Quantum Computing

Chao Liang

School of Computer Science
Wuhan University

Review: Lecture 1

- Introduction to Quantum Computing
  - Superposition
  - Quantum Computer vs. Classic Computer
- Complex Number
- The Algebra Property
  - Ordered pair representation
  - Modulus
  - conjugate
- The Geometry Property
  - Benefits of polar representation

Lecture 2: Complex Vector Space

1

Complex vector space

- Complex vector space
- Transpose, conjugate, adjoint
- Matrix multiplication
- Linear map

2

Basis and Dimension

- Linear combination
- Linear independent
- Basis and dimension
- Transition matrix
- Change of basis

3

Inner Product and Hilbert Space

- Inner product, norm and distance
- Orthonormal basis
- Cauchy sequence, complete and Hilbert space

4

Eigenvalue and Eigenvector

- Definition

5

Hermitian and Unitary Matrices

- Hermitian matrix, properties and physical meaning
- Unitary matrix, properties and physical meaning
- Types of matrices

1. Complex Vector Space

- Definitions: three operations
  - Addition(+): $\mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{V}$
  - Negation(-): $\mathbb{V} \longrightarrow \mathbb{V}$
  - Scalar multiplication(·): $\mathbb{C} \times \mathbb{V} \longrightarrow \mathbb{V}$
- Definition: zero
  - Zero vector: $\boldsymbol{0} \in \mathbb{V}$

If these operations and zero satisfy the properties:

（感谢弘毅学堂 2020 级董弘禹同学指出零向量未加粗错误）

1. Complex Vector Space

- Definition: complex vector space $\mathbb{V}$

  $\forall \boldsymbol{v},\ \boldsymbol{w},\ \boldsymbol{x} \in \mathbb{V}$ and $\forall c,\ c_1,\ c_2 \in \mathbb{C}$,

  - Commutativity: $\boldsymbol{v}+\boldsymbol{w}=\boldsymbol{w}+\boldsymbol{v}$
  - Associativity: $(\boldsymbol{v}+\boldsymbol{w})+\boldsymbol{x}=\boldsymbol{v}+(\boldsymbol{w}+\boldsymbol{x})$
  - Additive identity: $\boldsymbol{v}+\boldsymbol{0}=\boldsymbol{v}=\boldsymbol{0}+\boldsymbol{v}$
  - Additive inverse: $\boldsymbol{v}+(-\boldsymbol{v})=\boldsymbol{0}=(-\boldsymbol{v})+\boldsymbol{v}$
  - Multiplication identity: $1 \cdot \boldsymbol{v}=\boldsymbol{v}$
  - Distributive properties: $\begin{cases} c \cdot (\boldsymbol{v}+\boldsymbol{w}) = c \cdot \boldsymbol{v} + c \cdot \boldsymbol{w} \\ (c_1+c_2) \cdot \boldsymbol{v} = c_1 \cdot \boldsymbol{v} + c_2 \cdot \boldsymbol{v} \end{cases}$

（感谢弘毅学堂 2020 级董弘禹同学指出零向量未加粗错误）

1. Complex Vector Space

- Examples

Example 2.2.1 $\mathbb{C}^n$, the set of vectors of length n with complex entries, is a complex vector space that serves as our primary example for the rest of the book. In Section 2.1, we exhibited the operations and described the properties that are satisfied. □

Example 2.2.4 $\mathbb{C}^{m\times n}$, the set of all m-by-n matrices (two-dimensional arrays) with complex entries, is a complex vector space. □

1. Complex Vector Space

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

    $$\mathbf{A}^T \in \mathbb{C}^{n \times m} \text{ such that } \mathbf{A}^T(j,k) = \mathbf{A}(k,j)$$

  - Conjugate

    $$\overline{\mathbf{A}} \in \mathbb{C}^{m \times n} \text{ such that } \overline{\mathbf{A}}(j,k) = \overline{\mathbf{A}(j,k)}$$

  - Adjoint (dagger)

    $$\mathbf{A}^\dagger \in \mathbb{C}^{n \times m} \text{ such that } \mathbf{A}^\dagger(j,k) = \overline{\mathbf{A}(k,j)}$$

1. Complex Vector Space

- Properties of transpose

  $\forall c \in \mathbb{C} \ \text{and} \ \forall \mathbf{A}, \mathbf{B} \in \mathbb{C}^{m \times n}$

  - Transpose is idempotent: $(\mathbf{A}^T)^T = \mathbf{A}$
  - Transpose respects addition: $(\mathbf{A} + \mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$
  - Transpose respects scalar multiplication: $(c \cdot \mathbf{A})^T = c \cdot \mathbf{A}^T$

1. Complex Vector Space

- Properties of conjugate

  $\forall c \in \mathbb{C} \text{ and } \forall \mathbf{A}, \mathbf{B} \in \mathbb{C}^{m \times n}$

  - Conjugate is idempotent: $\overline{\overline{\mathbf{A}}} = \mathbf{A}$
  - Conjugate respects addition: $\overline{\mathbf{A} + \mathbf{B}} = \overline{\mathbf{A}} + \overline{\mathbf{B}}$
  - Conjugate respects scalar multiplication: $\overline{c \cdot \mathbf{A}} = \bar{c} \cdot \overline{\mathbf{A}}$

1. Complex Vector Space

- Properties of adjoint

$$\forall c \in \mathbb{C} \ \text{and} \ \ \forall \mathbf{A}, \mathbf{B} \in \mathbb{C}^{m \times n}$$

