2\boldsymbol{v}_2\rangle && \% \text{ inner product respects scalar multiplication} && (2.64)\\
&= \langle \boldsymbol{v}_1, \mathbf{A}\boldsymbol{v}_2\rangle && \% \text{ definition of eigenvalue and eigenvector} && (2.65)\\
&= \langle \mathbf{A}\boldsymbol{v}_1, \boldsymbol{v}_2\rangle && \% \text{ see Proposition 2} && (2.66)\\
&= \langle c_1\boldsymbol{v}_1, \boldsymbol{v}_2\rangle && \% \text{ definition of eigenvalue and eigenvector} && (2.67)\\
&= \overline{c_1}\langle \boldsymbol{v}_1, \boldsymbol{v}_2\rangle && \% \text{ inner product respects scalar multiplication} && (2.68)\\
&= c_1\langle \boldsymbol{v}_1, \boldsymbol{v}_2\rangle && \% \text{ see proposition 3} && (2.69)
\end{aligned}$$

□

Proposition 5 (The Spectral Theorem for Finite-Dimensional Self-Adjoint Operators.)**.** *Every self-adjoint operator* $\mathbf{A}$ *on a finite-dimensional complex vector space* $\mathbb{V}$ *can be represented by a diagonal matrix whose diagonal entries are the eigenvalues of* $\mathbf{A}$*, and whose eigenvectors form an orthonormal basis for* $\mathbb{V}$ *(we shall call this basis an eigenbasis).*

Physical Meaning of Hermitian Matrix. Hermitian matrices and their eigenbases will play a major role in our story. We shall see in the following lectures that associated with every physical observable of a quantum system there is a corresponding Hermitian matrix. Measurements of that observable always lead to a state that is represented by one of the eigenvectors of the associated Hermitian matrix.

2.5.2 Unitary Matrix

Definition 2.19 (Unitary). *Given a reversible matrix* $\mathbf{U} \in \mathbb{C}^{n\times n}$ *such that*

$$\mathbf{U} \times \mathbf{U}^\dagger = \mathbf{U}^\dagger \times \mathbf{U} = \mathbf{I}_n \tag{2.70}$$

then $\mathbf{U}$ *is a unitary matrix.*

Example 2.8: Unitary Matrices

$$\mathbf{U}_1 = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ for any } \theta. \qquad \mathbf{U}_2 = \begin{bmatrix} \frac{1+i}{2} & \frac{i}{\sqrt{3}} & \frac{3+i}{2\sqrt{15}} \\ \frac{-1}{2} & \frac{1}{\sqrt{3}} & \frac{4+3i}{2\sqrt{15}} \\ \frac{1}{2} & \frac{-i}{\sqrt{3}} & \frac{5i}{2\sqrt{15}} \end{bmatrix}$$

Proposition 6 (Unitary Matrices Preserve Inner Products). *If* $\mathbf{U} \in \mathbb{C}^{n\times n}$ *is unitary,* $\forall \boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$ *we have*

$$\langle \mathbf{U}\boldsymbol{v}, \mathbf{U}\boldsymbol{w} \rangle = \langle \boldsymbol{v}, \boldsymbol{w} \rangle \tag{2.71}$$

Proof. Let $\mathbf{A} \in \mathbb{C}^{n\times n}$ be a Hermitian matrix with two distinct eigenvectors $\boldsymbol{v}_1 \neq \boldsymbol{v}_2 \in \mathbb{C}^n$ and their related eigenvalues $c_1, c_2 \in \mathbb{C}$

$$\begin{aligned} \langle \mathbf{U}\boldsymbol{v}, \mathbf{U}\boldsymbol{w} \rangle &= (\mathbf{U}\boldsymbol{v})^\dagger \times (\mathbf{U}\boldsymbol{w}) && \text{\% definition for inner product} && (2.72)\\ &= \boldsymbol{v}^\dagger \mathbf{U}^\dagger \times \mathbf{U}\boldsymbol{w} && \text{\% multiplication relates to adjoint} && (2.73)\\ &= \boldsymbol{v}^\dagger \times \mathbf{I} \times \boldsymbol{w} && \text{\% definition for unitary matrices} && (2.74)\\ &= \langle \boldsymbol{v}, \boldsymbol{w} \rangle && \text{\% definition for inner product} && (2.75) \end{aligned}$$

