CSE 534 – Quantum Computing
Assignment 0

Problems

Polar representation of complex numbers.

Consider a complex number $z \in \mathbb{C}$ such that $z = re^{i\theta}$ for $r \in \mathbb{R}_{\geq 0}$ and $\theta \in [0, 2\pi)$.

1. Show that every complex number $a + bi$ for $a, b \in \mathbb{R}$ can be expressed with a polar representation. Show that the polar representation is unique; that is $z = r'e^{i\theta'}$ if and only if $r' = r$ and $\theta' = \theta$.
   Proof:

When $z = 0$, any choice of $\theta \in [0, 2\pi)$ works since it must be that $\rho = 0$. Therefore, we restrict our consideration to when $z \neq 0$.

Given an arbitrary non-zero complex number $z = a + ib$, where $a, b \in \mathbb{R}$. Then z can be represented as a point on the complex plane (a, b). By the Pythagorean Theorem, we have that

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

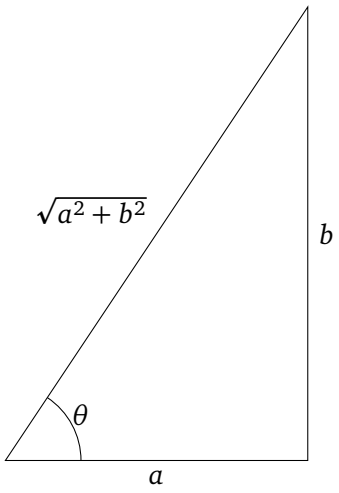
We can now find the angle between the positive x- axis, and the line segment from the origin (0, 0) to (a, b), which we already showed is $|z|$. This gives us

$$\cos(\theta) = \frac{a}{|z|} \quad \text{and} \quad \sin(\theta) = \frac{b}{|z|}$$

which necessarily implies that

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

Given below is a visual representation of the right angled triangle with side lengths a and b, and an application of the Pythagorean theorem to conclude the hypotenuse of this triangle is given by $\sqrt{a^2 + b^2}$, where for the purposes of clarity, the triangle is more concretely defined as shown below



(Note that this visual diagram is not entirely accurate, since it depends on the angle θ is which can lead to the number being in different quadrants.) Therefore, we have that substituting in the above expression

$$\begin{aligned} z &= a + ib \\ &= |z|\cos(\theta) + i|z|\sin(\theta) \\ &= |z|\left(\cos(\theta) + i \cdot \sin(\theta)\right) \\ &= |z|e^{i\theta} \qquad \text{using Euler's formula} \end{aligned}$$

where by definition $|z| \geq 0$. Setting $\rho = |z|$ and $\theta = \theta$, this is exactly what we wanted to show!

Uniqueness: We now show that the polar representation of z is unique. Suppose $z = a + ib$ has two polar representations $\rho e^{i\theta}$ and $\rho' e^{i\theta'}$ for some $\rho, \rho' \geq 0$ and $\theta, \theta' \in [0, 2\pi]$. Then we have that

$$\begin{aligned} \rho e^{i\theta} &= \rho\left(\cos(\theta) + i \cdot \sin(\theta)\right) && \text{using Euler's formula} \\ &= \rho\cos(\theta) + i \cdot \rho\sin(\theta) \end{aligned}$$

and similarly,

$$\begin{aligned} \rho' e^{i\theta'} &= \rho'\left(\cos(\theta') + i \cdot \sin(\theta')\right) && \text{using Euler's formula} \\ &= \rho'\cos(\theta') + i \cdot \rho'\sin(\theta') \end{aligned}$$

We can equate the real and imaginary parts of these two expressions to get that

$$\rho\cos(\theta) = \rho'\cos(\theta') \quad \text{and} \quad \rho\sin(\theta) = \rho'\sin(\theta')$$

Squaring and adding up both of the equations, we have that

$$\begin{aligned} \rho^2\cos^2(\theta) + \rho^2\sin^2(\theta) &= \rho'^2\cos^2(\theta') + \rho'^2\sin^2(\theta') \\ \rho^2 &= \rho'^2 && \text{since } \cos^2(\theta) + \sin^2(\theta) = 1 \text{ for all } \theta \end{aligned}$$

This means that $\rho = \rho^{'}$ or $\rho = -\rho^{'}$. (the opposite argument of $\rho^{'} = -\rho$ is symmetric) Since $\rho, \rho^{'} \geq 0$, we must have that $\rho = \rho^{'}$. This gives us that

$$\rho e^{i\theta} = \rho' e^{i\theta'} \implies e^{i\theta} = e^{i\theta'} \equiv e^{i(\theta - \theta')} = 1$$

Expanding the left-hand side using Euler's formula, we have that

$$\cos(\theta - \theta^{'}) + i \cdot \sin(\theta - \theta^{'}) = 1$$

This means that the real part of the left-hand side must be equal to 1. For $\cos(\theta - \theta^{'}) = 1$, it must be the case that $\theta - \theta^{'}$ is a multiple of 2π (since $\cos(2\pi k) = 1$). This means that

$$\theta - \theta^{'} = 2\pi k \quad \text{for some integer } k \in \mathbb{Z}$$

Now consider the possible values of $\theta - \theta^{'}$. Since $\theta, \theta^{'} \in [0, 2\pi]$, we have that $0 \leq \theta, \theta^{'} < 2\pi$. So then $-2\pi < \theta - \theta^{'} < 2\pi$. Since $\theta - \theta^{'}$ is a multiple of 2π, we have that k is either 0, or $\theta - \theta^{'} = 0$. This implies that $\theta = \theta^{'}$. This means that these two polar representations are actually the same. ■

2. For $z = re^{i\theta}$ and $z' = r'e^{i\theta'}$, what is the polar representation of the complex conjugate z^*? What is the polar representaiton of $z \cdot z'$?
Solution:

Complex conjugate: Given that $z = \rho e^{i\theta}$, we have that

$$z = \rho e^{i\theta} = \rho\left(\cos(\theta) + i \cdot \sin(\theta)\right)$$

This necessarily implies the following

$$\begin{aligned} z^* &= \overline{\rho\,(\cos(\theta)+i\cdot\sin(\theta))} = \overline{\rho}\cdot\overline{(\cos(\theta)+i\cdot\sin(\theta))} && \text{since } \rho\in\mathbb{R} \\ &= \rho\cdot(\cos(\theta)+i\cdot\sin(\theta)) = \rho\cdot(\cos(\theta)-i\cdot\sin(\theta)) \\ &= \rho\cdot(\cos(-\theta)+i\cdot\sin(-\theta)) && \text{since } \cos(-\theta)=\cos(\theta) \text{ and } \sin(-\theta)=-\sin(\theta) \\ &= \rho\cdot e^{-i\theta} && \text{using Euler's formula} \end{aligned}$$

Therefore if the polar representation of z is $\rho e^{i\theta}$, then the polar representation of its complex conjugate is given by $\rho e^{-i\theta}$. However, one small caveat, we want our angle θ to be in the prescribed range. If $\theta = -\theta = 0$, we can leave it as is. However if $\theta > 0$, then we simply add 2π to get $2\pi-\theta$ to be in the range $[0, 2\pi)$ which means the formal polar representation is given by

$$\overline{z} = \rho e^{i(2\pi-\theta)} \mod 2\pi$$

Product representation: Given that $z = \rho e^{i\theta}$ and $z' = \rho' e^{i\theta'}$, we have that

$$z\cdot z' = \rho e^{i\theta}\cdot\rho' e^{i\theta'} = \left(\rho\rho'\right)\cdot e^{i\theta}e^{i\theta'} = \rho\rho'\cdot e^{i\theta+i\theta'} = \rho\rho'\cdot e^{i(\theta+\theta')}$$

3. The multiplicative inverse, denoted z^{-1}, is the unique complex number such that $z\cdot z' = 1$. What is the multiplicative inverse of $z = re^{i\theta}$ and what is the mulitplicative inverse of $z = a+bi$?
Solution:

I claim that the multiplicative inverse of $z = re^{i\theta}$ is given by $z^{-1} = r^{-1}e^{-i\theta}$. Indeed note that

$$z\cdot z^{-1} = re^{i\theta}\cdot r^{-1}e^{-i\theta} = rr^{-1}\cdot e^{i\theta}e^{-i\theta} = 1$$

In cartesian coordinates; $z = a+bi$, the multiplicative inverse is given by

$$z^{-1} = \frac{1}{a+bi} = \frac{1}{a+bi}\cdot\frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2}$$

4. For any natural number $n\in\mathbb{N}$, calculate the n roots (including multiplicities) of $re^{i\theta}$ and express them in terms of $\omega_n = e^{2\pi i/n}$.
Solution:

The n roots of $re^{i\theta}$ are given by

$$\sqrt[n]{r}\left(\cos\left(\frac{\theta+2\pi k}{n}\right)+i\cdot\sin\left(\frac{\theta+2\pi k}{n}\right)\right) \quad \text{for } k\in\{0,1,\ldots,n-1\}$$

Bra-ket notation

Definition 1. Bra-ket notation is a quantum mechanics notation that is popularly used in quantum information and computation. We use $|\mathbf{v}\rangle$ to denote a (column)-vector in $\mathbb{C}^d$. Recall that a vector is a matrix with only one column. Equivalently $|\mathbf{v}\rangle \in \mathbb{C}^{d\times 1}$. We use $\langle \mathbf{v}| \in \mathbb{C}^{1\times d}$ to denote the row-vector with complex conjugate entries as that of $|\mathbf{v}\rangle$. So if

$$|\mathbf{v}\rangle = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{pmatrix}, \text{ then } \quad \langle v| = \begin{pmatrix} v_0^* & v_1^* & \cdots & v_{d-1}^* \end{pmatrix}, \tag{1}$$

in terms of the entry-wise values of $|\mathbf{v}\rangle$.

