MA 399 Intro to Quantum Information Theory

Hayden Roszell

April 30, 2022

Abstract

Modern trends seem to conclude that the future of information processing will be increasingly completed using quantum computers. As opposed to their classical counterparts, quantum computers operate according to quantum mechanics. Quantum information theory discusses the possibilities and limitations of information representation and communication over quantum channels. This paper gives an overview of the inner workings of the math used by quantum information theory, and provides examples of the benefits over classical information theory.

Contents

1 Intro to Vector Spaces

Let's jump right in. This section is an abbreviation of the introduction to linear algebra session.

A vector space is a group of objects (vectors) which may be added together and multiplied by compatible scalars from $\mathbb{R}$ or $\mathbb{C}$. In this class, we primarily care about vector spaces $\mathbb{C}^n$ over $\mathbb{C}$ and $\mathbb{R}^n$ over $\mathbb{R}$. Recall that $\mathbb{C}$ is the scalar field of complex numbers $a + bi$, where multiplication is defined by the rule $i^2 = -1$, and is equipped with:

(a) a complex conjugation operation – $\overline{a + bi} = (a + bi)^* = a - bi$ and

(b) a size function called the **modulus** – $|a + bi| = \sqrt{a^2 + b^2}$.

Note that the modulus is similar to magnitude.
To work with complex numbers, it's useful to have an understanding of the basic operations.

(a) To add/subtract complex numbers, add/subtract the corresponding real/imaginary parts. For example – $(a + bi) + (c + di) = (a + c) + (b + d)i$

(b) To multiply/divide complex numbers, multiply both parts of the complex number by the real number. For example – $(a + bi) * (c + di) = ac + adi + bcj - bd = (ac - bd) + (ad + bc)i$. This form will be useful for the duration of the class.

1.1 Representing Vectors in Complex Spaces

As mentioned, this class primarily works in complex number spaces. For this reason, having useful tools for representing vectors in these abstract spaces is useful. Vectors are represented in **bra-ket** notation, where *bra* represents a *row* vector, and *ket* represents a *column* vector.

Definition 1.1 If $|v\rangle \in \mathbb{C}^n$ is a *ket* vector which consists of n complex numbers,

$$|v\rangle = \begin{bmatrix} v_1 \\ v_2 \\ ... \\ v_n \end{bmatrix} \text{ for } v_1, v_2, ..., v_n \in \mathbb{C} \tag{1.1}$$

♦

Definition 1.2 If $\langle v| \in \mathbb{C}^n$ is a *bra* vector which consists of n complex numbers,

$$\langle v| = \begin{bmatrix} v_1 & v_2 & ... & v_n \end{bmatrix} \text{ for } v_1, v_2, ..., v_n \in \mathbb{C} \tag{1.2}$$

♦

Note that the the integer n in definitions 1.1 and 1.2 is called the **dimension** of the vector space $\mathbb{C}^n$.

Example 1.3 $\mathbb{C}^2$ is a 2-dimensional vector space over $\mathbb{C}$.

$$\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} \alpha \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \text{ Note: } \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \text{ 'fills up' } \mathbb{C}^2\text{; IE it represents all values contained within } \mathbb{C}^2$$

♦

1.2 Linear Combinations

A linear combination is a useful tool for this class which is the 'combination' or multiplication of each term in a set by constants, and then adding the result. The interesting property of linear combinations is that the result is still contained within the initial set.

Definition 1.4 A linear combination of $\{|v_1\rangle, ..., |v_n\rangle\} \subset \mathbb{C}^n$ is a single vector in the form $\lambda_1 |v_1\rangle + \lambda_2 |v_2\rangle + ... + \lambda_n |v_n\rangle$ for some $\lambda_1, \lambda_2, ..., \lambda_k \in \mathbb{C}^n$. ♦

Remark 1.5 If $|w\rangle$ is a linear combination of $\{|v_1\rangle, ..., |v_n\rangle\} \subset \mathbb{C}^n$, we can say that it belongs to the **span** of the set of $\{|v_1\rangle, ..., |v_n\rangle\} \subset \mathbb{C}^n$. ♦

Example 1.6 Create a linear combination of $|v_1\rangle = \begin{bmatrix} i \\ 2 \end{bmatrix}, |v_2\rangle = \begin{bmatrix} -1 \\ i+1 \end{bmatrix}$

$$\begin{aligned} &(\textit{foil}) \\ (3+2i)\begin{bmatrix} i \\ 2 \end{bmatrix} &+ (2+i)\begin{bmatrix} -1 \\ i+1 \end{bmatrix} \\ &(\textit{add}) \\ = \begin{bmatrix} 3i-2 \\ 6+4i \end{bmatrix} &+ \begin{bmatrix} -2-i \\ 3i+1 \end{bmatrix} \\ = \begin{bmatrix} 2i-4 \\ 7i+7 \end{bmatrix} &= |w\rangle \ \textit{spans} \ \{|v_1\rangle, |v_2\rangle\} \end{aligned}$$

♦

1.3 Linear Independence

Another important concept is that of a set being *linearly independent.* Being linearly independent essentially means that every piece of 'information' given by a set of vectors adds some sort of new information/perspective on the problem.

Remark 1.7 Two vectors are **linearly independent** as long as they are not *parallel.* ♦

A good way of looking at this is that a system that is not linearly independent has more than one element that is some offset of the same constant. These elements are not giving new perspective, because they give the same information.

Definition 1.8 A set of vectors $\{|v_1\rangle, \ldots, |v_v\rangle\}$ is linearly independent if no vector is a linear combination of any other vectors. Algebraically, if $\lambda_1 |v_1\rangle + \lambda_2 |v_2\rangle + ... + \lambda_n |v_k\rangle = |0\rangle$, then $\lambda_1 = \lambda_2 = \lambda_k = 0$ ♦

The only way that the zero vector ($|0\rangle$) can be possible is if the complex constants (λ) are all the same, *and* zero.

Theorem 1.9 *If a set of k vectors in $\mathbb{C}^n$ is linearly independent, then $k \leq n$. Equivalently, if you have a set of k vectors in $\mathbb{C}^n$ such that $k > n$, then the set is linearly dependent.*

This theorem is important because it establishes the notion that a set can't contain more vectors than the space allows for. Said differently, the dimension of M is the number of vectors contained within that can be linearly independent.

1.4 Basis

Theorem 1.10 *A **basis** of a subspace $M \subseteq \mathbb{C}^n$ is a set of vectors such that*

1. *S is linearly independent*

2. Span(S) = M $\Longrightarrow$ S Spans M

It follows that the standard basis of $\mathbb{C}^n$ is $\begin{bmatrix}1\\0\\0\\...\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\...\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\...\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\...\\1\end{bmatrix}$

1.5 Inner Products

Recall that $|v\rangle$ is a column vector and $\langle v|$ is a row vector. Before talking about inner products, we must define operations that help the inner product process.

Remark 1.11 $(\mathbb{C}^n)^*$ is the *dual space* of $\mathbb{C}^n$. ♦

The dual space is the space of all row vectors. This is useful for the next definition, which is critical in completing inner products.

Definition 1.12 We equip $\mathbb{C}^n$ with an "involution" (*conjugate transpose*) operation:

$$\dagger : \mathbb{C}^n \longrightarrow (\mathbb{C}^n)^* \text{ given by } \begin{bmatrix}x_1\\...\\x_n\end{bmatrix} = \begin{bmatrix}x_1^* & ... & x_n^*\end{bmatrix} \text{ given a } |v\rangle \in \mathbb{C}^n,\ \langle v| = |v\rangle^\dagger$$ ♦

A quick example of this operation is helpful to explain the significance of these definitions.

Example 1.13 Given $|v\rangle = \begin{bmatrix}7\\8i\\\pi+3i\\0\end{bmatrix} \in \mathbb{C}^4$, find $|v\rangle^\dagger$

Take the complex conjugate of each entry
$\langle v| = \begin{bmatrix}7 & -8i & \pi - 3i & 0\end{bmatrix}$ ♦

Now, we can talk about inner products. Of primary importance for this section, the inner product can determine if two vectors are orthogonal, and operates the same as a dot product on $\mathbb{R}^n$.

Definition 1.14 Given $|v\rangle, |w\rangle \in \mathbb{C}^n$, the **inner product** of $|v\rangle$ and $|w\rangle$ is $\langle w|v\rangle = \langle w|^\dagger \cdot |v\rangle$ ♦

Remark 1.15 The inner product on $\mathbb{R}^n$ is the usual dot product. ♦

The following is a simple example showing the inner product on simple vectors in $\mathbb{R}^3$.

Example 1.16 Given $|v\rangle = \begin{bmatrix}1\\1\\3\end{bmatrix}, |w\rangle = \begin{bmatrix}5\\-2\\1\end{bmatrix} \in \mathbb{R}^3$, find $\langle w|v\rangle$

Perform a complex conjugate on $|w\rangle$ (In $\mathbb{R}^3$, this is the same as flipping $nx1$ to $1xn$)

$$\langle w|v\rangle = \begin{bmatrix}5 & -2 & 1\end{bmatrix} \cdot \begin{bmatrix}1\\1\\3\end{bmatrix} = (5*1) + (-2*1) + (1*3) = 6$$ ♦

Now, the following example shows the inner product on two simple vectors in $\mathbb{C}^2$.

Example 1.17 Given $|v\rangle = \begin{bmatrix} i \\ 1 \end{bmatrix}, |w\rangle = \begin{bmatrix} i \\ -1 \end{bmatrix} \in \mathbb{C}^2$, find $\langle w \mid v\rangle$

$$\langle w \mid v\rangle = \begin{bmatrix} -i & -1 \end{bmatrix} \cdot \begin{bmatrix} i \\ 1 \end{bmatrix} = 1 + (-1 * 1) = 0 \qquad \blacklozenge$$

Recall from calculus III that the dot product of two vectors can give us insight on orthogonality. In the case of example 1.17, the inner product of $\langle w|v\rangle$ was zero. This tells us that the two vectors are orthogonal.

Definition 1.18 The **norm** (similar to magnitude) of $|v\rangle \in \mathbb{C}^n$ is $\||v\rangle\| := \sqrt{\langle v \mid v\rangle}$ ♦

Example 1.19 $|v\rangle = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \in \mathbb{R}^2 \longrightarrow ||\,|v\rangle\,|| = \sqrt{1^2 + 1^2} = \sqrt{2}$ ♦

Remark 1.20

- $|v\rangle \in \mathbb{C}^n$ with $||\,|v\rangle\,|| = 1$ is called a unit vector
- Unit vectors in $\mathbb{C}^n$ represent a *quantum state*
- An important property of a norm is the *triangle inequality* $\longrightarrow \||v\rangle + |w\rangle\| \leq \||v\rangle\| + \||w\rangle\|$ ♦

Definition 1.21 A set of non-zero vectors $S = \{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\} \leq \mathbb{C}^n$ is called an orthogonal set if $\langle v_i \mid w_j\rangle = 0$ if $i \neq j$ ♦

Theorem 1.22 *If $S = \{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$ is an orthogonal set of non-zero vectors in $\mathbb{C}^n$, then S is linearly independent.*

Proof. Let $c_1, ..., c_k \in \mathbb{C}$ such that $c_1 |v_1\rangle + ... + c_k |v_k\rangle = |0\rangle$.
Goal: show that $c_1 = c_2 = c_k = 0 \longrightarrow$ linearly independent using S is orthogonal
Additionally, let
$j \in 1, ..., k$.
Then,
$\langle v_j| (c_1 |v_1\rangle + ... + c_k) = \langle v_j \mid 0\rangle$
$\longrightarrow c_1 \langle v_j \mid v_1\rangle + ... + c_k \langle v_j \mid v_k\rangle$
$c_j \langle v_j \mid v_j\rangle =$ (v_j *is the only component allowed to have magnitude*)
Thus, $c_j = 0$ since $|v_j\rangle \neq |0\rangle$
Note: Since j was arbitrary, $c_1 = c_2 = ... = c_k = 0$. Hence, S is linearly independent. ■

Remark 1.23 S is an orthonormal basis if:

- S is an orthonormal set if n unit vectors
- $\text{Span}(S) = \mathbb{C}^n$ ♦

1.6 Projections

Definition 1.24 Define $|f_i\rangle \langle f_i|$ to be the **projection** operator onto Span $(|f_i\rangle)$ ♦

Theorem 1.25 *Let* $\beta = \{|f_1\rangle, |f_2\rangle, \ldots, |f_n\rangle\}$ *be an orthonormal basis for* $\mathbb{C}^n$. *Then, any* $|x\rangle = c_1 |f_1\rangle + ... + c_n |f_n\rangle = \langle f_1 \mid x\rangle |f_1\rangle + ... + \langle f_n \mid x\rangle |f_n\rangle$.

It follows that $\sum_{j=1}^{n} |f_j\rangle \langle f_j| = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$

Example 1.26 Let $|f_1\rangle = \frac{-2}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, |x\rangle = \begin{bmatrix} -2 \\ 1 \end{bmatrix}$.
$|x_{|}\rangle = \langle f_1 \mid x\rangle |f_1\rangle$
$P_1(|x\rangle) = |f_1\rangle \langle f_1 \mid x\rangle$ ♦

In the above example, $|x_{|}\rangle$ is the projection of x onto f_1 in the direction of f_1. Note that the projection operation is similar to *comp* from calculus III. Now, let's look at some properties of the projection operator.

Proposition 1.27 *Let* $\beta = \{|f_1\rangle, |f_2\rangle, \ldots, |f_n\rangle\}$ *be an orthonormal basis for* $\mathbb{C}^n$. *Then,* $\{P_1, P_2, P_n\}$ *is a set of* $n \times n$ *matrices such that*

1. $P_i(|v\rangle) \in$ *Span* $(|f_i\rangle)$
2. $|v\rangle - P_i(|v\rangle)$ *is orthogonal to* $|f_i\rangle$
3. $P_i^2 = P_i * P_i = P_i$
4. $P_i P_j = 0$ *when* $i \neq \jmath$, *and* $P_i^\dagger = P_i$
5. $\sum_{i=1}^{n} P_i = I_n$ *IE the sum of* P*'s gives us the identity matrix.*

Projection operators make it easy for us to find c_1, c_2, c_n for $|x\rangle = c_1 |f_1\rangle + ... + c_k |f_k\rangle$ when $\{|f_1\rangle, |f_2\rangle, \ldots, |f_n\rangle\}$ is an orthonormal set. Side note, in quantum land, P_i's are how we measure the probability that $|x\rangle$ is actually in $|f_i\rangle$.