  - Adjoint is idempotent: $(\mathbf{A}^{\dagger})^{\dagger} = \mathbf{A}$
  - Adjoint respects addition: $(\mathbf{A} + \mathbf{B})^{\dagger} = \mathbf{A}^{\dagger} + \mathbf{B}^{\dagger}$
  - Adjoint respects scalar multiplication:

$$(c \cdot \mathbf{A})^{\dagger} = \overline{c} \cdot \mathbf{A}^{\dagger}$$

1. Complex Vector Space

- Selected properties for matrix multiplication

  $\forall \mathbf{A} \in \mathbb{C}^{m \times n},\ \mathbf{B} \in \mathbb{C}^{n \times p},\ \mathbf{C} \in \mathbb{C}^{n \times p},\ \mathbf{D} \in \mathbb{C}^{p \times q}$

  - Matrix multiplication distributes over addition:

$$\mathbf{A} * (\mathbf{B} + \mathbf{C}) = (\mathbf{A} * \mathbf{B}) + (\mathbf{A} * \mathbf{C})$$

$$(\mathbf{B} + \mathbf{C}) * \mathbf{D} = (\mathbf{B} * \mathbf{D}) + (\mathbf{C} * \mathbf{D})$$

  - Matrix multiplication respects scalar multiplication:

$$c \cdot (\mathbf{A} * \mathbf{B}) = (c \cdot \mathbf{A}) * \mathbf{B} = \mathbf{A} * (c \cdot \mathbf{B})$$

（感谢弘毅学堂2020级汪昊楠同学指正此页关于矩阵乘法维度不匹配的错误）

1. Complex Vector Space

- Selected properties for matrix multiplication

  $\forall \mathbf{A} \in \mathbb{C}^{m \times n}, \ \mathbf{B} \in \mathbb{C}^{n \times p}$

  - Matrix multiplication relates to the transpose:

    $$(\mathbf{A} * \mathbf{B})^T = \mathbf{B}^T * \mathbf{A}^T$$

  - Matrix multiplication respects to the conjugate:

    $$\overline{\mathbf{A} * \mathbf{B}} = \overline{\mathbf{A}} * \overline{\mathbf{B}}$$

  - Matrix multiplication relates to the adjoint:

    $$(\mathbf{A} * \mathbf{B})^\dagger = \mathbf{B}^\dagger * \mathbf{A}^\dagger$$

（感谢弘毅学堂2020级汪昊楠同学指正此页关于矩阵乘法维度不匹配的错误）

1. Complex Vector Space

- The physical explanation of matrix * vector
  - Matrix * vector --> Action * state

Let A be any element in $\mathbb{C}^{n\times n}$. Then for any element $B \in \mathbb{C}^n$, we have that $A \star B$ is in $\mathbb{C}^n$. In other words, multiplication by A gives one a function from $\mathbb{C}^n$ to $\mathbb{C}^n$. From Equations (2.39) and (2.41), we see that this function preserves addition and scalar multiplication. We will write this map as $A : \mathbb{C}^n \longrightarrow \mathbb{C}^n$.

Let us look ahead for a moment and see what relevance this abstract mathematics has for quantum computing. Just as $\mathbb{C}^n$ has a major role, the complex algebra $\mathbb{C}^{n\times n}$ shall also be in our cast of characters. The elements of $\mathbb{C}^n$ are the ways of describing the states of a quantum system. Some suitable elements of $\mathbb{C}^{n\times n}$ will correspond to the changes that occur to the states of a quantum system. Given a state $X \in \mathbb{C}^n$ and a matrix $A \in \mathbb{C}^{n\times n}$, we shall form another state of the system $A \star X$ which is an element of $\mathbb{C}^n$.[4] Formally, $\star$ in this case is a function $\star : \mathbb{C}^{n\times n} \times \mathbb{C}^n \longrightarrow \mathbb{C}^n$. We say that the algebra of matrices "**acts**" on the vectors to yield new vectors. We shall see this **action** again and again in the following chapters.

1. Complex Vector Space

- Definition: linear map
  - A linear map from $\mathbb{V}$ to $\mathbb{V}'$ is a function

$$f: \mathbb{V} \longrightarrow \mathbb{V}', \ \forall \boldsymbol{v}, \boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{V}, \text{ and } c \in \mathbb{C}$$

    - f respects the addition:

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

    - f respects the scalar multiplication:

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

1. Complex Vector Space

- The physical explanation of linear map

Almost all the maps that we shall deal with in this text are linear maps. We have already seen that when a matrix acts on a vector space, it is a linear map. We shall call any linear map from a complex vector space to itself an **operator**. If $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ is an operator on $\mathbb{C}^n$ and A is an n-by-n matrix such that for all V we have $F(V) = A \star V$, then we say that F is **represented** by A. Several different matrices might represent the same operator

2. Basis and Dimension

- Definition: linear combination

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

where $\boldsymbol{v},\ \boldsymbol{v}_0,\ \boldsymbol{v}_1,\ \cdots,\ \boldsymbol{v}_{n-1} \in \mathbb{V}$

and $c_0,\ c_1,\ \cdots,\ c_{n-1} \in \mathbb{C}$

（感谢人工智能专业2022级张烨同学指出标量c_0，c_1，c_{n-1}不应该加粗的错误）

2. Basis and Dimension

- Definition: linearly independent

  A set $\{\boldsymbol{v}_i | \boldsymbol{v}_i \in \mathbb{V}\}_{i=0}^{n-1}$ is called linearly independent *if*