1. What is the value of $\langle \mathbf{v}|\mathbf{v}\rangle$? What is this quantity in traditional mathematical terms? Show this value is always real.
   Solution:

   Given the exposition provided in Definition 1, one can see that

   $$\langle \mathbf{v}|\mathbf{v}\rangle = \langle \mathbf{v}|\,|\mathbf{v}\rangle = \begin{pmatrix} v_0^* & v_1^* & \cdots & v_{d-1}^* \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{pmatrix}$$
   $$= v_0^* v_0 + v_1^* v_1 + \cdots + v_{d-1}^* v_{d-1} = |v_0|^2 + |v_1|^2 + \cdots + |v_{d-1}|^2 = \|\mathbf{v}\|^2$$

   This is the sum of the squares of the magnitudes of the entries of $|v\rangle$, which is always real since the magnitude of a complex number is always real.

2. What is the matrix representation of $|\mathbf{v}\rangle\langle \mathbf{v}|$? What is the trace of this matrix? How could you have calculated that using cyclicality of trace?
   Solution:

   Matrix representation: Once again assuming the usual definition for $|\mathbf{v}\rangle$, we have that

   $$|\mathbf{v}\rangle\langle \mathbf{v}| = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{pmatrix} \begin{pmatrix} v_0^* & v_1^* & \cdots & v_{d-1}^* \end{pmatrix} = \begin{pmatrix} v_0 v_0^* & v_0 v_1^* & \cdots & v_0 v_{d-1}^* \\ v_1 v_0^* & v_1 v_1^* & \cdots & v_1 v_{d-1}^* \\ \vdots & \vdots & \ddots & \vdots \\ v_{d-1} v_0^* & v_{d-1} v_1^* & \cdots & v_{d-1} v_{d-1}^* \end{pmatrix}$$

   Trace: Using the standard definition of the trace and observing the diagonal entries of the above matrix, one sees

   $$\mathrm{Tr}(|\mathbf{v}\rangle\langle \mathbf{v}|) = v_0 v_0^* + v_1 v_1^* + \cdots + v_{d-1} v_{d-1}^* = \sum_{k=0}^{d-1} |v_k|^2 = \|\mathbf{v}\|^2$$

   However; as the question rather *subtly* suggests; we can compute this quantity without going through the trouble of computing the matrix representation of $|\mathbf{v}\rangle\langle \mathbf{v}|$. Indeed, making use of the cyclicity of the trace

   $$\mathrm{Tr}(|\mathbf{v}\rangle\langle \mathbf{v}|) = \mathrm{Tr}(|\mathbf{v}\rangle\,\langle \mathbf{v}|) = \mathrm{Tr}(\langle \mathbf{v}|\mathbf{v}\rangle) = \langle \mathbf{v}|\mathbf{v}\rangle = \|\mathbf{v}\|^2$$

3. We use $\||\mathbf{v}\rangle\|$ to denote $\sqrt{\langle \mathbf{v}|\mathbf{v}\rangle}$. A vector is unit norm if this equals 1. Notationally, we use the following convention

to describe the unit vectors pointing in each of the coordinate directions:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \tag{2}$$

These vectors form a basis for $\mathbb{C}^d$ which is known as the *standard* or *canonical* basis. How can we express the vector $|v\rangle$ in terms of these basis vectors?

Solution:

Assuming the standard component-wise definition of $|\mathbf{v}\rangle$, we can express $|\mathbf{v}\rangle$ in terms of the standard basis vectors as

$$|\mathbf{v}\rangle = v_0 |0\rangle + v_1 |1\rangle + \cdots + v_{d-1} |d-1\rangle = \sum_{k=0}^{d-1} v_k |k\rangle$$

4. What is the matrix $\sum_{i=0}^{d-1} |i\rangle\langle i|$ in traditional mathematical terms?

Solution:

I claim that the matrix $\mathbf{M} = \sum_{i=0}^{d-1} |i\rangle\langle i|$ is the identity matrix $\mathbf{I}_d$. Indeed, one can see this by recalling the operator definition of the identity, which for all $\mathbf{v} \in \mathbb{C}^d$ satisfies

$$\mathbf{I}_d \mathbf{v} = \mathbf{v}$$

Let $|\mathbf{v}\rangle \in \mathbb{C}^d$ be an arbitrary vector. Making use of the decomposition in terms of standard basis vectors; we have

$$\begin{aligned} \mathbf{M}|\mathbf{v}\rangle &= \left(\sum_{i=0}^{d-1} |i\rangle\langle i| \right) |\mathbf{v}\rangle = \sum_{i=0}^{d-1} |i\rangle\langle i| \left(\sum_{k=0}^{d-1} v_k |k\rangle \right) \\ &= \sum_{i=0}^{d-1} \sum_{k=0}^{d-1} v_k |i\rangle \langle i|k\rangle = \sum_{i=0}^{d-1} v_i |i\rangle \underbrace{\langle i|i\rangle}_{1} + \sum_{i=0}^{d-1} \sum_{k \neq i} v_k |i\rangle \underbrace{\langle i|k\rangle}_{0} \\ &= \sum_{i=0}^{d-1} v_i |i\rangle = |\mathbf{v}\rangle \end{aligned}$$

Remark: The really nice thing about this kind of argument is that it's basis-invariant; and while this fact might be easier to digest for the standard basis as asked in the question; it's much less obvious for an arbitrary basis :)

5. For $i \in \{0, \ldots, d-1\}$, what is the value of $\langle i|\mathbf{v}\rangle$ for $|\mathbf{v}\rangle$ from before? Show that

$$|\mathbf{v}\rangle = \sum_{i=0}^{d-1} \langle i|\mathbf{v}\rangle |i\rangle . \tag{3}$$

Proof:

Given the decomposition of $|\mathbf{v}\rangle$ in terms of the standard basis vectors, we have that

$$\langle i|\mathbf{v}\rangle = \langle i|\left(\sum_{k=0}^{d-1} v_k |k\rangle\right) = \sum_{k=0}^{d-1} v_k \langle i|k\rangle = v_i$$

Therefore, we have that

$$|\mathbf{v}\rangle = \sum_{i=0}^{d-1} v_i |i\rangle = \sum_{i=0}^{d-1} \langle i|\mathbf{v}\rangle |i\rangle$$

This completes the proof. ■

6. Let $|\mathbf{v}\rangle$ and $|\mathbf{w}\rangle$ be unit vectors. Let $\mathbf{M} = |\mathbf{w}\rangle\langle\mathbf{v}|$. What is the value of $\mathbf{M}|\mathbf{v}\rangle$? Let $\left|\mathbf{v}^{\perp}\right\rangle$ be a vector such that $\left\langle\mathbf{v}\middle|\mathbf{v}^{\perp}\right\rangle = 0$. What is $\mathbf{M}\left|\mathbf{v}^{\perp}\right\rangle$?
Solution:

Plugging in the definitions of $\mathbf{M}$ and $|\mathbf{v}\rangle$

$$\mathbf{M}|\mathbf{v}\rangle = |\mathbf{w}\rangle\langle\mathbf{v}|\,|\mathbf{v}\rangle = |\mathbf{w}\rangle\,\langle\mathbf{v}|\mathbf{v}\rangle = |\mathbf{w}\rangle$$
$$\mathbf{M}\left|\mathbf{v}^{\perp}\right\rangle = |\mathbf{w}\rangle\langle\mathbf{v}|\left|\mathbf{v}^{\perp}\right\rangle = |\mathbf{w}\rangle\left\langle\mathbf{v}\middle|\mathbf{v}^{\perp}\right\rangle = \mathbf{0}$$

7. Let $\mathbf{M}$ be a square matrix $\in \mathbb{C}^{d\times d}$ with columns $|v_0\rangle, |v_1\rangle, \ldots, |v_{d-1}\rangle$. Show that

$$M = \sum_{i=0}^{d-1} |v_i\rangle\langle i|\,. \tag{4}$$

Proof:

By the definition of the matrix $\mathbf{M}$, we have that

$$\mathbf{M} = \begin{pmatrix} \vdots & \vdots & & \vdots \\ |v_0\rangle & |v_1\rangle & \cdots & |v_{d-1}\rangle \\ \vdots & \vdots & & \vdots \end{pmatrix}$$
$$= \begin{pmatrix} \vdots & \vdots & & \vdots \\ |v_0\rangle & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \vdots & & \vdots \end{pmatrix} + \begin{pmatrix} \vdots & \vdots & & \vdots \\ \mathbf{0} & |v_1\rangle & \cdots & \mathbf{0} \\ \vdots & \vdots & & \vdots \end{pmatrix} + \cdots + \begin{pmatrix} \vdots & \vdots & & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & |v_{d-1}\rangle \\ \vdots & \vdots & & \vdots \end{pmatrix}$$
$$= |v_0\rangle\langle 0| + |v_1\rangle\langle 1| + \cdots + |v_{d-1}\rangle\langle d-1| = \sum_{i=0}^{d-1} |v_i\rangle\langle i|$$

This settles the proof. ■

8. Let $\mathbf{M}$ be a matrix in $\mathbb{C}^{d\times d}$ and $|\mathbf{v}\rangle$ a vector in $\mathbb{C}^d$. Argue that the $\langle\mathbf{v}|\,\mathbf{M}^\dagger$ is the conjugate transpose of $\mathbf{M}\,|\mathbf{v}\rangle$.
Proof:

Let $\mathbf{M}$ be a matrix in $\mathbb{C}^{d\times d}$ with columns $|m_0\rangle, |m_1\rangle, \ldots, |m_{d-1}\rangle$. In the same vein; let $|\mathbf{v}\rangle$ be a vector in $\mathbb{C}^d$ with entries $v_0, v_1, \ldots, v_{d-1}$. Then we have that from the previous result,

$$\mathbf{M}\,|\mathbf{v}\rangle = \left(\sum_{i=0}^{d-1} |m_i\rangle\langle i|\right)|\mathbf{v}\rangle = \sum_{i=0}^{d-1} |m_i\rangle\langle i|\,|\mathbf{v}\rangle = \sum_{i=0}^{d-1} |m_i\rangle\,\langle i|\mathbf{v}\rangle = \sum_{i=0}^{d-1} v_i\,|m_i\rangle$$

Taking the conjugate transpose of this expression yields

$$(\mathbf{M}\,|\mathbf{v}\rangle)^\dagger = \left(\sum_{i=0}^{d-1} v_i\,|m_i\rangle\right)^\dagger = \sum_{i=0}^{d-1} v_i^*\,\langle m_i| = \sum_{i=0}^{d-1} \langle\mathbf{v}|i\rangle\,\langle m_i| = \langle\mathbf{v}|\left(\sum_{i=0}^{d-1} |i\rangle\langle m_i|\right) = \langle\mathbf{v}|\,\mathbf{M}^\dagger$$

This completes the proof. ■

Bases for vector spaces:

Definition 2. A set $V \subset \mathbb{C}^d$ is a subspace if it is closed under scalar multiplication and addition. A basis $\mathcal{B}$ for a vector space is a collection of vectors such that every vector can be expressed as a linear combination of vectors from $\mathcal{B}$ and $\mathcal{B}$ is of minimal cardinality.