1.7 Gram-Schmidt

Let $\beta = \{|b_1\rangle, |b_2\rangle, \ldots, |b_n\rangle\}$ be a basis for $\mathbb{C}^n$

- Linearly independent
- Span $(\beta) = \mathbb{C}^n$ (IE no redundancy)

Goal: Turn β into an orthonormal basis, $\{|f_1\rangle, |f_2\rangle, \ldots, |f_n\rangle\}$

1. First, make an orthogonal basis.
   $|f_{i+1}\rangle := |b_{i+1}\rangle - (\sum_{j=1} i \frac{\langle f_j | b_{i+1}\rangle}{\langle f_j | f_j\rangle} |f_j\rangle)$
2. Then, make an orthonormal basis by normalizing the resultant $(|f\rangle)$ vectors.
   For each $|f\rangle$, $|f\rangle = \frac{1}{\||f\rangle\|} |f\rangle$

1.8 Exercise 1

Consider $S = |v_1\rangle, |v_2\rangle, |v_3\rangle$ **where** $|v_1\rangle = \begin{bmatrix} 1 \\ -1 \end{bmatrix}, |v_2\rangle = \begin{bmatrix} i \\ 1 \end{bmatrix}, |v_3\rangle = \begin{bmatrix} 0 \\ i \end{bmatrix}$

(a) **Give a linear combination of the vectors in** S**.**

$$\alpha \begin{bmatrix} 1 \\ -1 \end{bmatrix} + \beta \begin{bmatrix} i \\ 1 \end{bmatrix} + \gamma \begin{bmatrix} 0 \\ i \end{bmatrix} = |w\rangle$$

Note that the next problem asks to determine if a vector is in span(S). To 'kill two birds with one stone', try to find a linear combination that satisfies the question. To do this, assign values for α, β, and γ. Note that $1 + i = i + i$ (the top row), and $-1 + 1 = 0$. This allows us to set α and β to 1 and operate on γ.

$$i(x + yi) = 200 - i$$
$$xi - y \implies x = -1 \implies \gamma = -1i - 200$$

Now plug in values. $1 * \begin{bmatrix} 1 \\ -1 \end{bmatrix} + 1 * \begin{bmatrix} i \\ 1 \end{bmatrix} + (-200 - 1i) * \begin{bmatrix} 0 \\ i \end{bmatrix} = |w\rangle$

(b) **Determine if** $\begin{bmatrix} 1+i \\ 200 - i \end{bmatrix}$ **in Span(**S**)**

Start with where we left off in the last part.

$$1 * \begin{bmatrix} 1 \\ -1 \end{bmatrix} + 1 * \begin{bmatrix} i \\ 1 \end{bmatrix} + (-200 - 1i) * \begin{bmatrix} 0 \\ i \end{bmatrix} = \begin{bmatrix} 1+i \\ 200 - i \end{bmatrix}$$

$\begin{bmatrix} 1+i \\ 200 - i \end{bmatrix}$ *is* in Span(S) because there existed values α, β, and γ such that $|w\rangle$ of S is a possible outcome of S.

(c) **Describe Span(**S**) "geometrically"**

Span(S) can be thought of as every possible vector ($\alpha \begin{bmatrix} 1 \\ -1 \end{bmatrix} + \beta \begin{bmatrix} i \\ 1 \end{bmatrix} + \gamma \begin{bmatrix} 0 \\ i \end{bmatrix}$) contained within $\mathbb{C}^2$

1.9 Exercise 2

Find the condition under which the following two vectors are linearly independent:

$$|v_1\rangle = \begin{bmatrix} x \\ y \\ 3 \end{bmatrix}, |v_2\rangle = \begin{bmatrix} 2 \\ x - y \\ 1 \end{bmatrix} \in \mathbb{R}^3$$

Multiply $|v_2\rangle$ by a scalar that makes $|v_1\rangle$ and $|v_2\rangle$ *not* linearly independent. This way, we can build a contradiction.

$$|v_1\rangle = \begin{bmatrix} x \\ y \\ 3 \end{bmatrix} = 3 * |v_2\rangle = \begin{bmatrix} 2 \\ x-y \\ 1 \end{bmatrix}$$
$$\begin{bmatrix} x \\ y \\ 3 \end{bmatrix} = \begin{bmatrix} 6 \\ 3*(x-y) \\ 3 \end{bmatrix}$$

It can be seen that in this case, $\implies x = 6$ and $y = 4.5$.
Therefore, as long as $x \neq 6$ and $y \neq 4.5$, $|v_1\rangle$ and $|v_2\rangle$ are linearly independent.

1.10 Exercise 3

Show that the set formed by the following vectors is a basis for $\mathbb{C}^3$

$$|v_1\rangle = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, |v_2\rangle = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, |v_3\rangle = \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}$$

Recall that for the vectors to be a basis for $\mathbb{C}^3$, they must be linearly independent and must span $\mathbb{C}^3$ (every vector must give additional information, IE no redundancy). To show that these vectors are linearly independent, we must use 1.4. Start by multiplying, each vector by some constant, and solving for them. In this case I put them in an augmented matrix.

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 1 & -1 & 0 \end{bmatrix} \longrightarrow (R_2 - R_3) \longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 1 & -1 & 0 \end{bmatrix} \longrightarrow (R_3 - R_1) \longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & 0 \end{bmatrix}$$
$$\longrightarrow (-1R_2 - \tfrac{1}{2}R_3) \longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Since the resultant matrix is row equivalent to the identity, it is invertible and therefore must form a basis for $\mathbb{C}^3$.

1.11 Exercise 4

Let $|x\rangle = \begin{bmatrix} 1 \\ i \\ 2+i \end{bmatrix}$, $|y\rangle = \begin{bmatrix} 2-i \\ 1 \\ 2+i \end{bmatrix}$, $|z\rangle = \frac{\sqrt{2+\sqrt{5}}}{2+\sqrt{5}} |x\rangle$.

1. **Find $\| \, |x\rangle \, \|$.**
   $\| \, |x\rangle \, \| = \sqrt{1^2 + i^2 + (2+i)^2} = \sqrt{1 - 1 + (2+i)^2} = 2 + i$

2. **Find $\langle x \mid y \rangle$**
   $$\langle x \mid y \rangle = \langle x|^{\dagger} \cdot |y\rangle = \begin{bmatrix} 1 & -i & 2-i \end{bmatrix} \begin{bmatrix} 2-i \\ 1 \\ 2+i \end{bmatrix} = 2 - i - i + 5 = 8 - 5i$$

3. **Find $\| \, |z\rangle \, \|$**
   $$\| \, |z\rangle \, \| = \frac{\sqrt{2+\sqrt{5}}}{2+\sqrt{5}} \begin{bmatrix} 1 \\ i \\ 2+i \end{bmatrix} = (2+i) \cdot \frac{\sqrt{2+\sqrt{5}}}{2+\sqrt{5}}$$

1.12 Exercise 7

Let $\beta = \{|b_1\rangle, |b_2\rangle\}$, where $|b_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, |b_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$

(a) Show that β is an orthonormal basis for $\mathbb{C}^2$

(i) Show that they're orthogonal

$$\langle w \mid v\rangle = \langle w|^{\dagger} \cdot |v\rangle$$

$$\tfrac{1}{\sqrt{2}}(\begin{bmatrix}1 & 1\end{bmatrix}\begin{bmatrix}1\\-1\end{bmatrix}$$

$$= \tfrac{1}{\sqrt{2}}((1*1)+(1*-1)) = 0 \longleftarrow \text{Recall that if the inner product is zero, the vectors are orthogonal}$$

(ii) Determine if $|b_1\rangle$ and $|b_2\rangle$ are unit vectors

$$\tfrac{1}{\sqrt{2}}\sqrt{1^2+1^2} = \tfrac{\sqrt{2}}{\sqrt{2}} = 1 \longleftarrow \text{Unit vector}$$

Therefore, β is an orthonormal basis.

(b) Find the coordinates (or components) of $|x\rangle = \begin{bmatrix}-2\\1\end{bmatrix}$ relative to β. IE find the scalars $c_1, c_2 \in \mathbb{C}$ such that $c_1|b_1\rangle + c_2|b_2\rangle = |x\rangle$.

(i) Multiply both sides by $\langle b_1|$

$$\langle b_1|(c_1|b_1\rangle + c_2|b_2\rangle) = \langle b_1 \mid x\rangle$$

$$c_1\langle b_1 \mid b_1\rangle + c_2\langle b_1 \mid b_2\rangle = c_1 * 1 + c_2 * 0 = c_1$$

Note that inner product of itself is parallel, and since β is an orthonormal basis, $\langle b_1 \mid b_2\rangle = 1$ (IE they're orthogonal).

$$c_1 = \langle b_1 \mid x\rangle$$

$$c_1 = \tfrac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\end{bmatrix}\begin{bmatrix}-2\\1\end{bmatrix} \longrightarrow = \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}-2\\1\end{bmatrix}$$

$$\tfrac{-2}{\sqrt{2}} + \tfrac{1}{\sqrt{2}} = \tfrac{-1}{\sqrt{2}}$$

(ii) Multiply both sides by $\langle b_2|$

$$\langle b_2|(c_1|b_1\rangle + c_2|b_2\rangle) = \langle b_2 \mid x\rangle$$

$$c_1\langle b_2 \mid b_1\rangle + c_2\langle b_2 \mid b_2\rangle = c_1 * 0 + c_2 * 1 = c_2$$

$$c_2 = \langle b_2 \mid x\rangle$$

$$c_2 = \tfrac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\end{bmatrix}\begin{bmatrix}-2\\1\end{bmatrix} \longrightarrow = \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}-2\\1\end{bmatrix}$$

$$\tfrac{-2}{\sqrt{2}} + \tfrac{-1}{\sqrt{2}} = \tfrac{-3}{\sqrt{2}}$$

Therefore, $c_1 = \frac{-1}{\sqrt{2}}$ and $c_2 = \frac{-3}{\sqrt{2}}$ when $|x\rangle = \begin{bmatrix}-2\\1\end{bmatrix}$.

1.13 Exercise 8

Given $S = \} \left|v_1\right\rangle = \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix}, \left|v_2\right\rangle = \begin{bmatrix} 2 \\ -1 \\ 2 \end{bmatrix}, \left|v_3\right\rangle = \begin{bmatrix} 3 \\ 0 \\ 3 \end{bmatrix} \{$, turn S into an orthonormal basis for $\text{Span}\,(S) = \mathbb{R}^3$.

1. Find $\left|f_1\right\rangle$ $\left\|\left|v_1\right\rangle\right\| = 3$

   $\longrightarrow \left|f_1\right\rangle = \frac{1}{3} \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix}$

2. Find $\left|f_2\right\rangle$

$$\left|f_2\right\rangle = \left|v_2\right\rangle - \left(\frac{\langle v_1|v_2\rangle}{\langle v_1|v_1\rangle} \left|v_1\right\rangle\right)$$

$$\begin{bmatrix} 2 \\ -1 \\ 2 \end{bmatrix} - \left[\begin{bmatrix} -1 & 2 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ -1 \\ 2 \end{bmatrix}\right] = \begin{bmatrix} 2 \\ -1 \\ 2 \end{bmatrix} - \left|0\right\rangle$$

$$\left|f_2\right\rangle = \frac{1}{3} \begin{bmatrix} 2 \\ -1 \\ 2 \end{bmatrix}$$

3. Find $\left|f_3\right\rangle$ $\left|f_3\right\rangle = \left|v_3\right\rangle - \left[\left(\frac{\langle v_1|v_3\rangle}{\langle v_1|v_1\rangle} \left|v_1\right\rangle\right) + \left(\frac{\langle v_2|v_3\rangle}{\langle v_2|v_2\rangle} \left|v_2\right\rangle\right)\right]$

$$= \begin{bmatrix} 3 \\ 0 \\ 3 \end{bmatrix} - \left[\left(\frac{\begin{bmatrix} -1 & 2 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \\ 3 \end{bmatrix}}{\begin{bmatrix} -1 & 2 & 2 \end{bmatrix} \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix}}\right) + \left(\frac{\begin{bmatrix} 2 & -1 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \\ 3 \end{bmatrix}}{\begin{bmatrix} 2 & -1 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ -1 \\ 2 \end{bmatrix}}\right)\right]$$

$$= \begin{bmatrix} 3 \\ 0 \\ 3 \end{bmatrix} - \left(\begin{bmatrix} \frac{-1}{3} \\ \frac{2}{3} \\ \frac{2}{3} \end{bmatrix} + \begin{bmatrix} \frac{8}{3} \\ \frac{-4}{3} \\ \frac{8}{3} \end{bmatrix}\right) = \begin{bmatrix} \frac{2}{3} \\ \frac{2}{3} \\ \frac{-1}{3} \end{bmatrix}$$

   $\|f_3\| = 1$ *already normalized*

Therefore, $\left|f_{final}\right\rangle = \frac{1}{3} \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix}, \frac{1}{3} \begin{bmatrix} 2 \\ -1 \\ 2 \end{bmatrix}, \begin{bmatrix} \frac{2}{3} \\ \frac{2}{3} \\ \frac{-1}{3} \end{bmatrix}$

1.14 Exercise 9

Use the Gram-Schmidt Process to produce an orthonormal basis β for $M = \text{Span}\left(\left\{\left|v_1\right\rangle, \left|v_2\right\rangle\right\}\right)$ where $\left|v_1\right\rangle = \begin{bmatrix} 1 \\ i \\ 1 \end{bmatrix}$, $\left|v_2\right\rangle = \begin{bmatrix} 3 \\ 1 \\ i \end{bmatrix}$.

Step 1:

$|f_1\rangle = |b_1\rangle = \begin{bmatrix} 1 \\ i \\ 1 \end{bmatrix}$

Step 2:

$|f_2\rangle = |b_2\rangle - \frac{\langle f_1|b_2\rangle}{\langle f_1|f_1\rangle} |f_1\rangle = \begin{bmatrix} 3 \\ 1 \\ i \end{bmatrix} - \frac{3}{3} \begin{bmatrix} 1 \\ i \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1-i \\ -1+i \end{bmatrix}$

Step 3:

$\| \, |f_1\rangle \, \| = 1$, and $\| \, |f_2\rangle \, \| = \sqrt{4 + (1-i)^2 + (-1+i)^2} = \sqrt{4-4i} = 2\sqrt{1-i}$

Therefore, $|f_1\rangle = \sqrt{3} \begin{bmatrix} 1 \\ i \\ 1 \end{bmatrix}$ and $|f_2\rangle = 2\sqrt{2} \begin{bmatrix} 2 \\ 1-i \\ -1+i \end{bmatrix}$.

2 Matrices and Linear Transformations

Understanding matrices and linear transformations will be critical when it comes time to talk about quantum mechanics. Specifically, this section will discuss matrix properties and operations, as well as special theorems that will help us to work with more complex systems.