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

  $$\Leftrightarrow c_0 = c_1 = \cdots = c_{n-1} = 0$$

  - Corollary (推论，try to prove)
    - For any $\boldsymbol{v}_i|_{i=0,1,\cdots,n-1}$, cannot be written as a combination of the others $\{\boldsymbol{v}_j\}_{j=0,j\neq i}^{n-1}$
    - For any $\boldsymbol{0} \neq \boldsymbol{v} \in \mathbb{V}$, unique coefficients $\{c_i\}_{i=0}^{n-1}$

（感谢弘毅学堂 2020 级王骏峣同学指出$\boldsymbol{v}_i$公式下标粗体错误）

（感谢弘毅学堂 2020 级董弘禹同学指出零向量未加粗错误）

2. Basis and Dimension

- Definition: basis

  A set $\{\boldsymbol{v}_i|\boldsymbol{v}_i \in \mathbb{V}\}_{i=0}^{n-1}$ is called a basis of a vector space $\mathbb{V}$ *if*

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

- Canonical/standard basis

  - A basis that is easier to work with

2. Basis and Dimension

- Examples
  - $\mathbb{R}^3$:

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}. \tag{2.72}$$

  - $\mathbb{C}^n$ (and $\mathbb{R}^n$):

$$E_0 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad E_1 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, E_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \end{bmatrix}, \ldots, E_{n-1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}. \tag{2.73}$$

Every vector $[c_0, c_1, \ldots, c_{n-1}]^T$ can be written as

$$\sum_{j=0}^{n-1} (c_j \cdot E_j). \tag{2.74}$$

2. Basis and Dimension

- Examples
  - $\mathbb{C}^{m\times n}$: The canonical basis for this vector space consists of matrices of the form

$$E_{j,k} = \begin{array}{c} \\ \mathbf{0} \\ \mathbf{1} \\ \vdots \\ \boldsymbol{j} \\ \vdots \\ \boldsymbol{m-1} \end{array} \begin{array}{c} \begin{array}{cccccc} \mathbf{0} & \mathbf{1} & \cdots & \boldsymbol{k} & \cdots & \boldsymbol{n-1} \end{array} \\ \begin{bmatrix} 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{bmatrix} \end{array}, \tag{2.75}$$

where $E_{j,k}$ has a 1 in row j, column k, and 0's everywhere else. There is an $E_{j,k}$ for $j = 0, 1, \ldots, m-1$ and $k = 0, 1, \ldots, n-1$. It is not hard to see that for every m-by-n matrix, A can be written as the sum:

$$A = \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} A[j,k] \cdot E_{j,k}. \tag{2.76}$$

2. Basis and Dimension

- Definition: dimension
  - The dimension of a (complex) vector space is the number of elements in a basis of the vector space

    - $\mathbb{R}^3$, as a real vector space, is of dimension 3.
    - In general, $\mathbb{R}^n$ has dimension n as a real vector space.
    - $\mathbb{C}^n$ has dimension n as a complex vector space.
    - $\mathbb{C}^n$ is of dimension $2n$ as a real vector space because every complex number is described by two real numbers.
    - $Poly_n$ is isomorphic to $\mathbb{C}^{n+1}$; it is not hard to see that the dimension of $Poly_n$ is also $n+1$.
    - $\mathbb{C}^{m\times n}$: the dimension is mn as a complex vector space.

2. Basis and Dimension

- Definition: transition matrix
  - A transition matrix from basis $\mathfrak{B}$ to basis $\mathfrak{D}$ is a matrix $\mathbf{M}_{\mathfrak{D} \leftarrow \mathfrak{B}}$ such that their coefficients satisfy

$$\boldsymbol{v}_{\mathfrak{D}} = \mathbf{M}_{\mathfrak{D} \leftarrow \mathfrak{B}} * \boldsymbol{v}_{\mathfrak{B}}$$

  - Note

In other words, $M_{\mathcal{D} \leftarrow \mathcal{B}}$ is a way of getting the coefficients with respect to one basis from the coefficients with respect to another basis. For the above bases $\mathcal{B}$ and $\mathcal{D}$, the transition matrix is

2. Basis and Dimension

- Utilities of transition matrix
  - Operator re-representation in a new basis

$$\mathbf{A}_{\mathfrak{D}} = \mathbf{M}^{-1}_{\mathfrak{D} \leftarrow \mathfrak{B}} * \mathbf{A}_{\mathfrak{B}} * \mathbf{M}_{\mathfrak{D} \leftarrow \mathfrak{B}}$$

  - State re-representation in a new basis

$$\boldsymbol{v}_{\mathfrak{D}} = \mathbf{M}_{\mathfrak{D} \leftarrow \mathfrak{B}} * \boldsymbol{v}_{\mathfrak{B}}$$

2. Basis and Dimension

- Example: Hadamard matrix

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

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

to this other basis

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

is the **Hadamard matrix**:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix}. \tag{2.95}$$

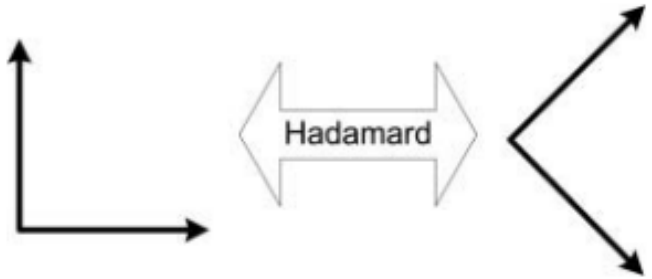


Figure 2.6. The Hadamard matrix as a transition between two bases.