1. Show that all bases for a vector space $V \subset \mathbb{C}^d$ have the same cardinality which is an integer between 0 and d.
Proof:

Suppose $\mathcal{U} = \{\mathbf{u}_0, \ldots, \mathbf{u}_m\}$ and $\mathcal{V} = \{\mathbf{v}_0, \ldots, \mathbf{v}_n\}$ are bases for $V \subset \mathbb{C}^d$. Then the $\mathbf{v}$'s span V and the $\mathbf{u}$'s are linearly indepedent. By Theorem 6 $m \leq n$. Reverse the roles; the $\mathbf{u}$'s span V and $\mathbf{v}$'s are linearly independent and using Theorem 6 once again allows us to assert $n \leq m$. Therefore $m = n$. ■

2. Show that $|\mathbf{v}_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ and $|\mathbf{v}_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$ form a basis for $\mathbb{C}^2$. Express the vectors $|0\rangle$ and $|1\rangle$ (see definitions above) in terms of this basis. The vectors $|\mathbf{v}_0\rangle$ and $|\mathbf{v}_1\rangle$ are used so much in quantum computation that they have special names: $|+\rangle$ and $|-\rangle$.
Solution:

We can write down the vector $\begin{bmatrix}1\\0\end{bmatrix}$ as a linear combination of the vectors $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ and $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$ as $\frac{\sqrt{2}}{2}$ times the sum of the two vectors, i.e. $\frac{\sqrt{2}}{2}(\mathbf{v}_1 + \mathbf{v}_2)$.

$$\frac{\sqrt{2}}{2}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\right) + \frac{\sqrt{2}}{2}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right) = \left(\frac{1}{2}\begin{bmatrix}1\\1\end{bmatrix} + \frac{1}{2}\begin{bmatrix}1\\-1\end{bmatrix}\right) = \frac{1}{2}\left(\begin{bmatrix}1\\1\end{bmatrix} + \begin{bmatrix}1\\-1\end{bmatrix}\right) = \frac{1}{2}\left(\begin{bmatrix}2\\0\end{bmatrix}\right) = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$$

We can write down the vector $\begin{bmatrix}0\\1\end{bmatrix}$ as a linear combination of the vectors $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ and $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$ with the coefficients $\frac{\sqrt{2}}{2}$ and $-\frac{\sqrt{2}}{2}$, i.e. $\frac{\sqrt{2}}{2}\mathbf{v}_1 - \frac{\sqrt{2}}{2}\mathbf{v}_2$.

$$\frac{\sqrt{2}}{2}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\right) + (-\frac{\sqrt{2}}{2})\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right) = \frac{1}{2}\left(\begin{bmatrix}1\\1\end{bmatrix} - \begin{bmatrix}1\\-1\end{bmatrix}\right) = \frac{1}{2}\left(\begin{bmatrix}1\\1\end{bmatrix} + \begin{bmatrix}-1\\1\end{bmatrix}\right) = \begin{bmatrix}0\\1\end{bmatrix} = |1\rangle$$

3. Express the vectors $|0\rangle$ and $|1\rangle$ in terms of $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$ and $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$.
Solution:

We can write down the vector $\begin{bmatrix}1\\0\end{bmatrix}$ as a linear combination of the vectors $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$ and $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}$ as $\frac{\sqrt{2}}{2}$ times the sum of the two vectors, i.e. $\frac{\sqrt{2}}{2}(v_1 + v_2)$.

$$\frac{\sqrt{2}}{2}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}\right) + \frac{\sqrt{2}}{2}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}\right) = \left(\frac{1}{2}\begin{bmatrix}1\\-i\end{bmatrix} + \frac{1}{2}\begin{bmatrix}1\\i\end{bmatrix}\right) = \frac{1}{2}\left(\begin{bmatrix}1\\-i\end{bmatrix} + \begin{bmatrix}1\\i\end{bmatrix}\right) = \frac{1}{2}\left(\begin{bmatrix}2\\0\end{bmatrix}\right) = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$$

We can write down the vector $\begin{bmatrix}0\\1\end{bmatrix}$ as a linear combination of the vectors $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$ and $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}$ with the coeffi-

cients $\frac{\sqrt{2}}{2}$ and $-\frac{\sqrt{2}}{2}$, i.e. $\frac{\sqrt{2}}{2}v_1 - \frac{\sqrt{2}}{2}v_2$.

$$\frac{\sqrt{2}}{2}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}\right)+(-\frac{\sqrt{2}}{2})\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}\right)=\frac{1}{2}\left(\begin{bmatrix}1\\-i\end{bmatrix}-\begin{bmatrix}1\\i\end{bmatrix}\right)=\frac{1}{2}\left(\begin{bmatrix}1\\-i\end{bmatrix}+\begin{bmatrix}-1\\i\end{bmatrix}\right)=\begin{bmatrix}0\\1\end{bmatrix}=|1\rangle$$

Inner product spaces

Definition 3. Consider a vector space V with a function $f : V \times V \to \mathbb{C}$ satisfying the following properties: For all vectors $u, v, w \in V$,

- (linearity) for all $\alpha, \beta \in \mathbb{C}$, $f(u, \alpha v + \beta w) = \alpha f(u, v) + \beta f(u, w)$.
- (complex conjugate symmetry) $f(u, v) = f(v, u)^*$.
- (positivity) $f(u, u) \in \mathbb{R}^+$ and $f(u, u) = 0$ iff $u = 0$.

Such a vector space is called an inner product space. When considering finite dimensional vector spaces, inner product spaces are *equivalent* to Hilbert spaces.

1. Show that $f(\alpha u, v) = \alpha^* f(u, v)$.
Proof:

We proceed as expected;

$$f(\alpha u, v) = \overline{f(v, \alpha u)} = \overline{\alpha f(v, u)} = \alpha^* f(u, v) \qquad \text{using conjugate symmetry and then linearity}$$

This completes the proof. ■

2. Show that the bilinear form given by $f(|\mathbf{u}\rangle, |\mathbf{v}\rangle) = \langle \mathbf{u}|\mathbf{v}\rangle$ for $|\mathbf{u}\rangle, |\mathbf{v}\rangle \in \mathbb{C}^d$ makes $\mathbb{C}^d$ an inner product space.
Proof:

Let $|\mathbf{u}\rangle, |\mathbf{v}\rangle, |\mathbf{w}\rangle \in \mathbb{C}^d$. We proceed by just doing because sometimes doing is easier than explaining.

- (linearity) For all $\alpha, \beta \in \mathbb{C}$, we have that

$$\begin{aligned} f(|\mathbf{u}\rangle, \alpha|\mathbf{v}\rangle + \beta|\mathbf{w}\rangle) = \langle \mathbf{u}|\alpha\mathbf{v} + \beta\mathbf{w}\rangle &= \sum_{i=0}^{d-1} \overline{u_i}(\alpha v_i + \beta w_i) \\ &= \alpha \sum_{i=0}^{d-1} \overline{u_i} v_i + \beta \sum_{i=0}^{d-1} \overline{u_i} w_i = \alpha \langle \mathbf{u}|\mathbf{v}\rangle + \beta \langle \mathbf{u}|\mathbf{w}\rangle \end{aligned}$$

- (complex conjugate symmetry) This follows from Theorem 2
- (positivity) Expanding the definition of the inner product, we have that

$$f(|\mathbf{u}\rangle, |\mathbf{u}\rangle) = \langle \mathbf{u}|\mathbf{u}\rangle = \sum_{i=0}^{d-1} \overline{u_i} u_i = \sum_{i=0}^{d-1} |u_i|^2 \geq 0$$

  and $f(|\mathbf{u}\rangle, |\mathbf{u}\rangle) = 0$ neccessitates $\|\mathbf{u}\|_2 = 0$ which implies $|\mathbf{u}\rangle = \mathbf{0}$.

This completes the proof. ■

Definition 4. In a lot of mathematical notation, the function f is often expressed as a bilinear form: $\langle \cdot, \cdot \rangle := f(\cdot, \cdot)$. The bra-ket notation was adopted in part because it matches this. We previously defined the norm as $\| |\mathbf{v}\rangle \| = \sqrt{\langle \mathbf{v}|\mathbf{v}\rangle}$.