2.1 Intro to Matrices

Definition 2.1 A map $T : \mathbb{C}^n \longrightarrow \mathbb{C}^m$ is a linear transformation if:

1. $T(|v\rangle + |u\rangle = T(|u\rangle \mid |v\rangle)$
2. $T(C \mid V) = CT(|v\rangle) \forall \, |u\rangle \, , |v\rangle \, , C \in \mathbb{C}^n$ ♦

Note that every linear transformation arises from a matrix.

Definition 2.2 $M_{mn}(\mathbb{C})$ is a set of all $m \times n$ matrices with complex entries $M_N(\mathbb{C}) := M_{nm}(\mathbb{C})$ ♦

This is traditionally written as M_n or M_{mn}. M_{mn} is a vector space with usual scalar multiplication and matrix addition.

Example 2.3 Given $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \in M_2$, $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, find $2\omega_x - i\omega_y$

$$\begin{aligned} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} - i \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix} \end{aligned}$$ ♦

Note that $\sigma_x, \sigma_y, \sigma_z$ are called Pauli or 'spin' matrices.
I_n is called the identity matrix whose 0's are the standard basis for $\{|e_1\rangle \, , |e_2\rangle \, , \ldots , |e_n\rangle\} \in \mathbb{C}^n$.

IE: $I_N = \begin{bmatrix} 1 & 0 & 0 & ... & 0 \\ 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 1 \end{bmatrix}$ M_N has well-defined multiplication of matrices.

In general, if $A \in M_{mn}$, $B = m_{nk}$, $A = (a_{ij})^{mn}_{j=1j=1}$, $B = (b_{rs})_{r=1,2=1}$. Additionally, the matrix $AB = \begin{bmatrix} A\,|b_1\rangle & ... & B\,|b_k\rangle \end{bmatrix} = (C_{pq})$ where C_{pq} is the dot product of the pth row of A against the qth column of B.

Here are some nice facts that will help us in further examples:

1. $AB = \begin{bmatrix} \langle a_1|\, B \\ ... \\ \langle a_m|\, B \end{bmatrix}$ where $\{|a_1\rangle, |a_2\rangle, \ldots, |a_n\rangle\}$ are the rows of A.

2. $AB = \sum_{i=1}^{n} |a_j\rangle \langle b_j|$ (IE ”the columns of A against the rows of B”)

It's useful to know some matrix operations to proceed. In general, $\begin{bmatrix} |a_1\rangle & ... & |a_n\rangle \end{bmatrix} \begin{bmatrix} d_1 & & 0 \\ & ... & \\ 0 & & d_n \end{bmatrix} = \begin{bmatrix} d_1\,|a_1\rangle & ... & d_n\,|a_n\rangle \end{bmatrix}$. Here's an example:

Example 2.4 $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 0 & -3i \\ i & 0 \end{bmatrix}$ ♦

2.2 Eigenvalues and Eigenvectors

Definition 2.5 An **eigenvalue** for $A \in M_n$ is a complex number $\lambda \in \mathbb{C}^n$ such that there is a non zero vector $|x\rangle \in \mathbb{C}^n$ satisfying $A\,|x\rangle = \lambda\,|x\rangle$. ♦

Definition 2.6 A matrix $A \in M_n$ is diagonalizable if:

1. There is a diagonal matrix D and an invertable matrix P such that $A = PDP^-1$.
2. There exists a basis for $\mathbb{C}^n$ consisting of eigenvectors for A ♦

Example 2.7 Consider $A \begin{bmatrix} I_2 & 0 \\ 0 & \sigma_y \end{bmatrix}$

First, let's get the eigenvalues and normalized vectors. Note that eigenvalues are the *roots* of the characteristic equation $det(A - \lambda I) = 0$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix} - \begin{bmatrix} \lambda & & & 0 \\ & \lambda & & \\ & & \lambda & \\ 0 & & & \lambda \end{bmatrix}$$

$$A - \lambda I = \begin{bmatrix} 1-\lambda & 0 & 0 & 0 \\ 0 & 1-\lambda & 0 & 0 \\ 0 & 0 & -\lambda & -i \\ 0 & 0 & i & \lambda \end{bmatrix} \longrightarrow det(A - \lambda I) = \begin{vmatrix} 1-\lambda & 0 & 0 & 0 \\ 0 & 1-\lambda & 0 & 0 \\ 0 & 0 & -\lambda & -i \\ 0 & 0 & i & \lambda \end{vmatrix}$$

$$= (1-\lambda)\begin{vmatrix} 1-\lambda & 0 & 0 \\ 0 & -\lambda & -i \\ 0 & i & \lambda \end{vmatrix} = (1-\lambda)\begin{bmatrix} 1-\lambda & \begin{bmatrix} -\lambda & -i \\ i & \lambda \end{bmatrix} & -0 & 0 \end{bmatrix}$$

$$= (1-\lambda)(1-\lambda)\begin{bmatrix} \lambda^2 & -1 \end{bmatrix} = 0$$

$$\lambda = 1, 1, 1, -1$$

These are our eigenvalues. Now, we need to find our eigenvectors

Note: $A\left|e_1\right\rangle = \left|e_1\right\rangle$ and $B\left|e_2\right\rangle = \left|e_2\right\rangle$.

$$A-(1)I = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -i \\ 0 & 0 & i & 1 \end{bmatrix} \xrightarrow{R_4+iR_3} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & i \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow[-1*R_1]{R_1\leftrightarrow R_3} = \begin{bmatrix} 0 & 0 & 1 & -i \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Therefore, our eigen vector is $\left|x\right\rangle = \begin{bmatrix} 0 \\ 0 \\ i \\ 1 \end{bmatrix}$.

Our normalized eigen vectors are $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 0 \\ i \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 0 \\ 1 \\ i \end{bmatrix} \right\}$ ♦

2.3 Matrix Classifications

Some, but not all matrices are diagonalizable; this property is highly desirable. Matrices are diagonalizable if and only if the eigenvalues form a basis.

1. Vectors must be self-adjoint (*hermitian*) IE $A \in M_n$ is **hermitian** if, for example, $A^\dagger = A$, $\sigma + \dagger_x = \sigma_x$, $\sigma + \dagger_y = sigma_y$, $\sigma + \dagger_z = \sigma_z$

2. As it turns out, *all* hermitian matricies (and in fact, all normal matrices too) are diagonalizable $\longleftrightarrow$ the eigenvectors for a basis (IE linearly independent and Span). Said differently, hermitian matrices are only hermitian matrices if their eigenvectors form an orthonormal basis (IE unit vector, norm, and Span). It's worth noting that the eigenvalues must be real for this to be the case.

3. A matrix in M_n is positive-semidefinite if for all $\left|x\right\rangle \in \mathbb{C}^n$, we have $\left\langle x\right| A \left|x\right\rangle \geq 0$

4. The following are equivalent:

   (a) $u \in M_n$ is unitary

   (b) $u^\dagger = u - 1$ (IE left *and* right inverse) $\longrightarrow u^{-1}u = uu^{-1}$

   (c) $uu^\dagger = I_n$ and $u^\dagger u = I_n$ (unitaries are normal, but not necessarily hermitian)

   (d) The columns of u form an orthonormal basis for $\mathbb{C}^n$

(e) $\forall |x\rangle, |y\rangle \in \mathbb{C}^n$, $\langle u \mid u\rangle = \langle x \mid y\rangle$. Think of this as a rotation of the entire matrix, such that the angle between the vectors are preserved. Related to calculus III, this operation gives us the angle.

Now, let's go over some examples of these properties in action.

Example 2.8 Example of a matrix that is *not* hermitian:

$$N = \begin{bmatrix} 2 & -i \\ -i & 2 \end{bmatrix} \longrightarrow N^\dagger = \begin{bmatrix} 2 & i \\ i & 2 \end{bmatrix}$$

Note: the columns of N are not orthogonal, so N is not unitary. ♦

Example 2.9 Example of a unitary matrix that's not hermitian:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \longrightarrow u^{-1} = u^\dagger = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$ ♦

Example 2.10 Recall that $\forall |x\rangle \in C^n$, $\langle x| A |x\rangle \geq 0$. Consider $A = |e_2\rangle \langle e_2|$ where $e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. This is positive semidefinite if:

proof Let $|x\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{C}^2$.

$\langle x| A |x\rangle = \begin{bmatrix} a^* & b^* \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$

$\begin{bmatrix} a^* & b^* \end{bmatrix} \begin{bmatrix} 0 \\ b \end{bmatrix} = 0 + b^* b =\mid b \mid^2 \geq 0$ ♦

2.4 Spectral Theorem for Normal Matrices

To perform decomposition of matrices, we can use the *spectral theorem for normal matrices*, and the fact that in general, $A \in M_n$ has a singular value decomposition. Note that both of these use eigenvectors of the given matrix. Note that $AB = BA$ doesn't always work for $A, B \in M_n$.

Theorem 2.11 *A matrix $N \in M_n$ is normal $\longleftrightarrow$ there is a unitary matrix $u = \begin{bmatrix} |u_1\rangle & \dots & |u_n\rangle \end{bmatrix}$ and a diagonalizable matrix $D = \begin{bmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$ such that $N = uDu^\dagger$*

Let's prove the forward case for this theorem. If you take $|u\rangle, ..., |u_n\rangle$ to be eigenvectors for N with respect to eigenvalues $\lambda_1, ..., \lambda_n$, then $u := [|u_1\rangle ... |u_n\rangle]$ is unitary and $D = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$. Therefore, $N = uDu^-1 = \sum_{j=1}^n \lambda_j |u_j\rangle \langle u_j|$. Note that $|u_j\rangle \langle u_j|$ is the projection P_j where $P_j |x\rangle$ is the projection of $|x\rangle$ onto $|u_j\rangle$. Now, let $|x\rangle = c_1 |u_1\rangle + ... + c_n |u_n\rangle$ for some $c_j \in \mathbb{C}^n$. Therefore,

$$
\begin{gathered}
N\left|x\right\rangle = \left(\sum_{j=1}^{n}\lambda_j\left|u_j\right\rangle\left\langle u_j\right|\right)\left(\sum_{i=1}^{n}c_i\left|u_i\right\rangle\right) \\
= \sum_{j=1}^{n}\sum_{i=1}^{n}c_i\lambda_j\left|u_j\right\rangle\left\langle u_j \mid u_i\right\rangle \\
= \sum_{j=1}^{n}c_j\lambda_j\left|u_j\right\rangle = D\left|x_u\right\rangle \\
\text{(fancy way of saying } Nu = uD\text{)}
\end{gathered}
$$

Let's do an example to illustrate this theorem.

Example 2.12 Consider $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Recall that a matrix $A \in M_n$ is

1. Normal if $A^\dagger A = AA^\dagger$, and
2. Hermitian if $A^\dagger = A$

Therefore, σ_x is Hermition because $\sigma_x^\dagger = \sigma_x$, so, $\sigma_x\sigma_x = \sigma_x\sigma_x^\dagger$ is normal. Thus, σ_x has a spectral decomposition. With this in mind, we're looking for $\sigma_x = uDu^\dagger$. First, let's find some eigenvalues.

$$
\begin{gathered}
\det\left(\sigma_x - \lambda I\right) = 0 \\
\left|\begin{bmatrix} -\lambda & 1 \\ 1 & -\lambda \end{bmatrix}\right| = 0 \\
\lambda^2 - 1 = 0 \\
\lambda \pm 1
\end{gathered}
$$

Now, use the eigenvalues to find eigenvectors.

$$
\begin{gathered}
\text{First, for } \lambda = 1,\ \sigma_x \begin{bmatrix} a \\ b \end{bmatrix} = 1 \begin{bmatrix} a \\ b \end{bmatrix}. \\
\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}. \\
\text{Therefore, } a = b \text{ and } \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \left|u_1\right\rangle \\
\text{Second, for } \lambda = -1,\ \sigma_x \begin{bmatrix} a \\ b \end{bmatrix} = -1 * \begin{bmatrix} a \\ b \end{bmatrix} \\
\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \\
\text{Therefore, } a = -b \text{ and } \tfrac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ 1 \end{bmatrix} = \left|u_2\right\rangle
\end{gathered}
$$

We now have $u = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$. Additionally, by theorem 2.11, $D = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Note that $u^\dagger = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$. Therefore,

$$
\begin{aligned}
\sigma_x &= \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \\
&= 1 * \left|u_1\right\rangle\left\langle u_1\right| + (-1) * \left|u_2\right\rangle\left\langle u_2\right| \\
&= 1 \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} + (-1) \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}
\end{aligned}
$$

♦

Let's take a break from this example to talk about an application of functional calculus for spectral projections.

Theorem 2.13 *Suppose $N \in M_n$. Write $N = uDu^\dagger = \sum_{i=1}^{n} \lambda_i \left|u_i\right\rangle \left\langle u_i\right|$ ($\left|u_i\right\rangle \left\langle u_i\right|$ are spectral projections) is an analytical function on $\mathbb{C}$ (IE a function f has a maclarin series $f(z) = \sum_{k=0}^{\inf} c_n z^k$). Then, $f(N) = \sum_{i=1}^{n} f(\lambda_i) \left|u_i\right\rangle \left\langle u_i\right|$.*

This exploits a useful property of projections, where the power of any projection is the same projection. Now, let's expand on example 2.12.