2. Basis and Dimension

- 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 2.7.

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 flow-

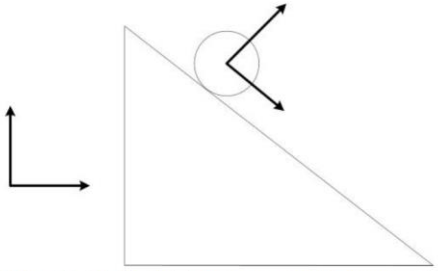


Figure 2.7. A ball rolling down a ramp and the two relevant bases.

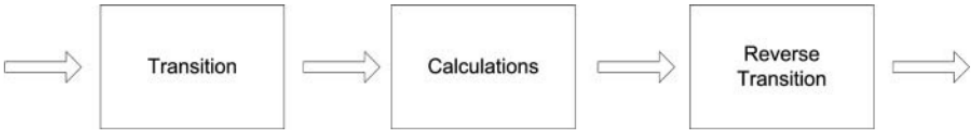


Figure 2.8. Problem-solving flowchart.

3. Inner Product and Hilbert Space

- Definition: inner product
  - A binary function $\langle \cdot,\cdot \rangle : \mathbb{V} \times \mathbb{V} \to \mathbb{C}$ that satisfies:
    - Nondegenerate: $\langle \boldsymbol{v},\boldsymbol{v} \rangle \geqslant 0$ and $\langle \boldsymbol{v},\boldsymbol{v} \rangle = 0 \Leftrightarrow \boldsymbol{v} = \boldsymbol{0}$
    - Respects additions: $\begin{cases} \langle \boldsymbol{v}_1 + \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_3 \rangle + \langle \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle \\ \langle \boldsymbol{v}_1, \boldsymbol{v}_2 + \boldsymbol{v}_3 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle + \langle \boldsymbol{v}_1, \boldsymbol{v}_3 \rangle \end{cases}$
    - Respects multiplication: $\begin{cases} \langle c \cdot \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \overline{c} \times \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle \\ \langle \boldsymbol{v}_1, c \cdot \boldsymbol{v}_2 \rangle = c \times \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle \end{cases}$
    - Skew symmetric: $\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \overline{\langle \boldsymbol{v}_2, \boldsymbol{v}_1 \rangle}$

（感谢弘毅学堂 2019级甘汶曦同学指正此页单词skew的拼写错误）
（感谢弘毅学堂 2018级谈喆灵同学指正此页内积运算相对于标量乘法的公式错误）
（感谢弘毅学堂 2020 级董弘禹同学指出零向量未加粗错误）

3. Inner Product and Hilbert Space

- Definition: inner product
  - A binary function $\langle \cdot,\cdot \rangle : \mathbb{V} \times \mathbb{V} \to \mathbb{C}$ that satisfies:
    - Nondegenerate: $\langle \boldsymbol{v},\boldsymbol{v} \rangle \geqslant 0$ and $\langle \boldsymbol{v},\boldsymbol{v} \rangle = 0 \Leftrightarrow \boldsymbol{v} = \boldsymbol{0}$
    - Respects additions: $\begin{cases} \langle \boldsymbol{v}_1 + \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_3 \rangle + \langle \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle \\ \langle \boldsymbol{v}_1, \boldsymbol{v}_2 + \boldsymbol{v}_3 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle + \langle \boldsymbol{v}_1, \boldsymbol{v}_3 \rangle \end{cases}$
    - Respects multiplication: $\begin{cases} \langle c \cdot \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \overline{c} \times \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle \\ \langle \boldsymbol{v}_1, c \cdot \boldsymbol{v}_2 \rangle = c \times \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle \end{cases}$
    - Skew symmetric: $\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \overline{\langle \boldsymbol{v}_2, \boldsymbol{v}_1 \rangle}$

Conjugate linear in the first slot and linear in the second slot

（感谢弘毅学堂 2019级甘汶曦同学指正此页单词skew的拼写错误）
（感谢弘毅学堂 2018级谈喆灵同学指正此页内积运算相对于标量乘法的公式错误）
（感谢弘毅学堂 2020 级董弘禹同学指出零向量未加粗错误）

Supplementary material

- Why must be skew symmetric rather than symmetric?

因为我们希望一个向量与自身的内积是一个非负**实数**。所以我们就不能直接把内积定义成相对于两个变量都是复线性的，也就是不能定义成 $< \vec{v}, \vec{w} >= \sum v_i w_i$,而是 $< \vec{v}, \vec{w} >= \sum v_i \bar{w}_i$ ，从而相对于v是线性，相对于w是**共轭线性**。所以你交换一下两个变量就应该得到原来的共轭。

与前面公式不一致，但是没关系

至于为什么要求向量与自身的内积是实数？因为我们希望把v,v内积的平方根定义成v的长度（范数），你如果内积是一个复数，取个平方根又得到一个复数，你不清楚“长度是复数”是什么意思。