3. Show that the function $\|\cdot\| : \mathbb{C}^d \to \mathbb{R}^+$ defined from the inner product yields a metric which is a function satisfying linearity, positivity, and the triangle inequality.
Proof:

Let $|\mathbf{u}\rangle, |\mathbf{v}\rangle, |\mathbf{w}\rangle \in \mathbb{C}^d$ and $\alpha \in \mathbb{C}$. We proceed as follows:

- (linearity) We have that

$$\| \alpha |\mathbf{u}\rangle \| = \sqrt{\langle \alpha \mathbf{u} | \alpha \mathbf{u} \rangle} = \sqrt{\sum_{i=0}^{d-1} \overline{\alpha u_i} \alpha u_i} = \sqrt{\sum_{i=0}^{d-1} |\alpha|^2 |u_i|^2} = |\alpha| \sqrt{\sum_{i=0}^{d-1} |u_i|^2} = |\alpha| \cdot \| |\mathbf{u}\rangle \|$$

- (positivity) We have that

$$\| |\mathbf{u}\rangle \| = \sqrt{\langle \mathbf{u}|\mathbf{u}\rangle} = \sqrt{\sum_{i=0}^{d-1} |u_i|^2} \geq 0$$

- (triangle inequality) We have that

$$\begin{aligned}
\| |\mathbf{u}\rangle + |\mathbf{v}\rangle \|^2 &= \langle \mathbf{u}+\mathbf{v} | \mathbf{u}+\mathbf{v} \rangle = \langle \mathbf{u}|\mathbf{u}\rangle + \langle \mathbf{u}|\mathbf{v}\rangle + \langle \mathbf{v}|\mathbf{u}\rangle + \langle \mathbf{v}|\mathbf{v}\rangle \\
&= \| |\mathbf{u}\rangle \|^2 + 2\Re(|\langle \mathbf{u}|\mathbf{v}\rangle|) + \| |\mathbf{v}\rangle \|^2 && \text{Theorem 2 and Observation} \\
&\leq \| |\mathbf{u}\rangle \|^2 + 2|\langle \mathbf{u}|\mathbf{v}\rangle| + \| |\mathbf{v}\rangle \|^2 && \text{Theorem 3} \\
&\leq \| |\mathbf{u}\rangle \|^2 + 2\|\mathbf{u}\|_2 \cdot \| |\mathbf{v}\rangle \|_2 + \| |\mathbf{v}\rangle \|^2 && \text{Cauchy Schwarz} \\
&= (\| |\mathbf{u}\rangle \|_2 + \| |\mathbf{v}\rangle \|_2)^2 \implies \| |\mathbf{u}\rangle + |\mathbf{v}\rangle \| \leq \| |\mathbf{u}\rangle \|_2 + \| |\mathbf{v}\rangle \|_2
\end{aligned}$$

This completes the proof. ■

4. Is it true that in a complex metric space, two unit vectors $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$ satisfy $\langle \mathbf{u}|\mathbf{v}\rangle = 0$ iff $\| |\mathbf{u}\rangle - |\mathbf{v}\rangle \| = \sqrt{2}$? Give a proof or counterexample. If not, is there a restricted metric space in which this is true.
Proof:

This one reveals itself after sufficients amounts of meditation. Consider the vectors $|\mathbf{u}\rangle = \begin{bmatrix} i \\ 0 \end{bmatrix}$ and $|\mathbf{v}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, we have that

$$\langle \mathbf{u}|\mathbf{v}\rangle = \left\langle \begin{bmatrix} i \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\rangle = -i \neq 0$$

while simultaneously we have that

$$\| |\mathbf{u}\rangle - |\mathbf{v}\rangle \| = \left\| \begin{bmatrix} i \\ 0 \end{bmatrix} - \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\| = \left\| \begin{bmatrix} i-1 \\ 0 \end{bmatrix} \right\| = \sqrt{|i-1|^2 + 0^2} = \sqrt{2}$$

While the Pythagorean theorem is not a bi-conditional in $\mathbb{C}^d$, it is true in $\mathbb{R}^d$. Indeed this is merely a consequence of expanding the square of the Euclidean norm and using the fact that the inner product is **completely**

symmetric in $\mathbb{R}^d$.

$$\begin{aligned} \| |\mathbf{u}\rangle - |\mathbf{v}\rangle \|_2^2 &= \langle \mathbf{u}|\mathbf{u}\rangle - \langle \mathbf{u}|\mathbf{v}\rangle - \langle \mathbf{v}|\mathbf{u}\rangle + \langle \mathbf{v}|\mathbf{v}\rangle \\ &= 2 - 2\,\langle \mathbf{u}|\mathbf{v}\rangle \text{ and therefore } \| |\mathbf{u}\rangle - |\mathbf{v}\rangle \|_2^2 = 2 \iff \langle \mathbf{u}|\mathbf{v}\rangle = 0 \end{aligned}$$

This completes the proof. ■

5. Generalize to show that if $|\langle \mathbf{u}|\mathbf{v}\rangle| \leq \epsilon$, then

$$\| |\mathbf{u}\rangle - |\mathbf{v}\rangle \|^2 \geq 2(1-\epsilon). \tag{5}$$

This says that when the inner product is small, then the two vectors are far from each other.
Proof:

From the definition of the Euclidean Norm and its relation to inner products we have that

$$\begin{aligned} \|\mathbf{u}-\mathbf{v}\|_2^2 &= \langle \mathbf{u}|\mathbf{u}\rangle - \langle \mathbf{u}|\mathbf{v}\rangle - \langle \mathbf{v}|\mathbf{u}\rangle + \langle \mathbf{v}|\mathbf{v}\rangle && \text{via linearity} \\ &= 2 - \langle \mathbf{u}|\mathbf{v}\rangle - \overline{\langle \mathbf{u}|\mathbf{v}\rangle} = 2 - 2\Re\left(\langle \mathbf{u}|\mathbf{v}\rangle\right) && \text{Theorem 2 and Observation} \\ &\geq 2 - 2|\,\langle \mathbf{u}|\mathbf{v}\rangle\,| \geq 2 - 2\epsilon = 2(1-\epsilon) && \text{Theorem 3} \end{aligned}$$

This completes the proof. ■

6. Show the converse is false. Find vectors such that $|\langle \mathbf{u}|\mathbf{v}\rangle| = 1$ but they are maximally far apart.
Solution:

Consider the vectors $|\mathbf{u}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|\mathbf{v}\rangle = \begin{bmatrix} -1 \\ 0 \end{bmatrix}$, we have that

$$|\,\langle \mathbf{u}|\mathbf{v}\rangle\,| = \left|\left\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix} \middle| \begin{bmatrix} -1 \\ 0 \end{bmatrix} \right\rangle\right| = \left| \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} -1 \\ 0 \end{bmatrix} \right| = |1 \cdot -1 + 0 \cdot 0| = 1$$

We also have that the distance between the two vectors is given by

$$\| |\mathbf{u}\rangle - |\mathbf{v}\rangle \|_2 = \left\| \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \begin{bmatrix} -1 \\ 0 \end{bmatrix} \right\| = \left\| \begin{bmatrix} 2 \\ 0 \end{bmatrix} \right\| = \sqrt{2^2 + 0^2} = \sqrt{4} = 2$$

However by the triangle inequality;

$$\| |\mathbf{u}\rangle - |\mathbf{v}\rangle \|_2 \leq \| |\mathbf{u}\rangle \|_2 + \| |\mathbf{v}\rangle \|_2 = 1 + 1 = 2$$

The desired result thus follows.

7. Show that if $|\langle \mathbf{u}|\mathbf{v}\rangle| \geq 1-\epsilon$, then there exists an angle $\theta \in [0, 2\pi)$ such that

$$\left\| |\mathbf{u}\rangle - e^{i\theta} |\mathbf{v}\rangle \right\| \leq \sqrt{2\epsilon}. \tag{6}$$

This shows that a large inner product implies that the two vectors are close "up to phase".
Proof:

We consider the square of the Euclidean norm as is convention. Let $|\mathbf{u}\rangle, |\mathbf{v}\rangle$ be arbitrary unit vectors in $\mathbb{C}^n$ and

$\epsilon > 0$. Fix $\theta \in [0, 2\pi)$ to be chosen later. We have that

$$\begin{aligned}
\| \, |\mathbf{u}\rangle - e^{i\theta} \, |\mathbf{v}\rangle \, \|_2^2 &= \langle \mathbf{u}|\mathbf{u}\rangle - \left\langle \mathbf{u}\middle| e^{i\theta}\mathbf{v}\right\rangle - \left\langle e^{i\theta}\mathbf{v}\middle|\mathbf{u}\right\rangle + \left\langle e^{i\theta}\mathbf{v}\middle| e^{i\theta}\mathbf{v}\right\rangle \\
&= 1 - \left\langle \mathbf{u}\middle| e^{i\theta}\mathbf{v}\right\rangle - \overline{\langle \mathbf{u}|e^{i\theta}\mathbf{v}\rangle} + \underbrace{|e^{i\theta}|^2}_{=1} \langle \mathbf{u}|\mathbf{v}\rangle = 2 - \left\langle \mathbf{u}\middle| e^{i\theta}\mathbf{v}\right\rangle - \overline{\langle \mathbf{u}|e^{i\theta}\mathbf{v}\rangle} && \text{Theorem 5} \\
&= 2 - 2\Re\left(\left\langle \mathbf{u}\middle| e^{i\theta}\mathbf{v}\right\rangle\right) = 2 - 2\Re\left(e^{i\theta} \, \langle \mathbf{u}|\mathbf{v}\rangle\right) && \text{Observation}
\end{aligned}$$

Let $z = \langle \mathbf{u}|\mathbf{v}\rangle$ which has the polar representation $z = |z|e^{i\phi}$ where $|z| \geq 0$ and $\phi \in [0, 2\pi)$. The time has arrived to pick θ. Define $\theta = 2\pi - \phi$. It is then clear that

$$\Re\left(e^{i\phi} \cdot \langle \mathbf{u}|\mathbf{v}\rangle\right) = \Re\left(e^{i(2\pi-\theta)} \cdot |z|e^{i\theta}\right) = \Re\left(e^{i(2\pi-\theta+\theta)} \cdot |z|\right) = \Re(|z|) = |z| = |\, \langle \mathbf{u}|\mathbf{v}\rangle \,|$$

This gives us that

$$\| \, |\mathbf{u}\rangle - e^{i\theta} \, |\mathbf{v}\rangle \, \|_2^2 = 2 - 2|\, \langle \mathbf{u}|\mathbf{v}\rangle \,| \leq 2 - 2(1-\epsilon) = 2\epsilon \quad \text{since } |\, \langle \mathbf{u}|\mathbf{v}\rangle \,| \geq 1 - \epsilon \implies -2|\, \langle \mathbf{u}|\mathbf{v}\rangle \,| \leq -2(1-\epsilon)$$

which therefore gives us that

$$\| \, |\mathbf{u}\rangle - e^{i\theta} \, |\mathbf{v}\rangle \, \|_2 \leq \sqrt{2\epsilon}$$

thereby settling the claim. ■

Linear transformations

Theorem 1. Recall that over a vector space $V \subseteq \mathbb{C}^d$, any linear transformation $T : V \to V$ has a matrix representation such that $T(|\mathbf{v}\rangle) = M_T |\mathbf{v}\rangle$.