Example 2.14 Consider $f(z) = e^{i\alpha z}$, which is analytic on $\mathbb{C}$. Let's compute $f(\sigma_x) = \exp(i\alpha\sigma_x)$.

$$\exp(i\alpha\sigma_x) = e^{i\alpha(1)} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} + e^{-i\alpha} \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

Recall that Eulier's Identity says $e^{i\alpha} = \cos\alpha + i\sin\alpha$ and $e^{-i\alpha} = \cos\alpha - i\sin\alpha$

$$\begin{gathered} \exp(i\alpha\sigma_x) = (\cos\alpha + i\sin\alpha)P_1 + (\cos\alpha - i\sin\alpha)P_2 \\ = \cos\alpha(P_1 + P_2) + (i\sin\alpha)(P_1 - P_2). \text{ Note that } P_1 + P_2 = I. \\ = \cos(\alpha)I + (i\sin\alpha)(P_1 - P_2) \\ \text{Now, we can see that } \exp(i\alpha\sigma_x) = \begin{bmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{bmatrix} \end{gathered}$$

♦

2.5 Exercise 2.1

Let $A, B, C \in M_n$, and $c \in \mathbb{C}$. Show the following relationships:

(a) $(cA)^\dagger = c^* A^\dagger$

Conjugate transpose is distributive - $(cA)^\dagger = {c^*}^T A^\dagger$. Transpose of a scalar is the same scalar. Basically, transpose is a linear map from $m \times n$ to $n \times m$. So, ${c^*}^T = c^*$ and $(cA)^\dagger = c^* A^\dagger$

(b) $(A + B)^\dagger = A^\dagger + B^\dagger$

Let $A = \begin{bmatrix} \alpha_{11} & \ldots\ldots\alpha_{1n} \\ \vdots & \ddots\ddots,\vdots \\ \alpha_{m1} & \ldots\ldots\alpha_{mn} \end{bmatrix}$ and $B = \begin{bmatrix} \beta_{11} & \ldots\ldots\beta_{1n} \\ \vdots & \ddots\ldots,\vdots \\ \beta_{m1} & \ldots\ldots\beta_{mn} \end{bmatrix}$ where $\alpha \in \mathbb{C}$ and $\beta \in \mathbb{C}$

$$(A + B)^\dagger = \left(\begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix} + \begin{bmatrix} \beta_{11} & \ldots & \beta_{1n} \\ \vdots & \ddots & \vdots \\ \beta_{m1} & \ldots & \beta_{mn} \end{bmatrix} \right)^\dagger$$

$$= \left(\begin{bmatrix} \alpha_{11} + \beta_{11} \cdot \ldots x_{1n} + \beta_{1n} \\ \vdots \\ \alpha_{m1} + \beta_{m1} \ldots \alpha_{mn} + \beta_{mn} \end{bmatrix} \right)^\dagger$$

$$= \begin{bmatrix} \alpha_{11}+ & \beta_{11} \cdot \ldots & \alpha_{m1} & +\beta_{m1} \\ \cdot & \ddots & & \cdot \\ \vdots & . & & \vdots \\ \alpha_{1n} & +\beta_{1n} \cdot\cdot & \alpha_{mn} & +\beta_{mn} \end{bmatrix} = \begin{bmatrix} \alpha_{11}+\beta_{11} & \ldots & \alpha_{m1}+\beta_{m1} \\ \vdots & \ddots & \vdots \\ . & . & . \\ \alpha_{1n}+\beta_{1n} & \cdots & \alpha_{mn}+\beta_{mn} \end{bmatrix}$$

Where $\alpha_{mn} = \gamma_{mn} - \sum_{mn} i$
and $\beta_{mn} = \mu_{mn} - P_{mn} i$

$$A^\dagger + B^\dagger = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & \ddots & ,\vdots \\ \alpha_{m1} & - \ldots - & \alpha_{mn} \end{bmatrix}^\dagger + \begin{bmatrix} \beta_{\vdots}, 1 & i^{\cdots\beta} & \frac{\beta}{\vdots} n \\ & \ddots & \\ \beta_{m1} & - \ldots - & \beta_{mn} \end{bmatrix}^\dagger$$

$$= \begin{bmatrix} \alpha_{11} & \ldots & x_m, \\ \vdots & \ddots\ddots & \vdots \\ \alpha_{1n} & - \ldots & \alpha_{mn} \end{bmatrix} + \begin{bmatrix} \beta_{11} & \ldots & \beta_{m1} \\ \vdots & \ddots. & \vdots \\ \beta_{1n} & \ldots & \beta_{mn} \end{bmatrix}$$

$$= \begin{bmatrix} \alpha_{11}+\beta_1, & \ldots & \alpha_{m1}+\beta_{m1} \\ \vdots & \ddots. & \vdots \\ \alpha_{1n}+\beta_{1n} & \ldots \alpha_{mn} & +\beta_{mn} \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} \alpha_{11}+\beta_{11} & \cdot\ldots & \alpha_{m1}+\beta_{m1} \\ \cdot & & \cdot \\ \vdots & \ddots & \vdots \\ \alpha_{1n}+\beta_{1n} & \ldots & \alpha_{mn}+\beta_{mn} \end{bmatrix} = \begin{bmatrix} \alpha_{11}+\beta_{11} & \ldots & \alpha_{m1}+\beta_{m1} \\ \vdots & \ddots. & \vdots \\ \alpha_{1n}+\beta_{1n} & \ldots & \alpha_{mn}+\beta_{mn} \end{bmatrix}$$

(c) $(AB)^\dagger = B^\dagger A^\dagger$

$$A = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{m1} \\ \vdots & \ddots & \vdots \\ \alpha_{11} & \ldots & \alpha_{mn} \end{bmatrix} B = \begin{bmatrix} \beta_{11} & \ldots & \beta_{m1} \\ \vdots & \ddots & \vdots \\ \beta_{11} & \ldots & \beta_{mn} \end{bmatrix}$$

$$(AB)^\dagger = \left(\begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \ldots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} \beta_{11} & \ldots & \beta_{1n} \\ \vdots & \ddots & \vdots \\ \beta_{n_1} & \ldots & \beta_{nn} \end{bmatrix} \right)^\dagger$$

$$= \begin{bmatrix} (\alpha_{11}\beta_{11} + \ldots + \alpha_{1n}\beta_{n1}) & \ldots & (\alpha_{11}\beta_1 n^t \ldots + \alpha_n \beta_{nn}) \\ \vdots & \ddots & \vdots \\ (\alpha_n, \beta_{11} + \ldots + \alpha_{nn}\beta_{n1}) & \ldots & (\alpha_n, \beta_{n1} + \ldots + \alpha_{nn}\beta_{nn}) \end{bmatrix}^\dagger$$

$$= \begin{bmatrix} (\alpha_{11}\beta_{11} + \ldots + \alpha_{1n}\beta_{n1}) \ldots & & (\alpha_{n1}\beta_{11} + \ldots + \alpha_{nn}\beta_{n1}) \\ \vdots & \ddots & \vdots \\ (\alpha_{11}\beta_{11} + \ldots + \alpha_{1n}\beta_{nn}) & \cdots & (\alpha_n, \beta_{n1} + \ldots + \alpha_{nn}\beta_{nn}) \end{bmatrix}$$

$$B^\dagger A^\dagger = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{in} \\ i & \ddots & \vdots \\ \alpha_{n1} & \ldots & \alpha_{nn} \end{bmatrix}^T \begin{bmatrix} \beta_{11} & \ldots & \beta_{1n} \\ \vdots & \ddots & \vdots \\ \beta_{n_1} & \ldots & \beta_{nn} \end{bmatrix}^t == \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{n1} \\ \vdots & \ddots & \vdots \\ \alpha_{1n} & \ldots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} \beta_{11} & \ldots & \beta_{n1} \\ \vdots & \ddots & \vdots \\ \beta_{1n} & \ldots & \beta_{nn} \end{bmatrix}$$

$$\begin{bmatrix}(\alpha_{11}\beta_{11}+\ldots+\alpha_{1n}\beta_{n1}) & \ldots & (x_n,\beta_{11}+\ldots+\alpha_{nn}\beta_{n1})\\ \vdots & \ddots & \vdots\\ \big(\alpha_{11}\beta_1 n^\dagger\ldots+A_{1n}B_{nn}\big) & \ldots & (\alpha_n,\beta_{n1}+\ldots+\alpha_{nn}\beta_{nn})\end{bmatrix}$$

$$\begin{bmatrix}(\alpha_{11}\beta_{11}+\ldots+\alpha_{1n}\beta_{n1}) & \ldots & (alpha_n,\beta_{11}+\ldots+\alpha_{nn}\beta_{n1})\\ \vdots & \ddots & \vdots\\ \big(\alpha_{11}\beta_1 n^\dagger\ldots+\alpha_{1n}\beta_{nn}\big) & \ldots & (\alpha_n,\beta_{n1}+\ldots+\alpha_{nn}\beta_{nn})\end{bmatrix}=$$

$$\begin{bmatrix}(\alpha_{11}\beta_{11}+\ldots+\alpha_{1n}\beta_{n1}) & \ldots & (\alpha_n,\beta_{11}+\ldots+\alpha_{nn}\beta_{n1})\\ \vdots & \ddots & \vdots\\ (\alpha_{11}\beta_{1n}+_{\ldots}+A_nB_{nn}) & \ldots & (\alpha_n,\beta_{n1}+\ldots+\alpha_{nn}\beta_{nn})\end{bmatrix}$$

2.6 Exercise 2.2

Let $A=\frac{1}{\sqrt{2}}\begin{bmatrix}0 & 1+i\\ i-1 & 0\end{bmatrix}$

(a) **Find the eigenvalues and normalized eigenvectors for A**

$$A-\lambda I=\begin{bmatrix}0 & \dfrac{1+i}{\sqrt{2}}\\ \dfrac{1-i}{\sqrt{2}} & 0\end{bmatrix}-\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}=\begin{bmatrix}-\lambda & \dfrac{1+i}{\sqrt{2}}\\ \dfrac{1-i}{\sqrt{2}} & -\lambda\end{bmatrix}$$

$$\det|A-\lambda I|=\left|\begin{bmatrix}-\lambda & \dfrac{1+i}{\sqrt{2}}\\ \dfrac{1-i}{\sqrt{2}} & -\lambda\end{bmatrix}\right|=0$$

$$\left(\lambda^2-\frac{1}{2}(1+i)(1-i)\right)=0$$

$$\lambda^2-\frac{1}{2}(2)=0$$

$$\lambda^2=1$$

$$\lambda=\pm1$$

$$\lambda=1:\ A-1I=\begin{bmatrix}-1 & \dfrac{1+i}{\sqrt{2}}\\ \dfrac{1-i}{\sqrt{2}} & -1\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}=0\longrightarrow|v_1\rangle=\sqrt{2}\begin{bmatrix}\dfrac{-1-i}{\sqrt{2}}\\ 1\end{bmatrix}$$

$$\lambda=-1:\ A+1I=\begin{bmatrix}1 & \dfrac{1+i}{\sqrt{2}}\\ \dfrac{1-i}{\sqrt{2}} & 1\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}=0\longrightarrow|v_2\rangle=\sqrt{2}\begin{bmatrix}\dfrac{1+i}{\sqrt{2}}\\ 1\end{bmatrix}$$

(b) **Show that the eigenvectors are mutually orthogonal**

To determine if the eigenvectors are mutually orthogonal, we can verify that the inner product is zero.

$\langle v_1\mid v_2\rangle=\begin{bmatrix}\dfrac{-1+i}{\sqrt{2}} & 1\end{bmatrix}\begin{bmatrix}\dfrac{1+i}{\sqrt{2}}\\ 1\end{bmatrix}=\frac{-1+i}{\sqrt{2}}\cdot\frac{1+i}{\sqrt{2}}+1=0\longleftarrow$ Therefore, the eigenvectors are mutually orthogonal.

(c) Show the projection operators associated to the mutually orthogonal eigenvectors satisfy the *completeness relation*; IE if $|u_1\rangle$, $|u_2\rangle$ are mutually orthogonal unit eigenvectors for A, then $I = \sum_{i=1}^{2} |u_i\rangle \langle u_i|$.
Recall $|u_i\rangle \langle u_i|$.
$|v_1\rangle \langle v_1| = \begin{bmatrix} \frac{-1-i}{\sqrt{2}} \\ 1 \end{bmatrix} \begin{bmatrix} \frac{-1+i}{\sqrt{2}} & 1 \end{bmatrix} = \begin{bmatrix} 1 & \frac{-1-i}{\sqrt{2}} \\ \frac{-1+i}{\sqrt{2}} & 1 \end{bmatrix}$
$|v_2\rangle \langle v_2| = \begin{bmatrix} \frac{1+i}{\sqrt{2}} \\ 1 \end{bmatrix} \begin{bmatrix} \frac{1-i}{\sqrt{2}} & 1 \end{bmatrix} = \begin{bmatrix} 1 & \frac{1+i}{\sqrt{2}} \\ \frac{1-i}{\sqrt{2}} & 1 \end{bmatrix}$
$|v_1\rangle \langle v_1| + |v_2\rangle \langle v_2| = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I$. Therefore, the projection operators associated to the eigenvectors satisfy the completeness relation.

(d) **Find a unitary matrix which diagonalizes A, IE find a unitary matrix U and a diagonal matrix D such that $A = UDU^\dagger$.**
$D = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $u = \begin{bmatrix} \frac{1+i}{\sqrt{2}} & \frac{-(1+i)}{\sqrt{2}} \\ 1 & 1 \end{bmatrix}$, $u^\dagger = \begin{bmatrix} \frac{-(1-i)}{\sqrt{2}} & 1 \\ 1 & \frac{1+i}{\sqrt{2}} \end{bmatrix}$
Symbolab says $A = uDu^\dagger$... maybe a later problem

2.7 Exercise 2.3

Prove the following:

(a) Suppose A is *skew-Hermitian*, i.e., $A^\dagger = -A$. Show that the eigenvalues of A are pure imaginary, i.e., if λ is an eigenvalue for A, then $\lambda = bi$ for some $b \in R$.

Proof. Let $A \in M_n$ be skew-Hermitian (IE $A^\dagger = -A$). We will prove that the eigenvalues for A are pure imaginary. First, we must show that $|u_i\rangle \langle u_i|$ is Hermitian. Recall that $(AB)^\dagger = B^\dagger A^\dagger$ Observe

$$(|u_i\rangle \langle u_i|)^\dagger = (\langle u_i|)^\dagger (\langle u_i|)^\dagger = |u_i\rangle \langle u_i|.$$

We can use this property and the spectral theorem for normal matrices to show that the corresponding eigenvalues are pure imaginary. Note that A has negative eigenvalues, IE $\langle x| A^\dagger |x\rangle = -\lambda$, IE $\lambda^* = -\lambda$ Observe

$$A^\dagger = \sum \lambda_i^* (|u_i\rangle \langle u_i|)^\dagger = \sum \lambda_i^* |u_i\rangle \langle u_i| = -A.$$

Therefore, the eigenvalues of A are pure imaginary. ■

(b) **Let U be a unitary matrix. Show that the eigenvalues of U are unimodular, i.e., if λ is an eigenvalue of U, then $|\lambda| = 1$.**

Proof. Let $u \in M_n$ where $u^\dagger u = uu^\dagger = I$ (IE unitary). We will show that the eigenvalues of u are unimodular. By definition of eigenvalue and eigenvector, $u|x\rangle = \lambda |x\rangle$. Observe

$$\begin{gathered}
(u\left|x\right\rangle)^\dagger = (\lambda\left|x\right\rangle)^\dagger \\
\left|x\right\rangle^\dagger u^\dagger = \left|x\right\rangle^\dagger \lambda^\dagger \\
\left|x\right\rangle^\dagger \underbrace{u^\dagger u}_{1} \left|x\right\rangle = \left|x\right\rangle^\dagger \lambda^\dagger \lambda \left|x\right\rangle \\
\left|x\right\rangle^\dagger \left|x\right\rangle = \lambda^\dagger \lambda \left|x\right\rangle^\dagger \left|x\right\rangle \\
|x|^2 = \lambda^\dagger \lambda |x|^2 \\
1 = \lambda^* \lambda = |\lambda|^2 \\
|\lambda| = 1
\end{gathered}$$

