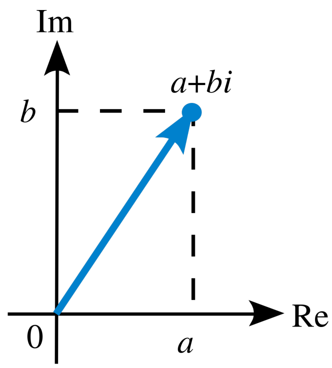
CS333 - Math for Quantum

1 Complex Numbers

A complex number is written as $a + bi$, where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$. It is useful to think about complex numbers as points on a plane:



If $x = a + bi$, then the *complex conjugate* of x, denoted x^*, is $a - bi$. If w and x are complex numbers, then

$$\begin{aligned}(wx)^* &= w^* x^* \\ (w + x)^* &= w^* + x^* \end{aligned} \tag{1}$$

Question: If we think of complex numbers as points on a plane, and conjugation as a function that takes a complex number to its conjugate, how does the operation of conjugation transform points on a plane?

For $w \in \mathbb{R}$, Euler's formula is the following:

$$e^{iw} = \cos(w) + i \sin(w). \tag{2}$$

This formula lets us use a complex exponential to represent complex numbers.

Question: If $w \in \mathbb{R}$, which of the following is the complex conjugate of e^{iw}?

$$e^{-iw}, \qquad \cos(w) - i\sin(w), \qquad -\cos(w) + i\sin(w), \qquad e^{w} \tag{3}$$

If $x = a + bi$, we denote the magnitude of x as $|x|$, where $|x| = \sqrt{xx^*}$.

Question: Explain why $|e^{ix}| = 1$ twice. The first time, use the e^{ix} representation, and the second use the $\cos(x) + i\sin(x)$ representation. Note: $a^0 = 1$ for any non-zero number a. Also, note: $a^b a^c = a^{b+c}$. Finally, note: $\cos^2(a) + \sin^2(a) = 1$ for any real number a.

Question: What is a simpler expression for $e^{i3\pi/2}$, and where does it appear as a point on the plane?

2 Vector Spaces

We will deal with vector spaces $\mathbb{C}^d$. $\mathbb{C}^d$ is the set of column vectors of length d (dimension d) whose elements are complex numbers. So for example

$$\begin{pmatrix} 1 \\ i \\ e^{2i} \end{pmatrix} \in \mathbb{C}^3. \tag{4}$$

If $\mathbf{x} \in \mathbb{C}^d$, then the conjugate transpose of $\mathbf{x}$, denoted by $\mathbf{x}^\dagger$, is the d-dimensional row vector where the jth element of $\mathbf{x}^\dagger$ is the complex conjugate of the jth element of $\mathbf{x}$. For example, if

$$\mathbf{x} = \begin{pmatrix} 1 \\ i \\ e^{2i} \end{pmatrix} \qquad \text{then} \qquad \mathbf{x}^\dagger = \begin{pmatrix} 1, & -i, & e^{-2i} \end{pmatrix}. \tag{5}$$

More generally, if you have a matrix $\mathbf{A}$, then $\mathbf{A}^\dagger$ denotes the conjugate transpose of $\mathbf{A}$, where you take the transpose of the matrix, and then take the complex conjugate of each element. For example

$$\begin{pmatrix} 1, & 2, & 3 \\ -1i, & -2i, & -3i \end{pmatrix}^\dagger = \begin{pmatrix} 1, & 1i \\ 2, & 2i \\ 3, & 3i \end{pmatrix}$$