□

Proposition 7 (Unitary Matrices Preserve Norm). *If* $\mathbf{U} \in \mathbb{C}^{n\times n}$ *is unitary,* $\forall \boldsymbol{v}, \in \mathbb{C}^n$ *we have*

$$|\mathbf{U}\boldsymbol{v}| = |\boldsymbol{v}| \tag{2.76}$$

Proof. Let $\mathbf{A} \in \mathbb{C}^{n\times n}$ be a Hermitian matrix with two distinct eigenvectors $\boldsymbol{v}_1 \neq \boldsymbol{v}_2 \in \mathbb{C}^n$ and their related eigenvalues $c_1, c_2 \in \mathbb{C}$

$$
\begin{aligned}
|\mathbf{U}\boldsymbol{v}| &= \sqrt{\langle \mathbf{U}\boldsymbol{v}, \langle \mathbf{U}\boldsymbol{v}\rangle} && \text{\% definition for norm} && (2.77)\\
&= \sqrt{\langle \boldsymbol{v}, \boldsymbol{v}\rangle} && \text{\% unitary matrices preserve inner product} && (2.78)\\
&= |\boldsymbol{v}| && \text{\% definition for norm} && (2.79)\\
& && && (2.80)
\end{aligned}
$$

□

Proposition 8 (Unitary Matrices Preserve Distance)**.** *If* $\mathbf{U} \in \mathbb{C}^{n\times n}$ *is unitary,* $\forall \boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$ *we have*

$$d(\mathbf{U}\boldsymbol{v}, \mathbf{U}\boldsymbol{w}) = d(\boldsymbol{v}, \boldsymbol{w}) \tag{2.81}$$

Proof.

$$
\begin{aligned}
d(\mathbf{U}\boldsymbol{v}, \mathbf{U}\boldsymbol{w}) &= |\mathbf{U}\boldsymbol{v} - \mathbf{U}\boldsymbol{w}| && \text{\% definition for distance} && (2.82)\\
&= |\mathbf{U}(\boldsymbol{v} - \boldsymbol{w})| && \text{\% multiplication distributes over addition} && (2.83)\\
&= |\boldsymbol{v} - \boldsymbol{w}| && \text{\% unitary matrices preserve norm} && (2.84)\\
&= d(\boldsymbol{v}, \boldsymbol{w}) && \text{\% definition of distance} && (2.85)
\end{aligned}
$$

□

Proposition 9. *The modulus of eigenvalues of unitary matrix is* 1.

Proposition 10. *Unitary matrix is the transition matrix from an orthonormal basis to another orthonormal basis.*

Physical meaning of unitary Matrix. What does unitary really mean? As we saw, it means that it preserves the geometry. But it also means something else: If $\mathbf{U}$ is unitary and $\mathbf{UV} = \mathbf{V}'$, then we can easily form $\mathbf{U}^\dagger$ and multiply both sides of the equation by $\mathbf{U}^\dagger$ to get $\mathbf{U}^\dagger\mathbf{UV} = \mathbf{U}^\dagger\mathbf{V}'$ or $\mathbf{V} = \mathbf{U}^\dagger\mathbf{V}'$. In other words, because $\mathbf{U}$ is unitary, there is a related matrix that can undo the action that $\mathbf{U}$ performs. $\mathbf{U}^\dagger$ takes the result of $\mathbf{U}$'s action and gets back the original vector. In the quantum world, all actions (that are not measurements) are undoable or reversible in such a manner.