Therefore, the eigenvalues of a unitary matrix u are unimodular. ■

(c) **Let A be a normal matrix. Show that A is Hermitian if and only if all the eigenvalues of A are real.**

Proof. Let $A \in M_n$. We will prove that A is Hermitian if and only if all eigenvalues of A are real. First, we must show that $\left|u_i\right\rangle \left\langle u_i\right|$ is Hermitian. Recall that $(AB)^\dagger = B^\dagger A^\dagger$ Observe

$$(\left|u_i\right\rangle \left\langle u_i\right|)^\dagger = (\left\langle u_i\right|)^\dagger (\left\langle u_i\right|)^\dagger = \left|u_i\right\rangle \left\langle u_i\right|.$$

Now, we prove that if $\lambda \in \mathbb{R}$, A is Hermitian. Recall that A is Hermitian if $A^\dagger = A$. Observe

$$A^\dagger = \textstyle\sum_{i=1}^n \lambda_i^* (\left|u_i\right\rangle \left\langle u_i\right|)^\dagger = \sum_{i=1}^n \lambda_i (\left|u_i\right\rangle \left\langle u_i\right|) = A.$$

Therefore, if $\lambda \in \mathbb{R}$, A is Hermitian. Now, we must prove that if A is Hermitian, $\lambda \in \mathbb{R}$. Let $\left|x\right\rangle$ be a normalized eigenvector for A corresponding to λ. Observe

$$\begin{gathered}
A^\dagger = \textstyle\sum_{i=1}^n \lambda_i^* (\left|u_i\right\rangle \left\langle u_i\right|)^\dagger = \sum_{i=1}^n \lambda_i (\left|u_i\right\rangle \left\langle u_i\right|) \\
\left\langle x\right| A^\dagger \left|x\right\rangle = \lambda^* \left\langle x \mid x\right\rangle = \lambda^* = \lambda
\end{gathered}$$

Therefore, $\lambda \in \mathbb{R}$. We proved that if $\lambda \in \mathbb{R}$, A is Hermitian, and if A is Hermitian, $\lambda \in \mathbb{R}$. Therefore, A is Hermitian if and only if all eigenvalues of A are real. ■

2.8 Exercise 2.4

Let $U = \begin{bmatrix} 0 & 0 & i \\ 0 & i & 0 \\ i & 0 & 0 \end{bmatrix}$. Find the eigenvalues for U (without calculation if possible) and its corresponding eigenvectors.

First, we note that U is *skew-Hermitian* because the eigenvalues are pure imaginary. We also note that U is anti-diagonal. Maybe this will be helpful. There is likely a method of applying a rotation that diagonalizes U. Not gonna lie I don't really understand how to do that yet so check this out:

$$\begin{bmatrix} 0 & 0 & i \\ 0 & i & 0 \\ i & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -\lambda & 0 & -1 \\ 0 & -1-\lambda & 0 \\ -1 & 0 & -\lambda \end{bmatrix} \longrightarrow \lambda = -i, -i, i$$

2.9 Exercise 2.5

Let H be a Hermitian matrix.

(a) Show that $(I - iH)$ is invertible.

(b) Show that $U = (I + iH)(I - iH)^{-1}$ is unitary (*Cayley transformation.*

2.10 Exercise 2.6

Suppose a 2×2 matrix A has eigenvalues $-1, 3$ and corresponding eigenvectors

$$|b_1\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ i \end{bmatrix}, \quad |b_2\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$$

3 Framework of Quantum Mechanics

The axioms of quantum mechanics are choices made by humans to attempt to mathematically describe the behavior of particles. To dumb this down for my monkey brain, I'm going to describe these axioms with a story. To begin, let's suppose that we prepared a photon for experimentation in a laboratory. Realistically, despite 'preparing' this photon, IE understanding some of its initial conditions, we can never explicitly model it. Recall that $A \in M_n$ is:

1. normal if $A^\dagger A = AA^\dagger$
2. Hermitian if $A^\dagger = A$
3. unitary if $A^\dagger A = AA^\dagger = I$

3.1 Quantum Mechanics Axiom 1.1

A vector state $|x\rangle$ (IE $|x\rangle$ encodes all physical info about a photon) is a unit vector in a complex Hilbert state ($H = \mathbb{C}^n$). In our story, we first want to figure out the photon's polarization. To figure this out, we're going to 'shoot' it at a vertically polarized filter. In classical mechanics, our particle should be polarized either vertically or horizontally. IE there are two possible outcomes:

1. If $|x\rangle$ goes through the vertically polarized filter, it was oriented vertically
2. If $|x\rangle$ is deflected by the vertically polarized filter, it was oriented horizontally

After preparing our $|x\rangle$ 100 times and repeating this same process, we're *appalled* to find that sometimes the particle was vertically oriented, but sometimes it was horizontally oriented. IE

1. 64 times it was oriented vertically ($| \alpha |^2 = 0.64$)
2. 36 times it was oriented horizontally ($| \alpha |^2 = 0.36$)

3.2 Quantum Mechanics Axiom 1.2

Linear combinations (aka superposition) of the physical states are allowed to act as $|x\rangle$. Let's consider $|v\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ and $|h\rangle = \begin{bmatrix}1\\0\end{bmatrix}$. We'll call this the polarization basis for $\mathbb{C}^2$. Therefore, $|x\rangle = \alpha\begin{bmatrix}0\\1\end{bmatrix} + \beta\begin{bmatrix}1\\0\end{bmatrix}$ where α and β are probabilities and $\mid \alpha \mid^2 + \mid \beta \mid^2 = 1$. Since we've assigned representations to our states, we want some easy way to 'keep track' of the choices. Let $A = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$, which behaves/represents the vertically polarized filter. This choice makes sense because $|v\rangle$ and $|h\rangle$ are eigenvectors for A, with eigenvalues 1 and 0.

Example 3.1 Suppose $B = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}$. This might be a nice matrix to represent a horizontally polarized filter, because it has $|v\rangle$ and $|h\rangle$ as eigenvectors with eigenvalues 0 and 1. ♦

3.3 Quantum Mechanics Axiom 2

An observable of a state $|x\rangle$ corresponds to a Hermitian matrix A. IE $|x\rangle$ is in state $|u\rangle$; an eigenvector for A with probability $\mid \langle u \mid x\rangle \mid^2$. Note that we don't know the state of the particle *until* it hits the filter, at which point it's one state or the other. Remember that this is basically a Walmart version of this explanation, so this is more complex. When the particle is in the 'air,' it's in the state of *superposition*. Let's check this axiom:

$$\begin{aligned}\mid \langle v \mid u\rangle \mid^2 &= \mid \langle v| (\alpha |v\rangle \times \beta |h\rangle) \mid^2 \\ &= \mid \langle v \mid v\rangle + \beta \langle v \mid v\rangle \mid^2 \\ \longrightarrow |x\rangle &= \alpha\begin{bmatrix}0\\1\end{bmatrix} + \beta\begin{bmatrix}1\\0\end{bmatrix} = 1\end{aligned}$$

3.4 Quantum Mechanics Axiom 3

The time dependence of a state is governed by the Schrödinger equation:

$$i\hbar\frac{\partial |\psi\rangle}{\partial t} = H|\psi\rangle \tag{3.3}$$

where $\hbar$ is the reduced Planck's constant and H is a Hermitian matrix corresponding to the energy of the system, called "Hamiltonian." You'll note that this is just a differential equation at its core. The expectation value μ of the observable associated with A after measurements with respect to many copies of $|\psi\rangle$ is the weighted average of the expected outcomes.

$$\langle A\rangle_\psi = \sum_{i=1}^{n} \lambda_i \mid \langle u_i \mid \psi\rangle \mid^2 \tag{3.4}$$

Note that λ_i's are the "locations" of the probabilistic outcomes.

$$|\psi\rangle = \sum_{i=1}^{n} c_i |u_1\rangle \tag{3.5}$$

When H is time-independent, the solution to the Schrödinger equation is

$$|\psi(t)\rangle = \exp(-it\frac{H}{\hbar})\,|\psi(0)\rangle \tag{3.6}$$

This is effectively saying $\frac{dy}{dt} = ky \longrightarrow y = e^{kt}$. IE when we take the derivative, we get an exponent.

Example 3.2 Consider a physical system with Hamiltonian $H = \frac{-\hbar}{2}\omega\sigma_x$ and suppose $|\psi(0)\rangle = \begin{bmatrix}1\\0\end{bmatrix}$. Recall that $\begin{bmatrix}1\\0\end{bmatrix}$ is the first column of σ_z, and the spin points in the z-direction at $t = 0$.

(a) Find the wave function $|\psi(t)\rangle$ when $t > 0$.
By the Schrödinger equation, $|\psi(t)\rangle = e^{\frac{-itH}{\hbar}} * |\psi(0)\rangle$.
$|\psi(t)\rangle = \exp\left(i\left(\frac{-t}{\hbar}\right)\left(\frac{-\hbar}{2}\omega\sigma_x\right)\right)\begin{bmatrix}1\\0\end{bmatrix}$
$= \exp\left(i\left(\frac{-t}{2}\omega\right)\sigma_x\right)\begin{bmatrix}1\\0\end{bmatrix}$ where $\alpha = \frac{-t}{2}\omega$
$= \left(\cos\left(\frac{t}{2}\omega\right)I + i\sin\left(\frac{t}{2}\omega\right)\sigma_x\right)\begin{bmatrix}1\\0\end{bmatrix}$
$= \begin{bmatrix}\cos\left(\frac{t}{2}\omega\right) & i\sin\frac{t}{2}\\ i\sin\left(\frac{t}{2}\right) & \cos\left(\frac{t}{2}\omega\right)\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}$
$\longrightarrow |\psi(t)\rangle = \begin{bmatrix}\cos\left(\frac{t\omega}{2}\right)\\ i\sin\left(\frac{t\omega}{2}\right)\end{bmatrix}$ This is our wave function; we can now use it to find probabilities, etc.

(b) Find the probability for the system to have outcome $+1$ upon measurement of ω_z. Key idea: The coefficients of $|\psi(t)\rangle$ in the orthonormal basis of eigenvectors associated to σ_z give the probabilities. *Use the projections!*
Recall that $N = uDu^\dagger = \sum_{j=1}^{n}\lambda_i\,|u_j\rangle\langle u_j|$
$\sigma_z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} = 1\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + (-1)\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$
So, $P_1\,|\psi(t)\rangle = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}\cos\left(\frac{t\omega}{2}\right)\\ i\sin\left(\frac{t\omega}{2}\right)\end{bmatrix} = \begin{bmatrix}\cos\left(\frac{t\omega}{2}\right)\\0\end{bmatrix}\cos\left(\frac{t\omega}{2}\right)|u_1\rangle$. Now, recall that the probability of observing λ_i state is $|c_i|^2$. IE $|\psi(t)\rangle = \sum_{j=1}^{n} c_i\,|u_i\rangle$. Also note that $|u_i\rangle$ is an orthonormal basis of eigenvectors for an observable.
Therefore, the probability of seeing $+1$ upon measurement σ_z is $P(t) = |\cos\left(\frac{t\omega}{2}\right)|^2 = \cos^2\left(\frac{\omega t}{2}\right)$

(c) Find the probability of -1 upon measurement of σ_z
$P_2\,|\psi(t)\rangle = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}\cos\left(\frac{t\omega}{2}\right)\\ i\sin\left(\frac{t\omega}{2}\right)\end{bmatrix} = \begin{bmatrix}0\\ i\sin\left(\frac{t\omega}{2}\right)\end{bmatrix} = i\sin\left(\frac{t\omega}{2}\right)$
The probability of seeing -1 upon measurement σ_z is $P(t) = |i\sin\left(\frac{t\omega}{2}\right)|^2 = i\sin^2\left(\frac{\omega t}{2}\right)$
or $|\psi(t)\rangle = \langle u_1 \mid \psi(t)\rangle\,|u_1\rangle + \langle u_2 \mid \psi(t)\rangle\,|u_2\rangle$, so, $c_2 = \langle u_2 \mid \psi(t)\rangle = \begin{bmatrix}0 & 1\end{bmatrix}\begin{bmatrix}\cos\left(\frac{t\omega}{2}\right)\\ i\sin\left(\frac{t\omega}{2}\right)\end{bmatrix}$

(d) Find the expectation value under many measurements of σ_z.
Recall that $\langle A \rangle_\psi = \langle \psi | A | \psi \rangle$
$\langle \sigma_z \rangle_\psi = \langle \psi | \sigma_z | \psi \rangle = (+1)\left(\cos^2\left(\frac{\omega t}{2}\right)\right) + (-1)\sin^2\left(\frac{\omega t}{2}\right) = \left(\cos^2\left(\frac{\omega t}{2}\right)\right) - sin^2\left(\frac{\omega t}{2}\right)$ ◆

3.5 Exercise 3.1

Let $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$

(a) Explain why $\mathbb{C}^2$ must have an orthonormal basis of eigenvectors for A
Note that since $A^\dagger A = AA^\dagger$ (A is normal), AND $A^\dagger = A$ (A is Hermitian), we have an orthonormal basis. So, we can use the spectral theorem.