Given vectors $\mathbf{x}, \mathbf{y} \in \mathbb{C}^d$, we can take the inner product $\mathbf{y}^\dagger\mathbf{x}$ by doing matrix multiplication between $\mathbf{y}^\dagger$ and $\mathbf{x}$. That is: $\mathbf{y}^\dagger\mathbf{x} = \sum_{i=1}^d y_i^* x_i$, where x_i is the ith element of $\mathbf{x}$ and y_i is the

ith element of $\mathbf{y}$. For example, if $\mathbf{x}$ is as above, and $\mathbf{y} = \begin{pmatrix} i \\ 1+i \\ 2 \end{pmatrix}$, then

$$\mathbf{y}^\dagger \mathbf{x} = \begin{pmatrix} -i, & 1-i, & 2 \end{pmatrix} \begin{pmatrix} 1 \\ i \\ e^{2i} \end{pmatrix} = -i \times 1 + (1-i) \times i + 2 \times e^{2i} = -i + i + 1 + 2e^{2i}$$
$$= 1 + e^{2i}. \tag{6}$$

Question: If $\mathbf{x} = \begin{pmatrix} 1 \\ i \end{pmatrix}$ and $\mathbf{y} = \begin{pmatrix} 1 \\ -i \end{pmatrix}$, what is $\mathbf{y}^\dagger \mathbf{x}$? What is $\mathbf{x}^\dagger \mathbf{y}$?

Question: If $\mathbf{x}, \mathbf{y}$ are any vectors in $\mathbb{C}^d$, explain why $\left(\mathbf{y}^\dagger \mathbf{x}\right)^* = \mathbf{x}^\dagger \mathbf{y}$.

Question: Show that the inner product follows the distributive property. That is, if $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{C}^d$, explain why $\mathbf{z}^\dagger (\mathbf{x} + \mathbf{y}) = \mathbf{z}^\dagger \mathbf{x} + \mathbf{z}^\dagger \mathbf{y}$.

A *basis* for a vector space $\mathbb{C}^d$ is a set of vectors $\{\mathbf{v}_1, \ldots \mathbf{v}_d\}$ such that for every vector $\mathbf{x} \in \mathbb{C}^d$, there is a unique set of complex numbers $\{a_1, \ldots, a_d\}$ such that

$$\mathbf{x} = \sum_{j=1}^{d} a_j \mathbf{v}_j. \tag{7}$$

If you have a set of d vectors $\{\mathbf{v}_1, \ldots \mathbf{v}_d\}$ each in $\mathbb{C}^d$ such that

$$\mathbf{v}_j^\dagger \mathbf{v}_k = \begin{cases} 1 & \text{if } j = k \\ 0 & \text{if } j \neq k, \end{cases} \tag{8}$$

then they form a basis for $\mathbb{C}^d$. We call such a basis an *orthonormal basis*. Orthonormal combines the words "orthogonal" which refers to two vectors whose inner product is orthogonal, and "normal" which refers to a vector whose inner product with itself is 1.

For example you can verify that:

$$\mathbf{v}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \qquad \mathbf{v}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \tag{9}$$

from an orthonormal basis for $\mathbb{C}^2$ because there are two of them, and they satisfy Eq. (8). In quantum computing, we will exclusively deal with orthonormal bases.

Given a vector $\mathbf{x} \in \mathbb{C}^d$, it is often helpful to write that vector in terms of a given orthonormal basis $\{\mathbf{v}_1, \dots \mathbf{v}_d\}$. In other words, we would like to find the complex numbers a_j as in Eq. (7). When $\{\mathbf{v}_1, \dots \mathbf{v}_d\}$ is an orthonormal basis, finding this decomposition is fairly straightforward. We can apply $\mathbf{v}_i^\dagger$ to both sides of equation Eq. (7):

$$\begin{aligned}
\mathbf{v}_i^\dagger \mathbf{x} &= \mathbf{v}_i^\dagger \left(\sum_{j=1}^{d} a_j \mathbf{v}_j \right) \\
&= \sum_{j=1}^{d} a_j \mathbf{v}_i^\dagger \mathbf{v}_j \\
&= a_i
\end{aligned} \tag{10}$$

where the second line comes from the distributive property, and the final line comes from Eq. (8).