当然我上面这么说都是在解释为什么要这么定义，而不是去证明这个定义。定义就是定义，它是逻辑推导的出发点，无所谓证明不证明。

《为什么内积在复数向量空间中不具有交换性？》 https://www.zhihu.com/question/60961989

3. Inner Product and Hilbert Space

- Definition: inner product space
  - A vector space with an inner product.
- Examples
  - $\mathbb{R}^n$: The inner product is given as

$$\langle V_1, V_2 \rangle = V_1^T \star V_2. \tag{2.106}$$

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

$$\langle V_1, V_2 \rangle = V_1^\dagger \star V_2. \tag{2.107}$$

3. Inner Product and Hilbert Space

- Examples (cont.)
  - $\mathbb{R}^{n\times n}$ has an inner product given for matrices $A, B \in \mathbb{R}^{n\times n}$ as

$$\langle A, B\rangle = Trace(A^T \star B), \tag{2.108}$$

where the **trace** of a square matrix C is given as the sum of the diagonal elements. That is,

$$Trace(C) = \sum_{i=0}^{n-1} C[i,i]. \tag{2.109}$$

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

$$\langle A, B\rangle = Trace(A^\dagger \star B). \tag{2.110}$$

3. Inner Product and Hilbert Space

- Definition: norm
  - A unary function derived from inner product

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

    defined as $|\boldsymbol{v}| = \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}$

  - Properties
    - Norm is nondegenerate: $|\boldsymbol{v}| > 0$ if $\boldsymbol{v} \neq \boldsymbol{0}$ and $|\boldsymbol{0}| = 0$
    - Norm satisfies the triangular inequality: $|\boldsymbol{v} + \boldsymbol{w}| \leqslant |\boldsymbol{v}| + |\boldsymbol{w}|$
    - Norm respects scalar multiplication: $|c \cdot \boldsymbol{v}| = |c| \times |\boldsymbol{v}|$

（感谢弘毅学堂 2018级王浩冰同学指正此页三角不等式的不等号错误）
（感谢弘毅学堂 2020 级董弘禹同学指出零向量未加粗错误）

3. Inner Product and Hilbert Space

- Definition: distance
  - A binary function defined based on norm

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

    defined as $\mathrm{d}(\boldsymbol{v}_1,\boldsymbol{v}_2) = |\boldsymbol{v}_1 - \boldsymbol{v}_2| = \sqrt{\langle \boldsymbol{v}_1 - \boldsymbol{v}_2, \boldsymbol{v}_1 - \boldsymbol{v}_2 \rangle}$

  - Properties
    - Distance is nondegenerate:

$$\mathrm{d}(\boldsymbol{v},\boldsymbol{w}) > 0 \text{ if } \boldsymbol{v} \neq \boldsymbol{w} \text{ and } \mathrm{d}(\boldsymbol{v},\boldsymbol{w}) = 0 \Leftrightarrow \boldsymbol{v} = \boldsymbol{w}$$

    - Distance satisfies the triangular inequality:

$$\mathrm{d}(\boldsymbol{u},\boldsymbol{v}) \leqslant \mathrm{d}(\boldsymbol{u},\boldsymbol{w}) + \mathrm{d}(\boldsymbol{w},\boldsymbol{v})$$

    - Distance is symmetric: $\mathrm{d}(\boldsymbol{u},\boldsymbol{v}) = \mathrm{d}(\boldsymbol{v},\boldsymbol{u})$

（感谢弘毅学堂 2018级王浩冰同学指正此页nondegenerate公式不完整的错误）

3. Inner Product and Hilbert Space

- Definition: orthonormal basis
  - A basis $\mathfrak{B}=\{\boldsymbol{e}_0,\boldsymbol{e}_1,\cdots,\boldsymbol{e}_{n-1}\}$ for an inner space $\mathbb{V}$ satisfies

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

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

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

(Pay attention to the order!)

补充材料：内积

Inner product

$$\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle$$

Cos θ （夹角）

$$\cos\theta = \frac{\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle}{|\boldsymbol{v}_1| \cdot |\boldsymbol{v}_2|}$$

Orthogonal （正交）

$$\theta = \frac{\pi}{2} \Leftrightarrow \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = 0$$

Norm （长度）

$$|\boldsymbol{v}| = \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}$$

Distance （远近）

$$\mathrm{d}(\boldsymbol{v}_1, \boldsymbol{v}_2) = |\boldsymbol{v}_1 - \boldsymbol{v}_2| = \sqrt{\langle \boldsymbol{v}_1 - \boldsymbol{v}_2, \boldsymbol{v}_1 - \boldsymbol{v}_2 \rangle}$$

几何：长度、距离、角度、正交、…

3. Inner Product and Hilbert Space

- Definition (just a sketch): Cauchy sequence
  - Given a sequence of vectors $\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{v}_2, \cdots$, if for

    $\forall \epsilon > 0, \exists N_0 \in \mathbb{N}$ such that for all $m, n \geqslant N_0,\ \mathrm{d}(\boldsymbol{v}_m, \boldsymbol{v}_n) \leqslant \epsilon$
- Definition (just a sketch): Complete
  - For any Cauchy sequence $\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{v}_2, \cdots$,

    there exist a $\overline{\boldsymbol{v}} \in \mathbb{V}$, such that $\lim_{n \to \infty} \mathrm{d}(\boldsymbol{v}_n - \overline{\boldsymbol{v}}) = 0$
- Definition: Hilbert space
  - A complex inner space that is complete

4. Eigen-values and -vectors

- Definition: 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

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

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

5. Hermitian and Unitary Mat.

- Definition: Hermitian
  - $\mathbf{A} \in \mathbb{C}^{n \times n}$ such that $\mathbf{A}^{\dagger} = \mathbf{A}$

Example 2.6.1 The matrix

$$\begin{bmatrix} 5 & 4+5i & 6-16i \\ 4-5i & 13 & 7 \\ 6+16i & 7 & -2.1 \end{bmatrix}$$

is hermitian.