(b) Find eigenvalues for A, and its corresponding normalized eigenvectors.

$$\det \begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix} = \left| \begin{bmatrix} 2-\lambda & 1 \\ 1 & 2-\lambda \end{bmatrix} \right|$$
$$= 4 - 2\lambda - 2\lambda + \lambda^2 - 1 = \lambda^2 - 4\lambda + 3$$
$$= \lambda^2 - 3\lambda - \lambda$$
$$\lambda(\lambda - 3) - \lambda - 3 = (\lambda - 3)(\lambda - 1) \longrightarrow \lambda = 3, 1$$

Now, let's find our eigenvectors. Start with $\lambda = 3$

$$A - \lambda I = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} - 3 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} - \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$$
$$= \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}$$
$$\text{Therefore, } \lambda = 3 : \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Next, find the eigenvector for $\lambda = 1$

$$A - \lambda I = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} - 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Therefore, $\lambda = 1 : \tfrac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ 1 \end{bmatrix}$

(c) Find the spectral decomposition of A

$$
\begin{gathered}
A = uDu^{\dagger} \\
A = u \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix} u^{\dagger} \\
\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = \tfrac{1}{2} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \\
= \tfrac{1}{2} \begin{bmatrix} 3 & -1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \\
A = \tfrac{1}{2} \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}
\end{gathered}
$$

(d) Compute $\exp(i\alpha A)$

$$
\begin{gathered}
\frac{1}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \end{bmatrix} = \underbrace{\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}}_{P_1} \\
\frac{1}{2} \begin{bmatrix} -1 \\ 1 \end{bmatrix}^{[-11]} = \underbrace{\begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}}_{P_2} \\
\lambda_1 \cdot P_1 + \lambda_2 P_2 = A \longrightarrow \begin{bmatrix} \frac{3}{2} & \frac{3}{2} \\ \frac{3}{2} & \frac{3}{2} \end{bmatrix} + \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \\
\exp(i\alpha A) = \exp(i\alpha \underbrace{(3)}_{\lambda_1}) \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \exp(i\alpha \underbrace{(1)}_{\lambda_2}) \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \\
e^{(i3\alpha)} = \cos(3\alpha) + i\sin(3\alpha) \\
e^{(i\alpha)} = \cos(\alpha) + i\sin(\alpha) \\
= [\cos(3\alpha) + i\sin(3\alpha)]\, P_1 + [\cos(\alpha) + i\sin(\alpha)]\, P_2 \\
= \begin{bmatrix} \frac{\cos(3\alpha)+i\sin(3\alpha)+\cos(\alpha)+\sin(\alpha)}{2} & \frac{\cos(3\alpha)-i\sin(3\alpha)-\cos(\alpha)+\sin(\alpha)}{2} \\ \frac{\cos(3\alpha)+i\sin(3\alpha)-\cos(\alpha)-\sin(\alpha)}{2} & \frac{\cos(3\alpha)+i\sin(3\alpha)+\cos(\alpha)+\sin(\alpha)}{2} \end{bmatrix}
\end{gathered}
$$

4 Separable States and the Single Value Decomposition

4.1 Tensor Product

Consider a vector space with inner product $H = H_1 \otimes H_2$ (where $\otimes$ is the tensor product) combining H_1 and H_2 in such a way that the elements of H_1 affect H_2, and vice versa. A general vector in H is a linear combination of vectors $\{|v_1\rangle \otimes |v_2\rangle \,|\, |v_1\rangle, |v_2\rangle \in H_2\}$ taking the tensor product of $A \in M_{mn}$ and $B \in M_{pq}$:

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & ... & A_{1n}B \\ A_{21}B & A_{22}B & ... & A_{2n}B \\ ... & ... & ... & ... \\ A_{m1}B & A_{m2}B & ... & A_{mn}B \end{bmatrix} \in M_{(mp)(nq)}$$

Example 4.1 $\sigma_x \otimes i\sigma_y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$

$$\sigma_y \otimes \sigma_x = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

$$\sigma_x \otimes \sigma_y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$ ♦

4.2 Nice facts of the Tensor Product

Here are some nice facts of the tensor product:

1. $(\lambda A) \otimes B = B \otimes (\lambda B)$ IE scaling A affects B and vice versa
2. In general, $A \otimes B \neq B \otimes A$ IE generally noncommutative
3. $(A \otimes B)(C \otimes D) = AC \otimes BD$ IE distributive
4. $A \otimes (B + C) = (A \otimes B) + (A \otimes C)$ IE distributive
5. $(A \otimes B) + (C \otimes D) \neq (A + C) \otimes (B + D)$
6. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$ IE dagger can be distributed
7. If A and B are invertible, $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$

Example 4.2 $|1\rangle \otimes |1\rangle = |11\rangle$ (some funky notation) IE $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

$$|12\rangle = |1\rangle \otimes |2\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|21\rangle = |2\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$|22\rangle = |2\rangle \otimes |2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Note that $\{|11\rangle, |12\rangle, |21\rangle, |22\rangle\}$ forms a basis for $\mathbb{C}^4$, but these vectors live in $\mathbb{C}^2 \otimes \mathbb{C}^2$. IE $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ *(same shape)*. If $|v\rangle \in \mathbb{C}^m$ and $|w\rangle \in \mathbb{C}^n$, then $|vw\rangle = |v\rangle \otimes |w\rangle \in \mathbb{C}^m \oplus \mathbb{C}^n \cong \mathbb{C}^{mn}$.
Note that $\dim(\mathbb{C}^m \otimes \mathbb{C}^n) = \dim(\mathbb{C}^m) + \dim(\mathbb{C}^n) = m + n$ and $\dim(\mathbb{C}^m \otimes \mathbb{C}^n) = \dim(\mathbb{C}^m) \cdot \dim(\mathbb{C}^n) = m \cdot n$

Theorem 4.3 *If H_1 has orthonormal basis $\epsilon_1 = \{|e_{1,1}\rangle, |e_{1,2}\rangle, ..., |e_{1,m}\rangle\}$ and $\epsilon_2 = \{|e_{2,1}\rangle, |e_{2,2}\rangle, ..., |e_{2,n}\rangle\}$, then, $H = H_1 \otimes H_2$ has orthormal basis $\{|e_{1,i}\rangle \otimes |e_{2,j}\rangle \,|1 \leq i \leq m, 1 \leq j \leq n\}$ written as $i \in [m], j \in [n]$*

4.3 Inner Product on H

Let $v_1, w_1 \in H_1$ and $v_2, w_2 \in H_2$. Then, $\langle |v_1\rangle \otimes |v_2\rangle \mid |w_1\rangle \otimes |w_2\rangle\rangle = \langle v_1v_2 \mid w_1w_2\rangle = \langle v_1 \mid w_1\rangle_{H_1} \cdot \langle v_2 \mid w_2\rangle_{H_2}$. We need to check that ϵ is an orthonormal set. Let $\langle e_{1,i}e_{2,j} \mid e_{1,k}e_{2,j}\rangle = \langle e_{1,i} \mid e_{1,k}\rangle_{H_1} \cdot \langle e_{2,j} \mid e_{2,j}\rangle_{H_2}$.

4.4 Multipartite Physical Systems

Quantum systems comprised of multiple systems are called multipartite systems. This is to say $H = H_1 \otimes H_2 \otimes ... \otimes H_n$ is a multipartite system when $n = 2$, and $H = H_1 \otimes H_2$ is called bipartite. Note that a $|\psi\rangle$ state in $H = H_1 \otimes H_2$ is bipartite.

Definition 4.4 A vector $|\psi\rangle \in H = H_1 \otimes H_2$ is separable (IE elementary tensor) if $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ for some $|\psi_1\rangle \in H_1, |\psi_2\rangle \in H_2$. ♦

Recall that $H_1 \otimes H_2$ is a u.s. of linear combinations of vectors in the form $|\psi_1\rangle \otimes |\psi_2\rangle$. If $|\psi\rangle \in H_1 \otimes H_2$, $|\psi\rangle$ can be written as $\sum_{ij} c_{ij} |e_{1,i}\rangle \otimes |e_{2,j}\rangle$ where $|e_{1,i}\rangle$ is the basis vector for H_1 and $|e_{2,j}\rangle$ is a basis vector for H_2.

Example 4.5 Consider $|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle \otimes |1\rangle + |2\rangle \otimes |2\rangle)$
$\frac{1}{\sqrt{2}}(|11\rangle + |22\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2)$

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

How can we tell if a state $|\psi\rangle \in H_1 \otimes H_2$ is separable?

Definition 4.6 A vector that is **not separable** is called **entangled**. IE, there is a state that can't be expressed as a tensor of two vectors, and the state can't be analyzed because the system is in superposition. ♦

IE, if some $|\psi\rangle$ is separable, we should be able to write it as $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ where: $|\psi_1\rangle = c_1 |1\rangle + c_2 |2\rangle \in \mathbb{C}^2$ and $|\psi_2\rangle = d_1 |1\rangle + d_2 |2\rangle \in \mathbb{C}^2$. Note that the coefficient matrix for $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ is $C = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{bmatrix}$. Note that to put this in terms of classical encryption, the *states* H_1 or H_2 are similar to single (large) primes p, q, and *separable states* is similar to RSA where $N = pq$. Additionally, *entangled* is similar to multiple of these systems together, IE $N_1 + N_2 + ... + N_k$.

Remark 4.7 In $\mathbb{C}^2$, a state is separable if and only if the coefficient matrix is rank 1. ♦

This is to say that a state $|\psi\rangle = c_1 1 |11\rangle + c_1 2 |11\rangle + c_2 1 |21\rangle + c_2 2 |22\rangle$ is separable if and only if the rows of $C = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$ are scalar multiples of $|psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} c \\ d \end{bmatrix} \\ b \begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} c_{11} \\ c_{12} \\ c_{21} \\ c_{22} \end{bmatrix}$.

Definition 4.8 Let $A \in M_n$. The singular values for A are the square roots of the eigenvalues for $A^\dagger A \in M_n$ ♦

Let's do an example of the single value decomposition.

Example 4.9 Find the singular value decomposition (SVD) for $A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \\ i & i \end{bmatrix}$.

Note: $A^\dagger A = \begin{bmatrix} 1 & 0 & -i \\ 1 & 0 & -i \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \\ i & i \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$.

1. First, let's compute eigenvalues and eigenvectors for $A^\dagger A$
   $\lambda = 0 \longrightarrow |x\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ 1 \end{bmatrix}$
   $\lambda = 4 \longrightarrow |x\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
   Note: $A^\dagger A$ is positive semidefinite, so it must be normal. Therefore, it has a spectral decomposition.
   $$A^\dagger A = \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}}_{V} \underbrace{\begin{bmatrix} 4 & 0 \\ 0 & 0 \end{bmatrix}}_{D} \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^\dagger}_{V^\dagger}$$

2. Now, make sure our $V's$ are in decreasing order with respect to our eigenvalues. We'll also find our value Σ for the SVD.
   $V = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$
   $\Sigma = \begin{bmatrix} 2 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$

3. Next let's make some more eigenvectors using $A\left|\lambda_1\right\rangle + A\left|\lambda_2\right\rangle$

   $A\left|\lambda_1\right\rangle = \begin{bmatrix}1 & 1\\ 0 & 0\\ i & i\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix} = \sqrt{2}\begin{bmatrix}1\\ 0\\ i\end{bmatrix}$

   $A\left|\lambda_2\right\rangle = \begin{bmatrix}1 & 1\\ 0 & 0\\ i & i\end{bmatrix}\begin{bmatrix}-\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$

   Use $\left|u_1\right\rangle = \sqrt{2}\begin{bmatrix}1\\ 0\\ i\end{bmatrix}$ and $\left|u_2\right\rangle = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$ to create an orthonormal basis for $\mathbb{C}^3$. IE, find $\{\left|u_1\right\rangle, \left|u_2\right\rangle, \left|u_3\right\rangle\}$. Our $\left|u_2\right\rangle$ doesn't do much for us in this case, so we'll try to separate $\left|u_1\right\rangle$ into 3 linearly independent vectors. Let's use $\{\left|u_1\right\rangle, \left|2\right\rangle, \left|3\right\rangle\}$. These are linearly independent both to each other and to $\left|u_1\right\rangle$. Now, we need to create an orthonormal basis using the Gram-Schmidt process.

   (a) Normalize $\left|u_1\right\rangle \longrightarrow \left|u_1\right\rangle = \frac{\sqrt{2}}{2}\begin{bmatrix}1\\ 0\\ i\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}}\\ 0\\ \frac{i}{\sqrt{2}}\end{bmatrix}$

   (b) $\left|u_2\right\rangle = \left|2\right\rangle - \left\langle u_2 \mid 2\right\rangle \left|u_1\right\rangle = \begin{bmatrix}0\\ 1\\ 0\end{bmatrix} - 0\begin{bmatrix}\frac{1}{\sqrt{2}}\\ 0\\ \frac{1}{\sqrt{2}}\end{bmatrix} = \begin{bmatrix}0\\ 1\\ 0\end{bmatrix}$ (already orthogonal)

   (c) $\left|u_3\right\rangle = \left|3\right\rangle - \left\langle u_1 \mid 3\right\rangle \left|u_1\right\rangle - \underbrace{\left\langle u_2 \mid 3\right\rangle \left|u_1\right\rangle}_{0} = \left|3\right\rangle - \left(\frac{-i}{\sqrt{2}}\cdot 1\right) = \begin{bmatrix}0\\ 0\\ 1\end{bmatrix} - \begin{bmatrix}\frac{i}{2}\\ 0\\ \frac{1}{2}\end{bmatrix} = \begin{bmatrix}\frac{i}{2}\\ 0\\ \frac{1}{2}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}i\\ 0\\ 1\end{bmatrix} \longrightarrow \left|u_3\right\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}i\\ 0\\ 1\end{bmatrix}$

   Ok now we have some wacky new vectors which form an orthonormal basis for $\mathbb{C}^3$.

4. Form $u = \begin{bmatrix}\left|u_1\right\rangle & \left|u_2\right\rangle & \left|u_3\right\rangle\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}} & 0 & \frac{i}{\sqrt{2}}\\ 0 & 1 & 0\\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\end{bmatrix}$ By the way, u is unitary because its columns are orthonormal.

5. Finally, use $A = u\Sigma V^\dagger$ to find the SVD. ⧫

OK so basically we found the factorization of the matrix A into the product of u,Σ, and $V^\dagger$. Now, we're going to use another tool to accomplish a similar task, but instead use the result to express a vector as the tensor product of two inner product spaces.

Theorem 4.10 *Let $H = H_1 \cdot H_2$ where dim $H_1 = m < \inf$ and dim $H_2 = n < \inf$. Then, every vector $\left|\psi\right\rangle \in H$ admits a Schmidt decomposition*

$$\left|\psi\right\rangle = \textstyle\sum_{j=1}^{r} S_j \left|u_j\right\rangle \cdot \left|v_j\right\rangle$$

where $S_j > 0$ are the Schmidt coefficients satisfying $\sum_{j=1}^{r} S_j^2 = 1$, $\{|u_j\rangle\} \subseteq H_1$ and $\{|v_j\rangle\} \subseteq H_2$ are orthonormal and $r < min\{m, n\}$

5 Mixed States as Density Matrices

Let's go back to single particle systems for a little to motivate this idea of density matrices..

Example 5.1 Suppose $|\psi\rangle \in C^2$ is the state of some quantum system. Recall that this means that $\||\psi\rangle\| = 1$, and if we wanted to measure 'vertical' or 'horizontal' polarization; IE

$$\begin{gathered} \text{Vertical: } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ \text{Horizontal: } |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{gathered}$$

Where $|1\rangle$ and $|0\rangle$ are eigenstates of a chosen Hermitian matrix which represents our apparatus. Let's do a spectral decomposition:

$$A = 0\,|0\rangle\,\langle 0| + 1\,|1\rangle\,\langle 1| = |1\rangle\,\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Basically, we're interested in finding probabilistic information about $|\psi\rangle$ regarding its polarization.

$$|\psi\rangle = \alpha\,|0\rangle + \beta 1 \text{ where } \||\psi\rangle\| = \sqrt{\langle\psi \mid \psi\rangle}.$$

So, we interpret this expression of $|\psi\rangle$ in the $\{|0\rangle, |1\rangle\}$-basis as $|\psi\rangle$ in $|0\rangle$ with probability $|\alpha|^2$ and $|\psi\rangle$ in $|1\rangle$ with probability $|\beta|^2$.