Proof:

$\Longleftarrow$: Let $T : V \to V$ be a transformation that has a matrix representation $\mathbf{A}$ such that $T(|\mathbf{v}\rangle) = \mathbf{A}|\mathbf{v}\rangle$ for all $|\mathbf{v}\rangle \in V$. It is now sufficient to argue that T is linear. Let $|\mathbf{u}\rangle, |\mathbf{v}\rangle \in V$ and $\alpha, \beta \in \mathbb{C}$. We have that

$$T(\alpha|\mathbf{u}\rangle + \beta|\mathbf{v}\rangle) = \mathbf{A}(\alpha|\mathbf{u}\rangle + \beta|\mathbf{v}\rangle) = \alpha\mathbf{A}|\mathbf{u}\rangle + \beta\mathbf{A}|\mathbf{v}\rangle = \alpha T(|\mathbf{u}\rangle) + \beta T(|\mathbf{v}\rangle)$$

where we exploit the linearity of matrix-vector multiplication.
$\Longrightarrow$: Let $T : V \to V$ be a linear transformation. It remains to show that T has a matrix representation. Let $|\mathbf{v}\rangle \in V$ be an arbitrary vector. The astute reader will recall that $\{|\mathbf{e}_i\rangle\}_{i=0}^{d-1}$ is the standard basis for $\mathbb{C}^d$. We can write $|\mathbf{v}\rangle$ as a linear combination of the standard basis vectors, i.e.

$$|\mathbf{v}\rangle = \sum_{i=0}^{d-1} v_i |\mathbf{e}_i\rangle$$

where v_i are the entries of $|\mathbf{v}\rangle$. The result now follows since

$$\begin{aligned} T(|\mathbf{v}\rangle) &= T\left(\sum_{i=0}^{d-1} v_i |\mathbf{e}_i\rangle\right) = \sum_{i=0}^{d-1} v_i T(|\mathbf{e}_i\rangle) && \text{as per linearity of } T \\ &= \underbrace{\begin{bmatrix} \vdots & \vdots & \vdots & \vdots \\ T(|\mathbf{e}_0\rangle) & T(|\mathbf{e}_1\rangle) & \cdots & T(|\mathbf{e}_{d-1}\rangle) \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}}_{\mathbf{A}} \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{bmatrix} = \mathbf{A}|\mathbf{v}\rangle \end{aligned}$$

which completes the proof. ■

Definition 5. For a bilinear form $\langle \cdot, \cdot \rangle$ defining an inner product space, the adjoint of a linear transform T is the transformation $T^\dagger$ such that

$$\langle T^\dagger u, v \rangle = \langle u, Tv \rangle. \tag{7}$$

1. Show that the adjoint of a linear transform with matrix representation T for the bilinear form $\langle\cdot|\cdot\rangle$ is defined by the conjugate transpose.
Proof:

Given the definition of $\mathbf{A}^\dagger$, pick $\mathbf{u} = \mathbf{e}_i$ and $\mathbf{v} = \mathbf{e}_j$ for $0 \leq i, j \leq n$ where $\mathbf{e}_i, \mathbf{e}_j \in \mathbb{C}^n$ are the standard basis vectors of $\mathbb{C}^n$. It then reveals itself that

$$\langle \mathbf{A}^\dagger \mathbf{e}_i, \mathbf{e}_j \rangle = \langle \mathbf{A}^\dagger_{;i}, \mathbf{e}_j \rangle = \overline{\mathbf{A}^\dagger}_{j,i}$$

where we denote $\mathbf{A}_{;\,i}$ to be the i^{th} column of $\mathbf{A}$. To see this, consider an arbitrary matrix $\mathbf{B} \in \mathbb{C}^{n\times n}$, defined such that

$$\mathbf{B} = \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n} \end{bmatrix}$$

This therefore gives us that

$$\mathbf{B}\mathbf{e}_i = \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} b_{1,i} \\ b_{2,i} \\ \vdots \\ b_{n,i} \end{bmatrix} = \mathbf{B}_{;\,i}$$

Using the definition of the conjugate transpose, we know that

$$\langle \mathbf{A}^\dagger \mathbf{e}_i, \mathbf{e}_j \rangle = \langle \mathbf{e}_i, \mathbf{A}\mathbf{e}_j \rangle$$

and simplifying the right hand side, we have that this is equal to

$$\langle \mathbf{e}_i, \mathbf{A}\mathbf{e}_j \rangle = \langle \mathbf{e}_i, \mathbf{A}_{;\,j} \rangle = \mathbf{A}_{i,j}$$

The result thus follows since

$$\mathbf{A}_{i,j} = \overline{\mathbf{A}^\dagger}_{j,i} \iff \mathbf{A}^\dagger = \overline{\mathbf{A}}^\top$$

which completes the proof. ■

2. A matrix $\mathbf{H} \in \mathbb{C}^{d\times d}$ is Hermitian if $\mathbf{H}^\dagger = \mathbf{H}$ where $\mathbf{H}^\dagger$ is the conjugate transpose.

   - Show that the diagonal coordinates of $\mathbf{H}$ must be real.
   Proof:

   This follows immediately since

   $$\mathbf{H} = \mathbf{H}^\dagger \iff \mathbf{H}_{i,j} = \overline{\mathbf{H}^\dagger}_{j,i} \implies \mathbf{H}_{i,i} = \overline{\mathbf{H}^\dagger}_{i,i} \implies \mathbf{H}_{i,i} \in \mathbb{R}$$

   as desired. ■

   - Show that the eigenvalues of $\mathbf{H}$ must be real.
   Proof:

Let $|\mathbf{v}\rangle \in \mathbb{C}^n$ be an eigenvector of $\mathbf{H}$ with eigenvalue λ. We have that

$$\begin{aligned}
&\mathbf{H}|\mathbf{v}\rangle = \lambda|\mathbf{v}\rangle \implies \langle\mathbf{v}|\mathbf{H}^\dagger = \overline{\lambda}\langle\mathbf{v}| && \text{taking the conjugate transpose of both sides}\\
&\implies \langle\mathbf{v}|\underbrace{\mathbf{H}|\mathbf{v}\rangle}_{\lambda|\mathbf{v}\rangle} = \overline{\lambda}\langle\mathbf{v}|\mathbf{v}\rangle = \overline{\lambda}\|\mathbf{v}\|_2^2 && \text{taking an inner product with } |\mathbf{v}\rangle\\
&\implies \lambda\|\mathbf{v}\|_2^2 = \overline{\lambda}\|\mathbf{v}\|_2^2 \implies \lambda = \overline{\lambda} \implies \lambda \in \mathbb{R} && \text{since } \|\mathbf{v}\|_2 \neq 0
\end{aligned}$$

This completes the proof. ■

- Let $|\mathbf{v}\rangle$ be a unit eigenvector of eigenvalue $\lambda \in \mathbb{R}$. Let $\mathbf{H}' = \mathbf{H} - \lambda|\mathbf{v}\rangle\langle\mathbf{v}|$. Show that $\mathbf{H}'|\mathbf{v}\rangle = 0$. Next, let $|\mathbf{w}\rangle$ be a vector orthogonal to $|\mathbf{v}\rangle$. Show that $\mathbf{H}'|\mathbf{w}\rangle = \mathbf{H}|\mathbf{w}\rangle$.
Proof:

Let $|\mathbf{v}\rangle$ be a unit eigenvector of $\mathbf{H}$ with eigenvalue $\lambda \in \mathbb{R}$. We have that

$$\mathbf{H}'|\mathbf{v}\rangle = (\mathbf{H} - \lambda|\mathbf{v}\rangle\langle\mathbf{v}|)|\mathbf{v}\rangle = \mathbf{H}|\mathbf{v}\rangle - \lambda|\mathbf{v}\rangle\underbrace{\langle\mathbf{v}|\mathbf{v}\rangle}_{1} = \lambda|\mathbf{v}\rangle - \lambda|\mathbf{v}\rangle = 0$$

as desired. Let $|\mathbf{w}\rangle$ be a vector orthogonal to $|\mathbf{v}\rangle$. We have that

$$\mathbf{H}'|\mathbf{w}\rangle = (\mathbf{H} - \lambda|\mathbf{v}\rangle\langle\mathbf{v}|)|\mathbf{w}\rangle = \mathbf{H}|\mathbf{w}\rangle - \lambda|\mathbf{w}\rangle\underbrace{\langle\mathbf{v}|\mathbf{w}\rangle}_{0} = \mathbf{H}|\mathbf{w}\rangle$$

as desired. This completes the proof. ■

NOTE: I believe initially it said $\Pi = \mathbf{I} - |\lambda\rangle\langle\lambda|$; let me know if this modification makes sense and the definitions I assumed are correct - Luksh

- Let $\Pi = \mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|$. Recall that a matrix is a projection if it equals its square; or equivalently its eigenvalues are either 1 or 0. Show that Π is a projection i.e. $\Pi^2 = \Pi$. Show that $\mathbf{H}' = \Pi\mathbf{H}\Pi$.
Proof:

Π **is a projection**: We have that

$$\begin{aligned}
\Pi^2 = (\mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|)^2 &= (\mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|)(\mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|) = \mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}| - |\mathbf{v}\rangle\langle\mathbf{v}| + |\mathbf{v}\rangle\underbrace{\langle\mathbf{v}|\mathbf{v}\rangle}_{=1}\langle\mathbf{v}|\\
&= \mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}| - |\mathbf{v}\rangle\langle\mathbf{v}| + |\mathbf{v}\rangle\langle\mathbf{v}| = \mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}| = \Pi
\end{aligned}$$