The roles of Hermitian and unitary matrices in quantum computing. As shown in Figure 2.4, the Hermitian matrix plays an important role in the quantum measurement phrase, which decides the concrete basis to observe the final computational result $|\psi^*\rangle$. Once the basis ($\mathbf{H}_1$ or $\mathbf{H}_2$) is decided, the observation result must be probabilistically collapsed into one of the eigenvectors of the corresponding basis. The unitary matrix plays a role of action to change the state of the quantum computer. Considering its reversible property, all actions performed in quantum computing can be undone by performing an action described by $\mathbf{U}^\dagger$. The relations of identity, Hermitian, unitary, and square matrices are shown in Figure 2.5.

Instructor: Chao Liang

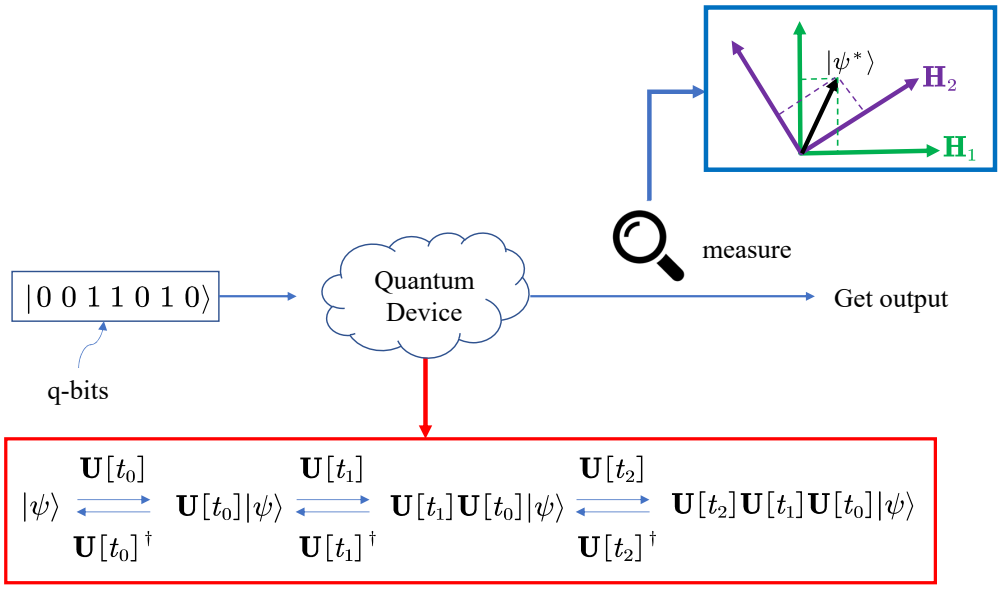


Figure 2.4: The role of Hermitian and unitary matrices.

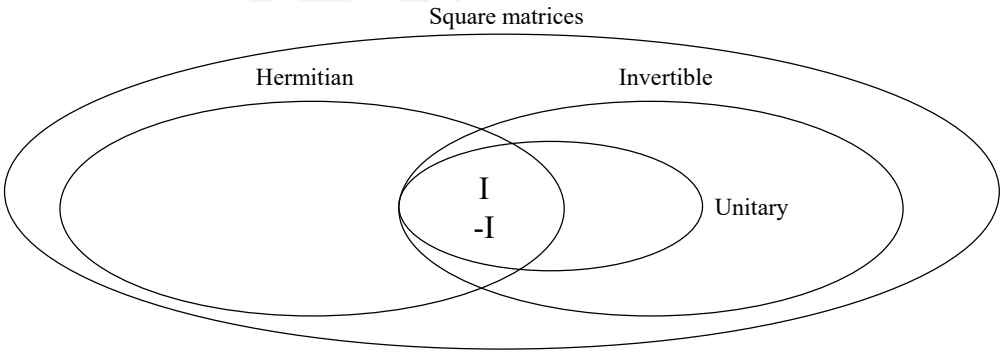


Figure 2.5: Types of matrices.