Quick side note: In figure 1, we can see that $|\psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, and $|\psi_2\rangle = e^{i\theta}\alpha\,|0\rangle + e^{i\theta}\beta\,|1\rangle$. Basically, instead of using vectors, we're going to use density matrices. Take $|\psi\rangle \in C^2 \longrightarrow \rho_\psi = |\psi\rangle\,\langle\psi|$.

$$\begin{gathered} \rho_\psi = |\psi_1\rangle\,\langle\psi_2| = (\alpha\,|0\rangle + \beta\,|1\rangle \cdot (\alpha^*\,\langle 0| + \beta^*\,\langle 1| \\ = |\alpha|^2\,|0\rangle\,\langle 0| + \alpha\beta^*\,|0\rangle\,\langle 1| + \beta\alpha^*\,|1\rangle\,\langle 0| + |\beta|^2\,|1\rangle\,\langle 1| \\ \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^2 & |\beta|^* \end{bmatrix} = \rho\,|\psi_1\rangle \end{gathered}$$

Note that det = 0, rank = 1, IE the state is not entangled and not invertable. This matrix encodes all information that we can get out of $|\psi\rangle$. That is, repeated experiments can give us more information about the system, but we can't gather much more out of $|\psi\rangle$.

$$\begin{gathered} \longrightarrow e^{i\theta}\alpha(e^{i\theta}\alpha)^* = e^{i\theta}\alpha e^{-i\theta}\alpha^* = \alpha\alpha^* = |\alpha|^* \\ \longrightarrow \rho_{|\psi_2\rangle} = \rho\,|\psi_2\rangle \\ = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \end{gathered}$$

♦

OK great now we're motivated about density matrices. Here's a more specific example:

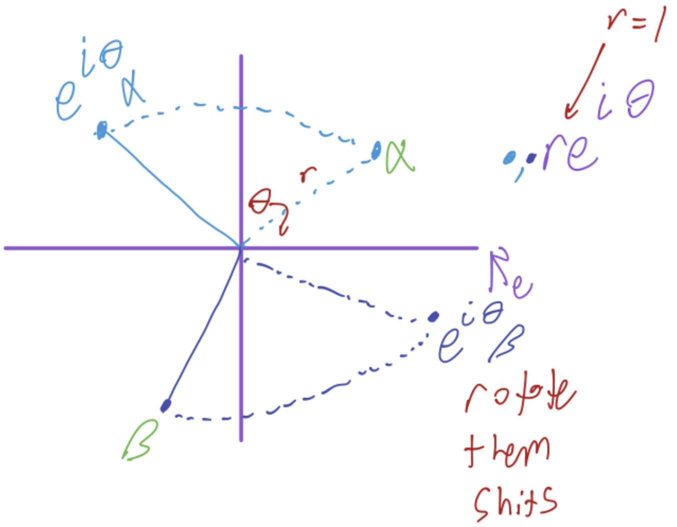

Figure 1: Rotate

Example 5.2 Given $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, find the density matrix ρ_ψ with respect to $\{|0\rangle, |1\rangle\}$.

$$\begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

$$\rho_\psi = |\psi\rangle\langle\psi| = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \\ -\frac{1}{2} & \end{bmatrix} \qquad \blacklozenge$$

Here are some observations:
If $|\psi\rangle \in C^n$ is a state,

- $\rho_\psi \in M_n(\mathbb{C})$
- ρ_ψ has trace 1
- ρ_ψ is Hermitian (IE $\rho_\psi^\dagger = \rho_\psi$).
  In fact, ρ_ψ is also positive semi-definite (IE non-negative eigenvalues).

To formalize these observations, here are some definitions:

Definition 5.3 The **trace** of an $n \times n$ matrix is the *sum* of its diagonal entries. ♦

Definition 5.4 A **density matrix** $\rho \in M_n$ is a Hermitian, positive-semidefinite matrix such that $\text{tr}(\rho) = 1$ ♦

Density matrices can be written with set-builder notation as follows:

$$\{P(|\psi\rangle) \mid |\psi\rangle \text{ states } \in \mathbb{C}^n\} = \{|\psi\rangle\langle\psi| \mid |\psi\rangle \in \mathbb{C}^n \text{ states}\}$$

Note that this is not actually a vector space. These sets are also called 'pure states' where there is no 'noise' in the system. We're actually particularly interested in looking at unit density matrices. We can write the linear combinations with set builder notation as:

$$\{\sum_{i=1}^{m} \rho_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \mid \sum_{i=1}^{m} \rho_i = 1, \rho_i > 0\}$$

Remark 5.5 Sometimes, states will be unit vectors. Other times, they're just the sums of pure states, IE they're the sums of rank 1 projection matrices. ⧫

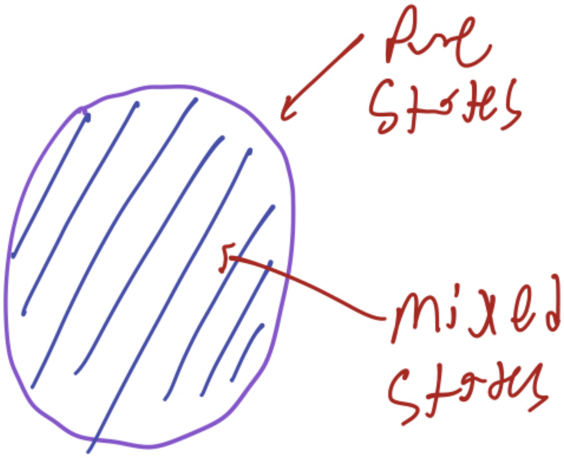

Figure 2: Illustration of pure vs. mixed states

This set contains all complex combinations of pure states, illustrated in Figure 2. This is essentially creating a weighted position average of some state $|\psi\rangle$.

5.1 Revisit Axiom 1

To complete computations using density matrices, it's useful to revisit Quantum Mechanics Axiom 1 discussed in section 3.1.

Remark 5.6 A physical state of a system, whose Hilbert space H is completely determined by its associated *density matrix* (IE $\operatorname{tr}(\rho) = 1 \longrightarrow$ unit condition) which we can think of as a map; IE $\rho : H \longrightarrow H$ ⧫

Example 5.7 Show that a mixed state $\rho = \sum_{i=1}^{n} \rho_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$ satisfies $\operatorname{tr}(\rho) = 1$. With our framework, Axiom 1 still holes.
First, pick a basis for H (Hilbert space) Then, fix an orthonormal basis $\{\left|e_1\right\rangle, \left|e_2\right\rangle, \ldots, \left|e_n\right\rangle\}$ for H. Recall that $(\rho)_{ij}$ has a "special inner product" $= \left\langle e_i\right| \rho \left|e_i\right\rangle$ (the i$^{\text{th}}$ column of e. Basically, we want to isolate a specific entry of the matrix. So,

$$\begin{gathered}\operatorname{tr}(\rho) = \sum_{i=1}^{n} \left\langle e_i\right| \rho \left|e_i\right\rangle = \sum_{i=1}^{n} \left\langle e_i\right| \sum_{j=1}^{n} P_j \left|\psi_j\right\rangle \left\langle\psi_j\right| \left|e_j\right\rangle \\ = \text{"evenly distributing"} \\ = \sum_{j=1}^{n} P_j \sum_{j=1}^{n} \left\langle e_i \mid \psi_i\right\rangle \left\langle\psi_j \mid e_i\right\rangle\end{gathered}$$

So,

$$\begin{gathered}\operatorname{tr}(\rho) = \sum_{j=1}^{n} p_j \sum_{i=1}^{n} \left\langle\psi_j \mid e_i\right\rangle \left\langle e_i \mid \psi_j\right\rangle \\ = \sum_{j=1}^{n} P_j \left\langle\psi_j\right| \sum_{i=1}^{n} \left|e_i\right\rangle \left\langle e_i \mid \psi_j\right\rangle \\ = \sum_{j=1}^{n} P_j \left\langle\psi_j \mid \psi_j\right\rangle = 1\end{gathered}$$ ⧫

OK now, here's a crazy fact: $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, even though in general, $AB \neq BA$. This is important because the trace allows us to consider a matrix as a Hilbert space. IE,

$$\operatorname{tr}((FA)F^\dagger) = \operatorname{tr}(F_\dagger(FA)) = texttr(IA) = texttr(A)$$

5.2 Revisit Axiom 2

Now, let's revisit Axiom 2 from section 3.3. The mean value of an observable is $\langle A \rangle = \operatorname{tr}\rho A$, where $\langle A \rangle$ is the probability after many measurements. Basically, we can find the probability with density matrices instead of vectors.

5.3 Revisit Axiom 3

The time evolution of a density matrix is given by the Louisville-Von Neumann equation:

$$i\hbar \frac{d}{dt}[\rho] = [H, P] = H\rho - \rho H \tag{5.7}$$

Recall that the probability of having an outcome of λ, an eigenvalue for an observable Hermitian A, given that the system is in state $|\psi\rangle$ is

$$|\langle \lambda \mid \psi \rangle|^2$$

Example 5.8 Recall that mixed density matrices are convex combinations of pure states.

$$|\psi\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \longrightarrow \rho = |\psi\rangle\langle\psi| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ 50\%}$$
$$|\phi_1\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \longrightarrow \rho_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \text{ 25\%}$$
$$|\phi_2\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \longrightarrow \rho_2 = |phi_2\rangle\langle phi_2| = \tfrac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \text{ 25\%}$$

♦

In the density matrix picture, $|\psi\rangle$ is replaced by $\rho = \sum_i P_i |\psi_i\rangle\langle\psi_i|$. The probability of outcome λ upon measuring an observable A, given state ρ is:

1. $\langle\lambda|\rho|\lambda\rangle = \sum_i P_i \langle \lambda \mid \psi_i\rangle\langle\psi_i \mid \lambda\rangle$
2. $\sum_i P_i |\lambda\psi_i|$ (IE weighting the state by a probability
3. $\operatorname{tr}(|\lambda\rangle\langle\lambda|\rho)$

OK but what about bipartite states with density matrices? Bad news.. tensors of pure states (density matrices). Recall:

$$|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$$
$$|\psi\rangle = \textstyle\sum_{i=1}^n c_i |\psi\rangle\langle\psi|$$
$$= |\psi_1\rangle \otimes |\psi_2\rangle$$

Basically, for vectors, separable means we can write them as a tensor. Now we're motivated to find the analog for density matrices.

Definition 5.9 Let $\rho \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ be a density matrix. Recall that $\rho = \sum_{i=1}^{n} c_i A_{1,i} \otimes A_{2,i}$ where $A_{1,i} \in M_n(\mathbb{C})$ and $A_{2,i} \in M_n(\mathbb{C})$. ♦

What can we say about ρ?

1. ρ is uncorrelated if $\rho_i = \rho_1 \otimes \rho_2$ where ρ_i is a density matrix
2. ρ is "separable" if $\rho = \sum_{i=1}^{n} c_i \rho_{1,i} \otimes \rho_{2,i}$. Note that each $\rho_{1,i}$ and $\rho_{2,i}$ are density matrices where $\sum P_i = 1$
3. If ρ is not "separable", we can call ρ inseparable.

Let's see an example to tie this together.

Example 5.10 Given $|02\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^3$, or $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, consider the following:

$$\rho = |02\rangle\langle 02| = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Is this separable? Our best case scenario is $\rho = \rho_1 \otimes \rho_2 \in M_2 \otimes M_3$. In other words, we need to find the matrices that make this possible. In this case it's pretty easy:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \rho = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = E_{33} \in M_6$$

Therefore, ρ is both pure AND uncorrelated. ♦

Definition 5.11 Suppose $A \in M_n(\mathbb{C}) \otimes M_m(\mathbb{C})$. The **partial trace** of A over $\mathbb{C}^m$ is

$$A = \sum_{i=1}^{n} c_i A_{1,i} \otimes A_{2,i} \tag{5.8}$$

$$A_1 = \mathrm{tr}_2(A) \sum_{i=1}^{n} c_i A_{1,i} \cdot \mathrm{tr}(A_{2,i}) \in M_n \tag{5.9}$$

Basically, if we add a bunch of M_n matrices, we get another M_n matrix.

$$A_2 = \mathrm{tr}_1(A) \sum_{i=1}^{n} c_i \mathrm{tr} A_{1,i} \cdot A_{2,i} \in M_n \tag{5.10}$$

♦

Note that these don't live inside the tensor anymore..

Example 5.12 What can we say about $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle \otimes |10\rangle)$?

$$\begin{gathered}\rho = |\psi\rangle\langle\psi| = \tfrac{1}{2}(|01\rangle + |10\rangle)(\langle 01| + \langle 10|) \\ = \tfrac{1}{2}(\underbrace{|01\rangle\langle 01|}_{E_{22}} + \underbrace{\langle 10|\,|10\rangle}_{E_{23}} + \underbrace{\langle 01|\,|01\rangle}_{E_{32}} + \underbrace{|10\rangle\langle 10|}_{E_{33}}) \in M_2 \otimes M_2 \\ = \tfrac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \in M_4\end{gathered}$$

OK check this out: We need to find some matrices such that

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = A_{11}B \text{ and } \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = A_{21}B \text{ and ...}$$

However, no such "B" can exist, since they all contradict each other! Therefore, these states are NOT uncorrelated. ♦

6 Quantum Information Theory (probably)

Quick highlights reel of my life as a computer scientist so far:

6.1 Classical framework of Information Theory

- A classical (Boolean) bit is an element $x \in \{0, 1\}$
- Data is transmitted in strings of bits (IE a bit string)

Example 6.1 0100 is a bit string of length 4 ♦

Example 6.2 A bit string of length 8 is a *byte*. Also, 00100100 in UTF-8 ASCII is the dollar sign ($) ♦

6.2 Qubits

Definition 6.3 A **qubit** is a unit vector in $\mathbb{C}^2$, IE $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ such that $|a|^2 + |b|^2 = 1$♦

- To extract information form a qubit, we somehow have to *measure* it, which results in *collapse* to either $|0\rangle$ or $|1\rangle$.
- Qutrits ($\mathbb{C}^3$) and qudits($\mathbb{C}^4$) also exist

Definition 6.4 A group/system of n qubits is called a **quantum register**. ♦

Quick classical example to motivate the idea of quantum registers:

Example 6.5 $xyzw$ is a bit string of length 4, and is completely determined by the values of x, y, z, w independent of each other. Basically, there are 4 values out of 2^4 possibilities.♦

OK, suppose we describe a quantum register of n-qubits analogous to the classical framework, meaning that we can write each qubit as

$$a_i\,|0\rangle + b_1\,|1\rangle \text{ for } i = 1, ..., n$$
$$(a_1\,|0\rangle + b_1\,|1\rangle) \otimes (a_2\,|0\rangle + b_2\,|1\rangle) \otimes ... \otimes (a_n\,|0\rangle + b_n\,|1\rangle)$$

This is sick, but not every state in a tensor product has this form, which means it's entangled. So, the state of the system

$$|\psi\rangle = \textstyle\sum_{i_k=0} a_i \cdot i_2 \cdot i_n\,|i_1\rangle \otimes |i_2\rangle \otimes ... \otimes |i_n\rangle \in \mathbb{C}^{2^n} \text{ (holy shit)}$$

is a linear combination of basis vectors.