- Definition: self-adjoint
  - If **A** is a Hermitian matrix then the operator that it represents is call self-adjoint (why called self-adjoint? see proposition 2.6.4)

5. Hermitian and Unitary Mat.

- Proposition 1
  - If $\mathbf{A} \in \mathbb{C}^{n \times n}$ is Hermitian, for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$ we have

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

  - Proof

$$\begin{aligned}
\langle \mathbf{A}\boldsymbol{v}, \boldsymbol{w} \rangle &= (\mathbf{A}\boldsymbol{v})^{\dagger} * \boldsymbol{w} && \% \textit{ definition of inner product} \\
&= \boldsymbol{v}^{\dagger} * \mathbf{A}^{\dagger} * \boldsymbol{w} && \% \textit{ multiplication relates to the adjoint} \\
&= \boldsymbol{v}^{\dagger} * \mathbf{A} * \boldsymbol{w} && \% \textit{ definition of Hermitian matrices} \\
&= \boldsymbol{v}^{\dagger} * (\mathbf{A}\boldsymbol{w}) && \% \textit{ multiplication is associative} \\
&= \langle \boldsymbol{v}, \mathbf{A}\boldsymbol{w} \rangle && \% \textit{ definition of inner product}
\end{aligned}$$

5. Hermitian and Unitary Mat.

- Proposition 2
  - 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 $\boldsymbol{v} \in \mathbb{C}^n$

$$
\begin{aligned}
c\langle \boldsymbol{v}, \boldsymbol{v} \rangle &= \langle \boldsymbol{v}, c\boldsymbol{v} \rangle && \% \textit{ inner product respects scalar multiplication} \\
&= \langle \boldsymbol{v}, \mathbf{A}\boldsymbol{v} \rangle && \% \textit{ definition of eigenvalue and eigenvector} \\
&= \langle \mathbf{A}\boldsymbol{v}, \boldsymbol{v} \rangle && \% \textit{ see last proposition} \\
&= \langle c\boldsymbol{v}, \boldsymbol{v} \rangle && \% \textit{ definition of eigenvalue and eigenvector} \\
&= \overline{c}\,\langle \boldsymbol{v}, \boldsymbol{v} \rangle && \% \textit{ inner product respects scalar multiplication}
\end{aligned}
$$

5. Hermitian and Unitary Mat.

- Proposition 3
  - 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 eigenvalues $c_1 \neq c_2 \in \mathbb{C}$ and their related eigenvectors $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{C}^n$

5. Hermitian and Unitary Mat.

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

$$
\begin{aligned}
c_2 \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle &= \langle \boldsymbol{v}_1, c_2 \boldsymbol{v}_2 \rangle && \% \textit{ inner product respects scalar multiplication} \\
&= \langle \boldsymbol{v}_1, \mathbf{A} \boldsymbol{v}_2 \rangle && \% \textit{ definition of eigenvalue and eigenvector} \\
&= \langle \mathbf{A} \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle && \% \textit{ previous proposition} \\
&= \langle c_1 \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle && \% \textit{ defintion of eignevalue and eigenvector} \\
&= \overline{c}_1 \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle && \% \textit{ inner product respects scalar multiplication} \\
&= c_1 \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle && \% \textit{ last proposition}
\end{aligned}
$$

5. Hermitian and Unitary Mat.

- Proposition 4 (try to prove)

Proposition 2.6.4 (The Spectral Theorem for Finite-Dimensional Self-Adjoint Operators.) Every self-adjoint operator A on a finite-dimensional complex vector space $\mathbb{V}$ can be represented by a diagonal matrix whose diagonal entries are the eigenvalues of A, and whose eigenvectors form an orthonormal basis for $\mathbb{V}$ (we shall call this basis an **eigenbasis**).

$$\mathbf{A} = \sum_{i=1}^{n} \alpha_i |\varphi_i\rangle \langle\varphi_i|$$

- Physical Meaning of Hermitian Matrix

Hermitian matrices and their eigenbases will play a major role in our story. We shall see in Chapter 4 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.

5. Hermitian and Unitary Mat.

- Definition: Unitary
  - Given a reversible matrix $\mathbf{U} \in \mathbb{C}^{n \times n}$ such that

$$\mathbf{U} * \mathbf{U}^{\dagger} = \mathbf{U}^{\dagger} * \mathbf{U} = \mathbf{I}_n$$

- Examples

Example 2.6.2 For any θ, the matrix

$$\begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is a unitary matrix.

Example 2.6.3 The matrix

$$\begin{bmatrix} \frac{1+i}{2} & \frac{i}{\sqrt{3}} & \frac{3+i}{2\sqrt{15}} \\ \frac{-1}{2} & \frac{1}{\sqrt{3}} & \frac{4+3i}{2\sqrt{15}} \\ \frac{1}{2} & \frac{-i}{\sqrt{3}} & \frac{5i}{2\sqrt{15}} \end{bmatrix}$$

is a unitary matrix.