$\mathbf{H}' = \Pi\mathbf{H}\Pi$: We have that

$$\begin{aligned}
\Pi\mathbf{H}\Pi &= (\mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|)\mathbf{H}(\mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|) = (\mathbf{H} - |\mathbf{v}\rangle\langle\mathbf{v}|)(\mathbf{H} - \underbrace{\mathbf{H}|\mathbf{v}\rangle}_{\lambda|\mathbf{v}\rangle}\langle\mathbf{v}|)\\
&= (\mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|)(\mathbf{H} - \lambda|\mathbf{v}\rangle\langle\mathbf{v}|) = \mathbf{H} - \lambda|\mathbf{v}\rangle\langle\mathbf{v}| - |\mathbf{v}\rangle\langle\mathbf{v}|\mathbf{H} + \lambda|\mathbf{v}\rangle\langle\mathbf{v}| = \mathbf{H} - |\mathbf{v}\rangle\langle\mathbf{v}|\mathbf{H}\\
&= \mathbf{H} - |\mathbf{v}\rangle(\mathbf{H}|\mathbf{v}\rangle)^\dagger = \mathbf{H} - |\mathbf{v}\rangle\langle\mathbf{v}|\lambda^\dagger = \mathbf{H} - \lambda|\mathbf{v}\rangle\langle\mathbf{v}| = \mathbf{H}'
\end{aligned}$$

as desired. This completes the proof. ■

- Use this and the Gram-Schmidt process to show that there exist eigenvalues $\lambda_0, \ldots, \lambda_{d-1} \in \mathbb{R}$ and an orthonormal set of eigenvectors $|\mathbf{v}_0\rangle, \ldots, |\mathbf{v}_{d-1}\rangle$ such that

$$\mathbf{H} = \sum_{i=0}^{d-1} \lambda_i |\mathbf{v}_i\rangle\langle\mathbf{v}_i| . \tag{8}$$

Proof:

Let $\mathbf{H} \in \mathbb{C}^{d\times d}$ be an arbitrary Hermitian matrix. We argue by induction on d.
Base Case: For $d = 1$, $\mathbf{H} = \mathbf{H}^\dagger \implies \mathbf{H} \in \mathbb{R}$ and therefore the trivial decomposition of $\mathbf{H} = 1 \cdot \mathbf{H} \cdot 1$ holds.
Inductive Hypothesis: Assume that the claim holds for $d = k$, i.e. any hermitian $\mathbf{H} \in \mathbb{C}^{k\times k}$ can be decomposed as

$$\mathbf{H} = \sum_{i=0}^{k-1} \lambda_i \left|\mathbf{v}_i\right\rangle\left\langle\mathbf{v}_i\right|$$

where $\lambda_i \in \mathbb{R}$ and $\{|\mathbf{v}_i\rangle\}_{i=0}^{k-1}$ is an orthonormal set of eigenvectors or as matrices

$$\mathbf{H} = \mathbf{U}\Lambda\mathbf{U}^\dagger \quad \text{where } \mathbf{U} \text{ is unitary and } \Lambda \text{ is diagonal}$$

Inductive Step: Let $\mathbf{H} = \mathbf{H}^\dagger \in \mathbb{C}^{(k+1)\times(k+1)}$ be an arbitrary Hermitian matrix. Let $|\mathbf{v}\rangle$ be a unit eigenvector with corresponding eigenvalue λ. Now define

$$\mathbf{P} := |\mathbf{v}\rangle\langle\mathbf{v}| \implies \mathbf{P}^\perp = \mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|$$

Making use that the projector onto the span of $|\mathbf{v}\rangle$ and its orthogonal complement sum to the identity, we have that

$$\mathbf{H} = \mathbf{I}\cdot\mathbf{H}\cdot\mathbf{I} = (\mathbf{P}+\mathbf{P}^\perp)\mathbf{H}(\mathbf{P}+\mathbf{P}^\perp) = \mathbf{PHP} + \mathbf{PHP}^\perp + \mathbf{P}^\perp\mathbf{HP} + \mathbf{P}^\perp\mathbf{HP}^\perp$$

We now simplify the individual terms in the sum above. We have that

- Let $|\mathbf{x}\rangle \in \mathbb{C}^{k+1}$ be an arbitrary vector. Then

$$\begin{aligned}\mathbf{P}^\perp\mathbf{HP}\left|\mathbf{x}\right\rangle &= (\mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|)\mathbf{H}\left|\mathbf{v}\right\rangle\left\langle\mathbf{v}|\mathbf{x}\right\rangle \\ &= \left\langle\mathbf{v}|\mathbf{x}\right\rangle\left[\mathbf{H}\left|\mathbf{v}\right\rangle - \left|\mathbf{v}\right\rangle\left\langle\mathbf{v}|\mathbf{H}|\mathbf{v}\right\rangle\right] = \left\langle\mathbf{v}|\mathbf{x}\right\rangle\left[\lambda\left|\mathbf{v}\right\rangle - \lambda\left|\mathbf{v}\right\rangle\left\langle\mathbf{v}|\mathbf{v}\right\rangle\right] = 0\end{aligned}$$

  where we have used the fact that $\mathbf{H}\left|\mathbf{v}\right\rangle = \lambda\left|\mathbf{v}\right\rangle$. Since $|\mathbf{x}\rangle$ was arbitrary, we have that $\mathbf{P}^\perp\mathbf{HP} = 0$.
- Let $|\mathbf{x}\rangle \in \mathbb{C}^{k+1}$ be an arbitrary vector. Then

$$\begin{aligned}\mathbf{PHP}^\perp\left|\mathbf{x}\right\rangle &= \left|\mathbf{v}\right\rangle\left\langle\mathbf{v}\right|\mathbf{H}(\mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}|)\left|\mathbf{x}\right\rangle = \left|\mathbf{v}\right\rangle\left\langle\mathbf{v}\right|\left[\mathbf{H}\left|\mathbf{x}\right\rangle - \left\langle\mathbf{v}|\mathbf{x}\right\rangle\mathbf{H}\left|\mathbf{v}\right\rangle\right] \\ &= \left|\mathbf{v}\right\rangle\left\langle\mathbf{v}|\mathbf{H}|\mathbf{x}\right\rangle - \left\langle\mathbf{v}|\mathbf{x}\right\rangle\cdot\underbrace{\left\langle\mathbf{v}|\mathbf{H}|\mathbf{v}\right\rangle}_{\lambda}\cdot\left|\mathbf{v}\right\rangle \\ &= \lambda\left\langle\mathbf{v}|\mathbf{x}\right\rangle\cdot\left|\mathbf{v}\right\rangle - \lambda\left\langle\mathbf{v}|\mathbf{x}\right\rangle\left|\mathbf{v}\right\rangle = 0\end{aligned}$$

  where we have used the fact that $\mathbf{H}\left|\mathbf{v}\right\rangle = \lambda\left|\mathbf{v}\right\rangle$. Since $|\mathbf{x}\rangle$ was arbitrary, we have that $\mathbf{PHP}^\perp = 0$.
- Since $\mathbf{P} = |\mathbf{v}\rangle\langle\mathbf{v}|$;

$$\mathbf{PHP} = \left|\mathbf{v}\right\rangle\left\langle\mathbf{v}\right|\mathbf{H}\left|\mathbf{v}\right\rangle\left\langle\mathbf{v}\right| = \left|\mathbf{v}\right\rangle\left\langle\mathbf{v}\right|\lambda\left|\mathbf{v}\right\rangle\left\langle\mathbf{v}\right| = \lambda\left|\mathbf{v}\right\rangle\left\langle\mathbf{v}\right|$$

- Finally we move to compute $\mathbf{P}^\perp\mathbf{HP}^\perp$. Observe that for any orthonormal basis $\{|\mathbf{v}_i\rangle\}_{i=0}^{k}$, we have that $\mathbf{I} = \sum_{i=0}^{k}\left|\mathbf{v}_i\right\rangle\left\langle\mathbf{v}_i\right|$. By Theorem 7 the normalized eigenvectors of $\mathbf{H}$ form an orthonormal basis for $\mathbb{C}^{k+1}$ and therefore satisfy the above completeness relation. Therefore

$$\mathbf{P}^\perp = \mathbf{I} - |\mathbf{v}\rangle\langle\mathbf{v}| = \sum_{i=1}^{k}|\mathbf{v}_i\rangle\langle\mathbf{v}_i| = \mathbf{V}\mathbf{V}^\dagger \quad \text{where } \mathbf{V} = \begin{bmatrix}|\mathbf{v}_1\rangle & \cdots & |\mathbf{v}_k\rangle\end{bmatrix} \in \mathbb{C}^{(k+1)\times k}$$

Therefore plugging this into the expression for $\mathbf{P}^{\perp}\mathbf{H}\mathbf{P}^{\perp}$, one yields

$$\mathbf{P}^{\perp}\mathbf{A}\mathbf{P}^{\perp} = \mathbf{V}\mathbf{V}^{\dagger}\mathbf{H}\mathbf{V}\mathbf{V}^{\dagger} = \mathbf{V}\underbrace{\mathbf{V}^{\dagger}\mathbf{H}\mathbf{V}}_{\Lambda}\mathbf{V}^{\dagger} = \mathbf{V}\Lambda\mathbf{V}^{\dagger} \qquad \text{where } \Lambda \in \mathbb{C}^{k\times k}$$

$$\mathbf{H} = \mathbf{H}^{\dagger} \implies \Lambda^{\dagger} = \mathbf{V}^{\dagger}\mathbf{H}^{\dagger}\mathbf{V} = \mathbf{V}^{\dagger}\mathbf{H}\mathbf{V} = \Lambda$$

Therefore applying the inductive hypothesis, we have that

$$\Lambda = \mathbf{U}\Lambda'\mathbf{U}^{\dagger} \quad \text{where } \Lambda' \text{ is diagonal and } \mathbf{U} \text{ is unitary}$$