Question: Consider the orthonormal basis $\{\mathbf{v_1}, \mathbf{v_2}\}$ for $\mathbb{C}^2$ where $\mathbf{v}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\mathbf{v}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Write $\mathbf{x} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$ in this basis. (In other words, write $\mathbf{x} = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2$ for some complex numbers a_1 and a_2.)

Let $\mathbb{C}^{n \times m}$ denote the set of matrices with n rows and m columns and complex elements. Let $\mathbf{A} \in \mathbb{C}^{n \times m}$ and $\mathbf{B} \in \mathbb{C}^{p \times q}$. Then the *tensor product* (technically the Kronecker product) of $\mathbf{A}$ and $\mathbf{B}$ is denoted by $\mathbf{A} \otimes \mathbf{B}$. If the element in the ith row and jth column of $\mathbf{A}$ is A_{ij}, then

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} A_{11}\mathbf{B}, & A_{12}\mathbf{B}, & \dots & A_{1m}\mathbf{B} \\ A_{21}\mathbf{B}, & A_{22}\mathbf{B}, & \dots & A_{2m}\mathbf{B} \\ \vdots & \vdots & \vdots & \vdots \\ A_{n1}\mathbf{B}, & A_{n2}\mathbf{B}, & \dots & A_{nm}\mathbf{B} \end{pmatrix}.$$

For example,

$$\begin{pmatrix} 1, & 2, & 3 \\ -1, & -2, & -3 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix}, & 2 \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix}, & 3 \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix} \\ -1 \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix}, & -2 \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix}, & -3 \begin{pmatrix} 0 \\ 1 \\ i \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & 3 \\ 1i & 2i & 3i \\ 0 & 0 & 0 \\ -1 & -2 & -3 \\ -1i & -2i & -3i \end{pmatrix}.$$

Question: If $\mathbf{A}$ is an $n \times m$ matrix and $\mathbf{B}$ is a $p \times q$ matrix, what are the dimensions of $\mathbf{A} \otimes \mathbf{B}$?

The tensor product has the following properties:

$$x \otimes y = xy \tag{11}$$
$$\mathbf{A} \otimes (\mathbf{B} + \mathbf{C}) = \mathbf{A} \otimes \mathbf{B} + \mathbf{A} \otimes \mathbf{C} \tag{12}$$
$$(\mathbf{B} + \mathbf{C}) \otimes \mathbf{A} = \mathbf{B} \otimes \mathbf{A} + \mathbf{C} \otimes \mathbf{A} \tag{13}$$
$$(\mathbf{A} \otimes \mathbf{B})^\dagger = \mathbf{A}^\dagger \otimes \mathbf{B}^\dagger \qquad \text{Note! the order stays the same!} \tag{14}$$
$$(\mathbf{A} \otimes \mathbf{B}) \cdot (\mathbf{C} \otimes \mathbf{D}) = \mathbf{A} \cdot \mathbf{C} \otimes \mathbf{B} \cdot \mathbf{D}, \tag{15}$$

where $\cdot$ denotes regular matrix multiplication. (The first line means that if you just have numbers rather than matrices, the tensor product is just the regular product.)

Question: Consider the orthonormal basis $\{\mathbf{v_1}, \mathbf{v_2}\}$ for $\mathbb{C}^2$ where $\mathbf{v}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\mathbf{v}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Show that $\{\mathbf{v_1} \otimes \mathbf{v_1}, \mathbf{v_1} \otimes \mathbf{v_2}, \mathbf{v_2} \otimes \mathbf{v_1}, \mathbf{v_2} \otimes \mathbf{v_2}\}$ is an orthonormal basis for $\mathbb{C}^4$.

Question: In this problem, we'll show that the previous problem generalizes. Suppose we have an orthonormal basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$ for $\mathbb{C}^d$, and an orthonormal basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_f\}$ for $\mathbb{C}^f$. Show that the set of vectors consisting of all possible pairs of tensor products $\mathbf{v}_i \otimes \mathbf{u}_j$ form an orthonormal basis, and say which space they form a basis for. (Use the tensor product properties!)