（感谢弘毅学堂2021级胡楷明同学指出本页截图错误）

5. Hermitian and Unitary Mat.

- Proposition 1
  - [Unitary matrices preserve inner products]

    If $\mathbf{U} \in \mathbb{C}^{n \times n}$ is unitary, for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$ we have

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

  - Proof

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

5. Hermitian and Unitary Mat.

- Proposition 2
  - [Unitary matrices preserve norm]

    If $\mathbf{U} \in \mathbb{C}^{n \times n}$ is unitary, for all $\boldsymbol{v} \in \mathbb{C}^n$ we have

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

  - Proof

    $$\begin{aligned} |\mathbf{U}\boldsymbol{v}| &= \sqrt{\langle \mathbf{U}\boldsymbol{v}, \mathbf{U}\boldsymbol{v} \rangle} && \%\ definition\ for\ norm \\ &= \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle} && \%\ unitary\ matrices\ preserve\ inner\ product \\ &= |\boldsymbol{v}| && \%\ definition\ for\ norm \end{aligned}$$

（感谢弘毅学堂 2018级魏瑄同学指正此页证明过程中根号遗漏的错误）

5. Hermitian and Unitary Mat.

- Proposition 3
  - [Unitary matrices preserve distance]

    If $\mathbf{U} \in \mathbb{C}^{n \times n}$ is unitary, for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$ we have

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

  - Proof

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

Supplementary material

- Proposition 4
  - The modulus of eigenvalues of unitary matrix is 1（酉矩阵的特征值的模为1）
- Proposition 5
  - Unitary matrix is the transition matrix from an orthonormal basis to another orthonormal basis （标准正交基到标准正交基的过渡矩阵是酉矩阵）

Source: https://www.youtube.com/watch?v=zQMUmaTxrbw

（感谢人工智能专业 2021级王之宪同学指正此页英文写作的语法错误）

补充材料

- 证明：标准正交基变换矩阵 $\mathbf{M}$ 是正交的
  - 给定两个标准正交基 $\mathbf{U}=[\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_n]$ 和 $\mathbf{V}=[\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n]$
  - 假设基变换矩阵 $\mathbf{M}:\mathbf{U}\to\mathbf{V}$，即 $\mathbf{V}=\mathbf{UM}$
    - 有 $\mathbf{I}=\mathbf{V}^\dagger\mathbf{V}=(\mathbf{UM})^\dagger(\mathbf{UM})$
      $=\mathbf{M}^\dagger\mathbf{U}^\dagger\mathbf{UM}=\mathbf{M}^\dagger\mathbf{IM}=\mathbf{M}^\dagger\mathbf{M}$
    - 即 标准基变换矩阵是正交的（即为酉矩阵）
  - 假设一个向量 $\boldsymbol{s}$ 在 $\mathbf{U}$ 和 $\mathbf{V}$ 下的坐标分别为 $\boldsymbol{x}$ 和 $\boldsymbol{y}$
    - 有 $\boldsymbol{s}=\mathbf{U}\boldsymbol{x}=\mathbf{V}\boldsymbol{y}=\mathbf{UM}\boldsymbol{y}\to\boldsymbol{x}=\mathbf{M}\boldsymbol{y}$

5. Hermitian and Unitary Mat.

- Physical Meaning of Unitary Matrix

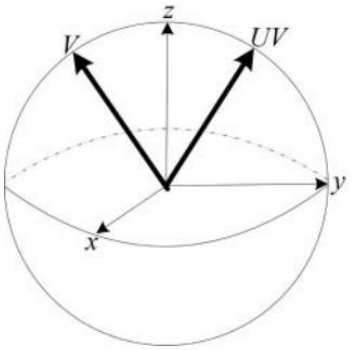
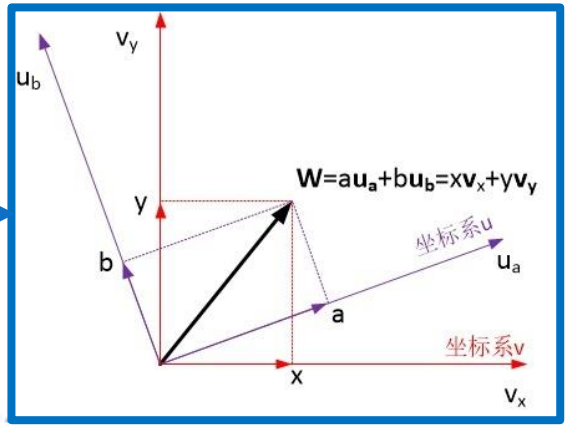


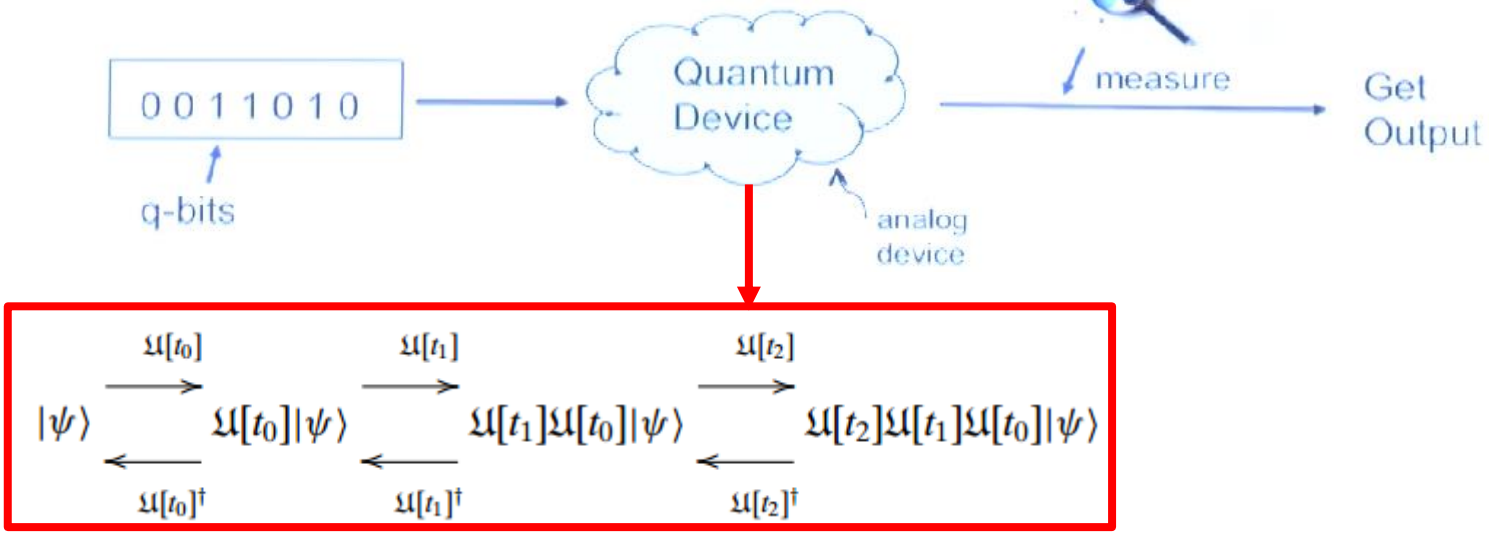
Figure 2.14. The unit sphere and the action of U on V.