We are nearing the end of the proof. It can be easily verified that the product of two matrices with orthonormal columns is another resultant matrix with orthonormal columns. Additionally making use of the column-representation of the matrix product, we can assert that the columns of $\mathbf{VU}$ are orthonormal to $\mathbf{V}$. We then obtain

$$\mathbf{P}^{\dagger}\mathbf{H}\mathbf{P}^{\dagger} = \underbrace{\mathbf{V}\mathbf{U}}_{\mathbf{S}\in\mathbb{C}^{(k+1)\times k}}\Lambda'\mathbf{U}^{\dagger}\mathbf{V}^{\dagger} = \mathbf{S}\Lambda'\mathbf{S}^{\dagger} \qquad \text{where } \mathbf{S}^{\dagger}\mathbf{S} = \mathbf{I}$$

$$\mathbf{S} = \begin{pmatrix} \vdots & \vdots & \vdots \\ \mathbf{s}_1 & \cdots & \mathbf{s}_k \\ \vdots & \vdots & \vdots \end{pmatrix} \implies \mathbf{P}\mathbf{H}\mathbf{P}^{\perp} = \mathbf{S}\Lambda'\mathbf{S}^{\dagger} = \sum_{i=1}^{k}\lambda_i |\mathbf{s}_i\rangle\langle\mathbf{s}_i|$$

Collecting non-zero contributions to the sum, we have that

$$\begin{aligned}\mathbf{H} &= \mathbf{P}\mathbf{H}\mathbf{P} + \mathbf{P}\mathbf{H}\mathbf{P}^{\perp} + \mathbf{P}^{\perp}\mathbf{H}\mathbf{P} + \mathbf{P}^{\perp}\mathbf{H}\mathbf{P}^{\perp} \\ &= \lambda|\mathbf{v}\rangle\langle\mathbf{v}| + 0 + 0 + \sum_{i=1}^{k}\lambda_i|\mathbf{s}_i\rangle\langle\mathbf{s}_i| = \tilde{\mathbf{U}}\tilde{\mathbf{\Lambda}}\tilde{\mathbf{U}}^{\dagger} \qquad \text{where } \tilde{\mathbf{U}} = \begin{pmatrix}|\mathbf{v}\rangle & \mathbf{S}\end{pmatrix} \text{ and } \tilde{\mathbf{\Lambda}} = \begin{pmatrix}\lambda & \mathbf{0} \\ \mathbf{0} & \Lambda'\end{pmatrix}\end{aligned}$$

Finally it can be seen that $\tilde{\mathbf{U}}$ has orthonormal columns and $\tilde{\mathbf{\Lambda}}$ is diagonal. This completes the proof. ■

3. A matrix $\mathbf{U} \in \mathbb{C}^{d\times d}$ is unitary if $\mathbf{U}^{\dagger}\mathbf{U} = \mathbf{I}$. Show the following are equivalent by proving that each implies the next and the last implies the first.

   - $\mathbf{U}$ is unitary.
   - $\mathbf{U}$ maps an orthonormal basis to an orthonormal basis.
   - $\mathbf{U}$ maps any unit vector to another unit vector.

   Proof:

   • Let $\mathbf{U} \in \mathbb{C}^{d\times d}$ be an arbitrary unitary matrix. Given some $\mathcal{B} = \{|\mathbf{b_i}\rangle\}_{i=0}^{d-1}$, an orthonormal basis for $\mathbb{C}^d$, we have that

   $$\langle \mathbf{U}\mathbf{b_i} | \mathbf{U}\mathbf{b_j}\rangle = \langle \mathbf{b_i} | \mathbf{b}_j\rangle = \begin{cases}1 & i = j \\ 0 & i \neq j\end{cases} \qquad \text{Theorem 4}$$

   $$\implies \{\mathbf{U}|\mathbf{b_i}\rangle\}_{i=0}^{d-1} = \mathbf{U}\mathcal{B} \text{ is an orthonormal basis}$$

   • Let $\mathbf{U} \in \mathbb{C}^{d\times d}$ be a matrix that maps an orthonormal basis to another orthonormal basis. Let $|\mathbf{u}\rangle \in \mathbb{C}^d$ be an arbitrary unit vector and $\mathcal{B} = \{|\mathbf{b_i}\rangle\}_{i=0}^{d-1}$ be an orthonormal basis. Let $|\mathbf{u}\rangle = \sum_{i=0}^{d-1} u_i |\mathbf{b_i}\rangle$ be the expansion of

$|\mathbf{u}\rangle$ in terms of the basis vectors. We have that

$$\begin{aligned}
\| \mathbf{U}|\mathbf{u}\rangle \|^2 &= \left\| \mathbf{U}\left(\sum_{i=0}^{d-1} u_i |\mathbf{b_i}\rangle\right)\right\|^2 = \left|\sum_{i=0}^{d-1} u_i \mathbf{U}|\mathbf{b}_i\rangle\right|^2 \\
&= \left\langle \sum_{i=0}^{d-1} u_i \mathbf{U}|\mathbf{b}_i\rangle \middle| \sum_{j=0}^{d-1} u_j \mathbf{U}\middle|\mathbf{b}_j\right\rangle = \sum_{i=0}^{d-1}\sum_{j=0}^{d-1} \overline{u}_i u_j \left\langle \mathbf{U}\mathbf{b}_i \middle| \mathbf{U}\mathbf{b}_j\right\rangle \\
&= \sum_{i=0}^{d-1}\sum_{j=0}^{d-1} \overline{u}_i u_j \left\langle \mathbf{b}'_i \middle| \mathbf{b}'_j\right\rangle = \sum_{i=0}^{d-1} |u_i|^2 \underbrace{\left\langle \mathbf{b}'_i \middle| \mathbf{b}'_i\right\rangle}_{1} + \sum_{i\neq j} \overline{u}_i u_j \underbrace{\left\langle \mathbf{b}'_i \middle| \mathbf{b}'_j\right\rangle}_{0} \\
&= \sum_{i=0}^{d-1} |u_i|^2 = \| |\mathbf{u}\rangle \|^2 = 1
\end{aligned}$$

• Since $\mathbf{U} : \mathbb{C}^n \to \mathbb{C}^n$ maps any unit vector to another unit vector, Theorem 5 tells us that for an arbitrary vector $\mathbf{v} \in \mathbb{C}^n$, $\|\mathbf{U}\mathbf{v}\|_2 = \|\mathbf{v}\|_2$. Let $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$; then this preservation gives us

$$\|\mathbf{U}(\mathbf{x}+\mathbf{y})\|_2 = \|\mathbf{x}+\mathbf{y}\|_2$$

The left hand side is

$$\begin{aligned}
\|\mathbf{U}(\mathbf{x}+\mathbf{y})\|_2^2 &= \langle \mathbf{U}(\mathbf{x}+\mathbf{y})|\mathbf{U}(\mathbf{x}+\mathbf{y})\rangle = \langle \mathbf{U}\mathbf{x}+\mathbf{U}\mathbf{y}|\mathbf{U}\mathbf{x}+\mathbf{U}\mathbf{y}\rangle \\
&= \langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{x}\rangle + \langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle + \langle \mathbf{U}\mathbf{y}|\mathbf{U}\mathbf{x}\rangle + \langle \mathbf{U}\mathbf{y}|\mathbf{U}\mathbf{y}\rangle \\
&= 2 + \langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle + \overline{\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle} = 2 + 2\Re(\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle) \qquad \text{Theorem 2 and Observation}
\end{aligned}$$

The right hand side is

$$\begin{aligned}
\|\mathbf{x}+\mathbf{y}\|_2^2 &= \langle \mathbf{x}+\mathbf{y}|\mathbf{x}+\mathbf{y}\rangle = \langle \mathbf{x}|\mathbf{x}\rangle + \langle \mathbf{x}|\mathbf{y}\rangle + \langle \mathbf{y}|\mathbf{x}\rangle + \langle \mathbf{y}|\mathbf{y}\rangle \\
&= 2 + \langle \mathbf{x}|\mathbf{y}\rangle + \overline{\langle \mathbf{x}|\mathbf{y}\rangle} = 2 + 2\Re(\langle \mathbf{x}|\mathbf{y}\rangle) \qquad \text{Theorem 2 and Observation}
\end{aligned}$$

Equality and cancellation gives us that

$$\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle + \overline{\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle} = \langle \mathbf{x}|\mathbf{y}\rangle + \overline{\langle \mathbf{x}|\mathbf{y}\rangle} \iff 2\Re(\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle) = 2\Re(\langle \mathbf{x}|\mathbf{y}\rangle) \iff \Re(\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle) = \Re(\langle \mathbf{x}|\mathbf{y}\rangle)$$

Let us call the equation above **Equation 1**. The only hurdle in demonstrating equality of inner products is illustrating that $\Im(\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle) = \Im(\langle \mathbf{x}|\mathbf{y}\rangle)$. With that intent, substitute $i\mathbf{x}$ for $\mathbf{x}$ into **Equation 1** to get

$$\begin{aligned}
\langle i\mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle + \overline{\langle i\mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle} &= -i\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle + i\overline{\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle} = -i(\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle - \overline{\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle}) \\
&= -i\cdot 2\Im(\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle) \qquad \text{by Observation} \\
\langle i\mathbf{x}|\mathbf{y}\rangle + \overline{\langle i\mathbf{x}|\mathbf{y}\rangle} &= -i\langle \mathbf{x}|\mathbf{y}\rangle + i\overline{\langle \mathbf{x}|\mathbf{y}\rangle} = -i(\langle \mathbf{x}|\mathbf{y}\rangle - \overline{\langle \mathbf{x}|\mathbf{y}\rangle}) \\
&= -i\cdot 2\Im(\langle \mathbf{x}|\mathbf{y}\rangle) \qquad \text{by Observation}
\end{aligned}$$

$$\textbf{Equation 1} \implies -i\cdot 2\Im(\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle) = -i\cdot 2\Im(\langle \mathbf{x}|\mathbf{y}\rangle) \implies \Im(\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle) = \Im(\langle \mathbf{x}|\mathbf{y}\rangle)$$

Therefore $\langle \mathbf{U}\mathbf{x}|\mathbf{U}\mathbf{y}\rangle = \langle \mathbf{x}|\mathbf{y}\rangle$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$ and by Theorem 4, $\mathbf{U}$ is unitary. This completes the proof. ■

