

Introduction to Quantum Information Theory

Joshua Parmenter

19 Jan, 2021

Abstract

Will finish this when i actually know what the jeebuz is going on in the class.

Contents

1	Vectors and Vector Spaces	2
1.1	Vector Spaces	2
1.1.1	Relevant Vector Spaces	2
1.2	Complex Number Operations	2
1.2.1	Addition	2
1.2.2	Multiplication	2
1.2.3	Conjugation	2
1.2.4	Modulus	2
1.3	Common Vector Space Notation and Definitions	3
1.3.1	Linear Algebra Terms	3
1.4	Inner/Outer Products, and Norms of Vectors	8
2	Matrices and Linear Transformations	14
2.1	Matrices	14
2.2	Eigenvectors and Eigenvalues	15
2.2.1	Eigenvalues/Eigenvectors	15
2.2.2	Eigenvectors and Eigenvalues Big Picture	17
3	Introduction to Quantum Theory	18
3.1	Quantum Theory Axioms	18
3.1.1	Axiom 1.1: A vector state x is a unit vector in a complex Hilbert space.	18
3.1.2	Axiom 1.2: Linear combinations (or superposition) of the physical states are allowed to act as x vectors.	18
3.1.3	Axiom 2: Observable	18
3.1.4	Axiom 3: The time dependence of a state is governed by the Schrödinger equation	19
3.2	More Introductory Quantum Concepts	20

1 Vectors and Vector Spaces

1.1 Vector Spaces

In modern mathematics, an area of importance is first defining what field the problems are being asked in. When speaking on vectors and vector spaces, it is easiest to work in two main fields of numbers.

1.1.1 Relevant Vector Spaces

1. \mathbb{R} : All Real Numbers $(-\infty, \infty)$

This includes all real numbers from zero to infinity, something of note is that this number field is **not algebraically closed**, meaning not all numbers can be produced from combinations of other numbers in the field. An example of this is $x^2 + 1 = 0$, meaning $x = 1 * i$

2. \mathbb{C} : All Complex Numbers

This number field is **algebraically closed**. This means that every possible number in the field can be produced from combinations of other numbers in the field. This makes sense as two complex numbers multiplied together can produce 1. A completely real number 2. A complex number with a real and imaginary component 3. A complex number with only an imaginary component.

1.2 Complex Number Operations

In the following sections, we will make the assumption $a, b, c, d, e \in \mathbb{R}$

1.2.1 Addition

$$(a + bi) + (c + di) = (a + c) + (b + d)i \quad (1.1)$$

1.2.2 Multiplication

$$(a + bi) * (c + di) = (ac + adi) + (bci - bd) \quad (1.2)$$

1.2.3 Conjugation

$$\overline{a + bi} = (a + bi)^* = a - bi \quad (1.3)$$

1.2.4 Modulus

$$|z| = |a + bi| = \sqrt{a^2 + b^2} \quad (1.4)$$

1.3 Common Vector Space Notation and Definitions

This section is to lay out some of the most important pieces of notation and definitions for the complex mathematics required for this course.

1.3.1 Linear Algebra Terms

Definition 1.1 An element $|v\rangle \in \mathbb{C}^n$ is called a **(ket) vector** and is expressed as a **column** of n complex numbers. The integer n is called the **dimension** of the vector space \mathbb{C}^n . ♦

Definition 1.2 A **linear combination** of $|v_1\rangle, \dots, |v_k\rangle \subset \mathbb{C}^n$ is just a single vector in the form $\lambda_1 |v_1\rangle + \lambda_2 |v_2\rangle + \dots + \lambda_k |v_k\rangle$ for some $\lambda_1, \lambda_2, \dots, \lambda_k \in \mathbb{C}$. ♦

Example 1.3 Create a **linear combination** of $|v_1\rangle = \begin{bmatrix} i \\ 1 \end{bmatrix}$, $|v_2\rangle = \begin{bmatrix} -1 \\ i+1 \end{bmatrix}$

To create a linear combination, we simply must add two complex number constants λ_1, λ_2 in the form shown in **Definition 1.2**, $\lambda_1 |\mathbf{v}_1\rangle + \lambda_2 |\mathbf{v}_2\rangle$.