What does unitary really mean? As we saw, it means that it preserves the geometry. But it also means something else: If U is unitary and $UV = V'$, then we can easily form $U^\dagger$ and multiply both sides of the equation by $U^\dagger$ to get $U^\dagger UV = U^\dagger V'$ or $V = U^\dagger V'$. In other words, because U is unitary, there is a related matrix that can "undo" the action that U performs. $U^\dagger$ takes the result of 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.

5. Hermitian and Unitary Mat.

- The roles of H and U





5. Hermitian and Unitary Mat.

- Types of Matrices

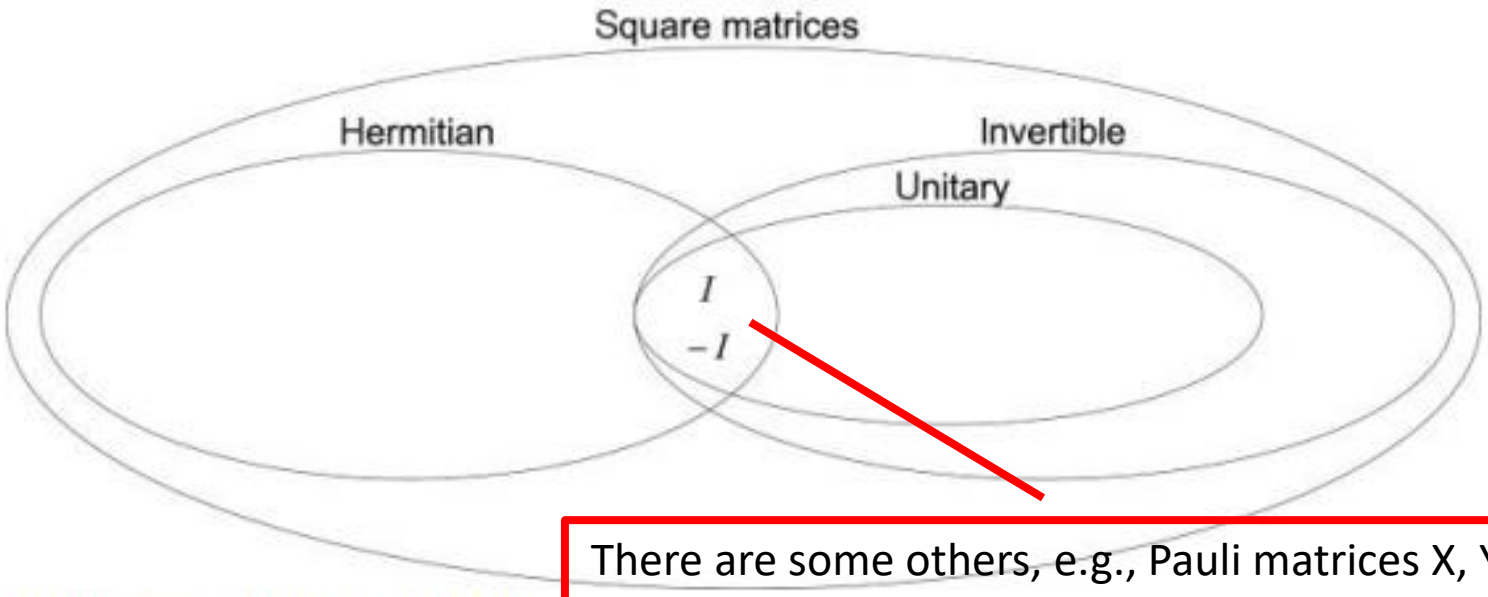


Figure 2.15. Types of matrices.

There are some others, e.g., Pauli matrices X, Y, Z

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Conclusion

1. Complex Vector Space
   - Transpose, conjugate and adjoint
2. Basis and Dimension
   - Change of basis
3. Inner Product and Hilbert Space
   - Inner product, norm and distance
4. Eigenvalues and Eigenvectors
5. Hermitian and Unitary Matrices
   - Properties and physical meanings

Quiz

- 以下这幅图让你想到什么矩阵？为什么？

Quiz

- 以下这幅图让你想到什么矩阵？为什么？