Theorems and references

Fact 1. For an arbitrary vector $u \in \mathbb{C}^n$ and some constant c, we have that

$$\|c \cdot u\|_2 = |c| \cdot \|u\|_2$$

Theorem 2. For complex vectors $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$, we have that

$$\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$$

Proof:

Let $\mathbf{u} = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}$ and $\mathbf{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$. Then we have that

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} \overline{u_i} v_i = \overline{\sum_{i=1}^{n} u_i \overline{v}_i} = \overline{\sum_{i=1}^{n} \overline{v}_i u_i} = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$$

This completes the proof. ■

Observation. *For any complex number $z \in \mathbb{C}$, we denote the real part of z by $\Re(z)$, and we have that $z + \overline{z} = 2\Re(z)$, where $\overline{z}$ denotes the complex conjugate of z.*

Proof:

Let $z = a + bi$ for some $a, b \in \mathbb{R}$. Then we have that

$$z + \overline{z} = (a + bi) + (a - bi) = 2a = 2\Re(z)$$

as desired. ■

Theorem 3. For a complex number $z \in \mathbb{C}$ where $z = a + ib$ for some $a, b \in \mathbb{R}$,

$$\Re(z) \leq |z|$$

Proof:

The modulus for a complex number $z = a + ib$ is defined as $|z| = \sqrt{a^2 + b^2}$ and the real part of z is defined as $\Re(z) = a$. Note that since $a, b \in \mathbb{R}$, we have that $b^2 \geq 0$ and therefore

$$|z| = \sqrt{a^2 + b^2} \geq \sqrt{a^2 + 0} = \sqrt{a^2} = |a| \geq a = \Re(z)$$

thereby settling the proof. ■

Theorem 4. Let $\mathbf{U} \in \mathbb{C}^{n\times n}$. Then $\mathbf{U}$ is unitary if and only if $\mathbf{U}$ preserves inner products, i.e. for all $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$, we have that

$$\langle \mathbf{Uu}, \mathbf{Uv} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle$$

Proof:

$\Longrightarrow$: Let $\mathbf{U}$ be unitary. Given some arbitrary vectors $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$, using the definition of the adjoint yields

$$\langle \mathbf{Uu}, \mathbf{Uv} \rangle = \langle \mathbf{U}^\dagger \mathbf{Uu}, \mathbf{v} \rangle = \langle \mathbf{Iu}, \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle$$

$\Longleftarrow$: Let $\mathbf{U}$ be such that it preserves inner products. Then for all $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$, we have that

$$\langle \mathbf{U}^\dagger \mathbf{Uu}, \mathbf{v} \rangle = \langle \mathbf{Uu}, \mathbf{Uv} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle$$

Pick $\mathbf{u} = \mathbf{e}_i$ and $\mathbf{v} = \mathbf{e}_j$ for $i, j \in \{1, \ldots, n\}$. Then we have that

$$\mathbf{U}^\dagger \mathbf{U}_{i,j} = \langle \mathbf{U}^\dagger \mathbf{U}\mathbf{e}_i, \mathbf{e}_j \rangle = \langle \mathbf{U}\mathbf{e}_i, \mathbf{U}\mathbf{e}_j \rangle = \langle \mathbf{e}_i, \mathbf{e}_j \rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \implies \mathbf{U}^\dagger \mathbf{U} = \mathbf{I}$$

This completes the proof. ■

Theorem 5. If a linear transformation $T : \mathbb{C}^n \to \mathbb{C}^n$ maps any unit vector $\mathbf{v}$ to another unit vector $\mathbf{w}$, then T more generally preserves norms.

Proof:

Let $\mathbf{x} \in \mathbb{C}^n$ be an arbitrary vector and $T : \mathbb{C}^n \to \mathbb{C}^n$ be a linear transformation such that $T(\mathbf{v}) = \mathbf{Av}$ for all $\mathbf{v} \in \mathbb{C}^n$ where $\mathbf{A}$ is the matrix representation of the transformation. Define $c = \|\mathbf{x}\|_2 \in \mathbb{R}^+$. Then we have that

$$\|\mathbf{Ax}\|_2 = \left\| \frac{\mathbf{Ax}}{c} \cdot c \right\| = c \cdot \left\| \mathbf{A}\left(\frac{\mathbf{x}}{c}\right) \right\| = c \cdot \|\mathbf{x}/c\|_2 = c \cdot c^{-1} \|\mathbf{x}\|_2 = \|\mathbf{x}\|_2 \qquad \text{via Fact 1}$$

where we made use of the fact that $\mathbf{x}/\|\mathbf{x}\|_2$ is a unit vector for all $\mathbf{x} \in \mathbb{C}^n$ and therefore $\|\mathbf{A}(\mathbf{x}/\|\mathbf{x}\|)\|_2 = \|\mathbf{x}/\|\mathbf{x}\|\|_2$. This completes the proof. ■

Observation. *For a complex number $z \in \mathbb{C}$, we have that*

$$z - \overline{z} = 2i \cdot \Im(z).$$

Proof:

For a complex number $z = a + ib$, its complex conjugate is denoted by $\overline{z} = a - ib$.

$$z - \overline{z} = (a + ib) - (a - ib) = (a + ib) - a + ib = 2i \cdot \Im(z)$$

as desired. ■

Theorem 6. Let $V \subset \mathbb{C}^d$ be a vector space over $\mathbb{C}$ that is spanned by the set $\mathcal{B} = \{\mathbf{b_1}, \ldots, \mathbf{b_k}\}$. If $\mathcal{U} = \{\mathbf{u_0}, \ldots, \mathbf{u_m}\}$ is any linearly independent subset of $\mathbb{C}$, then $m \leq k$.

Proof:

Since $\mathcal{B}$ is a spanning set for $\mathbb{C}^n$; we can write down $\mathbf{u}_0$ (and in fact any of the $\mathbf{u}_i$'s) as a linear combination of the vectors in $\mathcal{B}$. Therefore the set $\tilde{\mathbf{U}} = \{\mathbf{u}_0, \mathbf{b}_1, \ldots, \mathbf{b}_k\}$ is linearly dependent. Since $\tilde{\mathbf{U}}$ is linearly dependent; there exist $\alpha_0, \alpha_1, \ldots, \alpha_k \in \mathbb{C}$ not all zero such that

$$\alpha_0\mathbf{u}_0 + \alpha_1\mathbf{b}_1 + \cdots + \alpha_k\mathbf{b}_k = \mathbf{0}$$

Let ℓ be the largest index such that $\alpha_\ell \neq 0$. Then $\alpha_t = 0$ for all $t > \ell$ and therefore

$$\alpha_0\mathbf{u}_0 + \alpha_1\mathbf{b}_1 + \cdots + \alpha_\ell\mathbf{b}_\ell = \mathbf{0} \implies \alpha_\ell\mathbf{u}_\ell = -\alpha_0\mathbf{u}_0 - \alpha_1\mathbf{b}_1 - \cdots - \alpha_{\ell-1}\mathbf{b}_{\ell-1}$$

Since $\mathbb{C}$ is a field, α_0 admits an inverse and therefore

$$\mathbf{u}_\ell = -\alpha_0^{-1}\alpha_1\mathbf{u}_0 - \cdots - \alpha_0^{-1}\alpha_{\ell-1}\mathbf{b}_{\ell-1}$$

Therefore there exists an element that is a linear combination of the preceding elements in $\tilde{\mathbf{U}}$, say $\mathbf{b}_i$. If $\mathbf{b}_i$ is deleted from $\tilde{\mathbf{U}}$, then the remaining set still spans $\mathbb{C}^n$. In particular the element $\mathbf{u}_1$ can be expressed as a linear combination of the elements in the new set $\tilde{\mathbf{U}_1} = \tilde{\mathbf{U}} \setminus \{\mathbf{b}_i\}$. Therefore the set $\{\mathbf{u}_0, \mathbf{u}_1, \mathbf{b}_1, \ldots, \mathbf{b}_{i-1}, \mathbf{b}_{i+1}, \ldots \mathbf{b}_k\}$ is linearly independent. Once again one of the elements in $\tilde{\mathbf{U}_1}$ can be expressed as a linear combination of the preceding elements. This element can't be one of the $\mathbf{u}_i$'s since this contradicts the linear independence of $\mathcal{U}$. Therefore the element must be one of the $\mathbf{b}_i$'s. We can continue this process where we add a $\mathbf{u}_i$ and remove a $\mathbf{b}_i$ at each step. If $m > k$, then we will run out of $\mathbf{b}_i$'s to remove before all the $\mathbf{u}_i$'s are added which would result in a set of the form $\{\mathbf{u}_0, \ldots, \mathbf{u}_k\}$ which spans $\mathbb{C}^n$ and is linearly independent. This implies that $\mathbf{u}_m$ is a linear combination of the preceding elements thereby contradicting the linear independence of $\mathcal{U}$. Therefore $m \leq k$. ■

Theorem 7. For eigenvectors $\mathbf{v}_1$ and $\mathbf{v}_2$ of a Hermitian matrix $\mathbf{H}$ with distinct eigenvalues λ_1 and λ_2, we have that $\langle \mathbf{v}_1 | \mathbf{v}_2 \rangle = 0$.

Proof:

This one is a classic. Let us assume the usual exposition one incurs with an eigenvalue problem. We have that

$$\mathbf{H}\mathbf{v}_1 = \lambda_1\mathbf{v}_1 \implies \langle \mathbf{v}_2 | \mathbf{H} | \mathbf{v}_1 \rangle = \lambda_1 \langle \mathbf{v}_2 | \mathbf{v}_1 \rangle$$

$$\lambda_2 \langle \mathbf{v}_2 | \mathbf{v}_1 \rangle = \lambda_1 \langle \mathbf{v}_2 | \mathbf{v}_1 \rangle \implies (\lambda_2 - \lambda_1) \langle \mathbf{v}_2 | \mathbf{v}_1 \rangle = 0 \qquad \text{since } \overline{\lambda_2} = \lambda_2$$

Since $\lambda_1 \neq \lambda_2$, the desired result follows. ■