Example 6.6 Suppose we have two qubits (unit vectors in $\mathbb{C}^2 \otimes \mathbb{C}^2$). The set

$$\left\{|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |\Phi^-\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle), |\Psi^+\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle), |\Psi^-\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right\}$$

is called the Bell Basis, and is an orthonormal basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$. Each Bell State is entangled!♦

Back to classical land to motivate transmission of data with qubits:

Example 6.7 (Classical Repition Code) Suppose a user wants to send the message 1011 over some communication channel. Check it out:

$$1011 \longrightarrow 1001 \text{ IE data loss}$$

We can encode (super elementary) redundancy using 4 blocks of 4-bits.

$$1011 \longrightarrow \underbrace{1111000011111111}_{\text{send this}}$$

What if we receive 1111010011010111? By simple majority, we can see that we encountered some sort of data loss in this transmission. ♦

OK siiick now how can we do this with Qubits? First, here are some operations:

- Measurement, IE collapse ⟶ not ideal
- Unitary transformation ⟶ spin matrices (IE quantum gates)

Here is our first QIT theorem of the semester that illustrates whether example 6.7 is possible in quantum land.

Theorem 6.8 *(Non-Cloning Theorem)*
An unknown quantum system cannot be cloned by unitary transformations.

Basically, if we want to encode things with QIT, we need to develop new tools. IE, there is no such unitary operator u on $H \otimes H$ for all normalized states $|\psi\rangle, |e\rangle \in H$ such that $u(|\psi_e\rangle) = |\psi\psi\rangle$

6.3 Measuring Qubits

Measurement is basically enacting some operation on a system to output a classical bit. This operation is called collapse. To illustrate this operation, we consider a single qubit system in state $|x\rangle = a|0\rangle + b|1\rangle$. The goal is to find the probability that the state in question is $|0\rangle$ (+1 outcome) or $|1\rangle$ (-1 outcome) upon measurement. Basically, we want to use the spectral projections associated with $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

$$= \underbrace{1}_{\lambda_1}\underbrace{|0\rangle\langle 0|}_{M_0} + \underbrace{(-1)}_{\lambda_2}\underbrace{|1\rangle\langle 1|}_{M_1}$$
$$P(0) = a^2 = \langle x| M_0 |x\rangle$$
$$P(1) = b^2 = \langle x| M_1 |x\rangle$$

With this motivation, let's complete an example in a bi-partite system.

Example 6.9 Let $|\psi\rangle$ be a state in a 2-qubit system.

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

Suppose we want to find the probability that the first qubit is $|0\rangle$ or $|1\rangle$ after measurement of $|\psi\rangle$. Basically, we want to consider the observable associated to the Hermitian matrix $A = \sigma_z \otimes I_2$. This means that we should consider the projection operators

$$M_0 = |0\rangle\langle 0| \otimes I_2$$
$$M_1 = |1\rangle\langle 1| \otimes I_2$$

We tensor by I_2 to leave the second qubit alone, and only operate on the first one in the system.

$$|\psi\rangle = |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle)$$
$$= u|0\rangle \otimes (\tfrac{a}{u}|0\rangle + \tfrac{b}{u}|1\rangle) + |v\rangle \otimes (\tfrac{c}{v}|0\rangle + \tfrac{d}{v}|1\rangle)$$

where

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

and

$$v = \sqrt{|c|^2 + |d|^2}$$

OK, now, let's do our projections with these new M_0 and M_1.

$$\begin{gathered} P(0) = \langle\psi| M_0 |\psi\rangle = u^2 \\ P(1) = \langle\psi| M_1 |\psi\rangle = v^2 \end{gathered}$$

More specifically, we're collapsing onto $|0\rangle \otimes (a|0\rangle + b|1\rangle)$ and $|1\rangle \otimes (c|0\rangle + d|0\rangle)$ ♦

Example 6.10 Consider $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We want to measure the system to determine vertical/horizontal polarization.

$$\begin{gathered} (\sigma_z \text{ spectral projections}) \; M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \\ M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \end{gathered}$$

Basically, on the first qubit, we have $M_0 \otimes I$ and $M_1 \otimes I$.

$$\begin{gathered} |\Phi^+\rangle = \tfrac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + 0|0\rangle \otimes |1\rangle + 0|1\rangle \otimes |0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle \\ = \tfrac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle + 0|1\rangle) + \tfrac{1}{\sqrt{2}}|1\rangle \otimes (0|0\rangle + |1\rangle) \; (M_0 \otimes I\,|\Phi^+\rangle) \\ = \tfrac{1}{\sqrt{2}}|0\rangle\langle 0 \mid 0\rangle \otimes (|0\rangle \otimes 0|1\rangle) + 0 \\ = \tfrac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle + 0) = \tfrac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle \\ \langle\Phi^+| M_0 \otimes I\,|\Phi^+\rangle \\ = \tfrac{1}{2}(1+0) = \tfrac{1}{2} \end{gathered}$$

Therefore, the actual probability that the particle will be horizontal in the first qubit is $\frac{1}{2}$.♦

Recall that measurement causes collapse. So what now? Well, we found that $|\Phi^+\rangle$ collapses to $\frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle + 0|1\rangle)$, but note that the measurement also affected the second qubit.

6.4 BB84 Protocol for Quantum Key Distribution (QKD)

A nice example of single qubit measurement is quantum key distribution. Key distribution is a cryptographic concept that pertains to the production and distribution of a key to two parties wishing to communicate securely, by means of encrypting and decryption methods. The unique benefit of quantum key distribution is that two communicating parties can detect eavesdropping of the transfer of keys due to the quantum principal that in general, measurement results in disturbance and often collapse of the system. To i

Example 6.11 Suppose Alice and Bob are using a *one-time pad* encryption technique to communicate with each other. Alice wants to send the byte 00100100 to Bob. They use the BB84 protocol to distribute the encryption key for communication. First, they use the bases β_1 and β_2 to prepare and measure $4N = 32$ photons.

$$\beta_1 = \left\{ \begin{smallmatrix} 0 \mapsto |0\rangle \\ 1 \mapsto |1\rangle \end{smallmatrix} \right\} \text{ and } \beta_2 = \left\{ \begin{smallmatrix} 0 \mapsto |\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ 1 \mapsto |\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{smallmatrix} \right\}$$

Alice sends	0	1	0	0	1	1	0	1	0	0	1	0	0	0	1	0	...
Alice's basis	β_1	β_2	β_1	β_2	β_2	β_1	β_2	β_1	β_2	β_2	β_1	β_1	β_1	β_1	β_2	β_1	...

Then, Alice sends Bob these $4N = 32$ photons, each prepared with one of the two bases β_1 and β_2 at random.

Now, Bob measures each received photons with respect to one of each of the two bases at random.

Alice sends	0	1	0	0	1	1	0	1	0	0	1	0	0	0	1	0	...
Alice's basis	β_1	β_2	β_1	β_2	β_2	β_1	β_2	β_1	β_2	β_2	β_1	β_1	β_1	β_1	β_2	β_1	...
Bob's basis	β_1	β_2	β_2	β_1	β_2	β_2	β_1	β_2	β_1	β_2	β_1	β_1	β_1	β_1	β_2	β_1	...
Bob reads	0	1	?	?	1	?	?	?	?	0	?	0	?	?	?	?	...

$$\text{Where } \langle \psi \,|\nearrow\rangle \, \langle\searrow|\, \psi\rangle = \tfrac{1}{2} \Rightarrow 50/50 \text{ shot} \Rightarrow \, ?$$

We can see that when Bob measures the bits sent by Alice with a basis different than the one she used, he cannot get any discernible information. Next, Alice and Bob talk over a classical line and identify the photons that were prepared and measured using the same basis, or roughly $2N = 16$ photons. These photons are represented by the bits with a definitive collapse, IE non '?'. The remaining roughly $2N = 16$ photons that Alice will send should be prepared and measured according to this same basis. Now, Alice and Bob select $N = 8$ photons among the $2N = 16$ photons at random to detect any tampering on the quantum line.

Alice sends	0	1	1	0	0	1	0	0	1	0	0	0	1	1	1	0
Alice's basis	β_1	β_2	β_2	β_2	β_1	β_1	β_1	β_2	β_1	β_1	β_1	β_2	β_1	β_2	β_2	β_2
Bob's basis	β_1	β_2	β_2	β_2	β_1	β_1	β_1	β_2	β_1	β_1	β_1	β_2	β_1	β_2	β_2	β_2
Bob reads	0	1	1	0	0	1	0	0	1	0	0	0	1	1	1	0

If Eve were listening, they would have intercepted and measured the quantum photons using β_1 or β_2 at random before passing the collapsed state to Bob.

What this comes down to is that Alice and Bob *can absolutely* detect if Eve is EaVEsdropping. This can be easily be seen because despite Alice and Bob confirming the bases on which they communicated, Bob still received inconclusive states in the form of '?'. Said differently, the bits checked in the *Bob reads* column were supposed to 'line up' at this point, SO, we can assume that somebody was in the middle. ⧫

Alice sends	0	1	1	0	0	1	0	0	1	0	0	0	1	1	1	0
Alice's basis	β_1	β_2	β_2	β_2	β_1	β_1	β_1	β_2	β_1	β_1	β_1	β_2	β_1	β_2	β_2	β_2
Eve's basis	β_1	β_2	β_1	β_2	β_1	β_2	β_1	β_2	β_1	β_1	β_2	β_1	β_2	β_2	β_1	β_1
Eve reads/sends	0	1	?	0	0	?	0	0	1	0	?	?	?	1	?	?
Bob's basis	β_1	β_2	β_2	β_2	β_1	β_1	β_1	β_2	β_1	β_1	β_1	β_2	β_1	β_2	β_2	β_2
Bob reads	0	1	?	0	0	?	0	0	1	0	?	?	?	1	?	?

6.5 Quantum Gates

Quick recap: A quantum gate is

- A unitary matrix; IE reversible and allows us to change basis
- How we prepare messages

Now, we'll go over some of the basic quantum logic gates, and compare them to their classical counterparts.

- NOT gate
  Classically, a not gate performs the following actions:

  $$0 \mapsto 1 \text{ and } 0 \mapsto 1$$

  And as a function, the NOT gate operates as $\{0,1\} \mapsto \{0,1\}$, IE it is a bijection. A quantum not gate operates similarly. IE

  $$|0\rangle \mapsto |1\rangle \text{ and } |1\rangle \mapsto |0\rangle$$

  This is done using σ_x which is most often just called 'X'

- AND gate
  Classically, an and gate takes two bits, and outputs a 1 only if the two bits are the same, and is represented as a function by $\{0,1\}^2 \mapsto \{0,1\}$. A quantum and gate operates similarly. IE

  $$|xyz\rangle \mapsto \begin{cases} x = y = 1 & |xy\bar{z}\rangle \\ else \\ |xyz\rangle \end{cases}$$

  $$|101\rangle \overset{\text{QAND}}{\mapsto} |101\rangle$$
  $$|110\rangle \mapsto |111\rangle$$

  The quantum and gate is often called CCNOT.

- XOR gate
  Classically, the exclusive or gate takes two bits as input and outputs a 1 only if the two bits are different, and is represented as a function by $\{0,1\}^2 \mapsto \{0,1\}$. A quantum exclusive or gate operates slightly differently. Check it out:

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |11\rangle \\ |11\rangle &\mapsto |10\rangle \end{aligned}$$

Another useful quantum gate that doesn't exist classically is called the Hadamard gate, which maps the basis states

$$\begin{aligned} |0\rangle &\mapsto \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\mapsto \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

and is used to create an equal superposition of the two states. The Hadamard gate is represented by a matrix as $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. See the exercises for examples of these; we didn't do many in class.

6.6 Quantum Gates as Density Matrices

Quick motivation for the usefulness of density matrices representing quantum gates. The biggest question here is "what happens if quantum gates aren't dependable?" For example, noise in the quantum line or broken circuits could cause disturbances in the data transmitted.

Example 6.12 Imagine we want to send the bit $|10\rangle$ as $|11\rangle$ by applying CNOT. Maybe 80% of the time $|11\rangle$ is sent. Fantastic! But, 15% of the time, $(H \otimes I)|10\rangle$ is sent, and 5% of the time $(H \otimes H)CNOT(H \otimes H)$ is sent. IE, the vector received is

$$0.80\text{CNOT}\,|10\rangle + 0.15(H \otimes I)\,|10\rangle + 0.05\text{CNOT}'\,|10\rangle$$

Low key gross.. But what if we could just send a density matrix?? ♦

Well, first, we need to answer the question of how does the density matrix ρ evolve under a quantum unitary gate U? Vector evolution allows us to apply U as $|\psi\rangle \mapsto U|\psi\rangle$.

Theorem 6.13 *If ρ is a pure state density matrix $\rho = |\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathbb{C}^n$,*

$$\rho = |\psi\rangle\langle\psi| \mapsto (u\,|\psi\rangle)(u\,|\psi\rangle)^\dagger = U\,|\psi\rangle\langle\psi|\,U^\dagger = U\rho U^\dagger$$

We kind of ran out of time here... But there are some cool examples of this application in the exercises.

6.7 Light speed overview of Quantum Decoherence

Let's talk about a possibly multipartite Hilbert system $H_S \otimes H_\epsilon$, which is our hypothetical environment's quantum system. Suppose we only want to measure information about $|\psi\rangle \in H_S$, but when we measure, our environment has state $|\phi\rangle \in H_\epsilon$. Basically, we're actually measuring $|\psi\rangle \otimes |\phi\rangle \in H_S \otimes H_\epsilon$, which is represented by the density matrix $(|\psi\rangle \otimes |\phi\rangle)(|\psi\rangle \otimes |\phi\rangle)^\dagger$. So, in a perfectly isolated quantum system, we would measure ρ_S as it's actually represented supported by our axioms. But, if noise is introduced to the system during an action like measurement, coherence in the system is lost. Basically, quantum decoherence makes our density matrix $\begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^2 & |\beta|^* \end{bmatrix}$ slowly approach $\begin{bmatrix} \sim 0 & \alpha\beta^* \\ \beta\alpha^2 & \sim 0 \end{bmatrix}$. Eventually, it becomes something that is no longer a density matrix and no longer useful to us...

ok bye