$$\begin{aligned} \lambda_{final} |v_{final}\rangle &= \lambda_1 |v_1\rangle + \lambda_2 |v_2\rangle & \lambda_1 &= 1 \\ & & \lambda_2 &= 3 + 2i \end{aligned}$$

$$\begin{aligned} \lambda_{final} |v_{final}\rangle &= 1 \begin{bmatrix} i \\ 1 \end{bmatrix} + (3 + 2i) \begin{bmatrix} -1 \\ i+1 \end{bmatrix} \\ &= \begin{bmatrix} i \\ 1 \end{bmatrix} + \begin{bmatrix} -3 - 2i \\ 1 + 5i \end{bmatrix} & (1.5) \\ &= \begin{bmatrix} -3 - i \\ 3 + 5i \end{bmatrix} \end{aligned} \quad \blacklozenge$$

Definition 1.4 Two vectors $|v_1\rangle, |v_2\rangle$ are **linearly independent** if the only way to create the 0 vector from a linear combination is through setting all complex constants $\lambda_1, \lambda_2, \dots, \lambda_k$ to zero in the linear combination formula described in **Definition 1.2**. ♦

Definition 1.5 A **subspace** of complex plane \mathbb{C} is a set $\mathbf{M} \in \mathbb{C}^n$ that satisfies three properties:

- $|0\rangle \in \mathbf{M}$
- $|v\rangle + |u\rangle \in \mathbf{M}$ for all $|v\rangle, |u\rangle$
- $c|v\rangle \in \mathbf{M} \quad \forall \quad |v\rangle \in \mathbf{M}, c \in \mathbb{C}$ ♦

Definition 1.6 The **span** of a set \mathbf{S} is the smallest linear subspace $\in \mathbf{S}$. ♦

Theorem 1.7 (*Span of a set is always a subspace theorem*)

Let $\mathbf{s} = \{|v_1\rangle, |v_2\rangle, \dots, |v_k\rangle\} \subset \mathbb{C}^n$, then $\text{span}(\mathbf{s})$ is a subspace of \mathbb{C}^n

Proof. 1. Note that $|0\rangle = 0|v_1\rangle + 0|v_2\rangle + \dots + 0|v_k\rangle \in \text{span}(\mathbf{s})$.

2. Let $|v\rangle, |u\rangle \in \text{span}(\mathbf{s})$ be arbitrary.

Since $|v\rangle, |u\rangle \in \text{span}(\mathbf{s})$, there exists scalars c_1, c_2, \dots, c_k and d_1, d_2, \dots, d_k such that

$$\begin{aligned} |v\rangle &= c_1 |v_1\rangle, \dots, c_k |v_k\rangle \\ |u\rangle &= d_1 |v_1\rangle, \dots, d_k |v_k\rangle \end{aligned}$$

then,

$$\begin{aligned} |v\rangle + |u\rangle &= (c_1 |v_1\rangle, \dots, c_k |v_k\rangle) + (d_1 |v_1\rangle, \dots, d_k |v_k\rangle) \\ &= (c_1 + d_1) |v_1\rangle + \dots + (c_k + d_k) |v_k\rangle \in \text{span}(\mathbf{s}) \end{aligned}$$

This is true because all of these are linear combinations consisting of a complex constant and a ket vector, which coincides with the **Linear Combination Definition 1.2**.

3. Let $|w\rangle \in \text{span}(\mathbf{s})$ and $c \in \mathbb{C}$. If this is true, then there exists $\lambda_1, \lambda_2, \dots, \lambda_k$ such that $|w\rangle = \lambda_1 |v_1\rangle, \dots, \lambda_k |v_k\rangle$. Consider:

$$\begin{aligned} c|w\rangle &= c|w\rangle \\ &= C(\lambda_1 |v_1\rangle, \dots, \lambda_k |v_k\rangle) \\ &= (C\lambda_1) |v_1\rangle + \dots + (C\lambda_k) |v_k\rangle \end{aligned} \tag{1.6}$$

Equation 1.6 shows that after distributing **C** in, we have another linear combination, which must exist inside of $\text{span}(\mathbf{s})$, and since $\text{span}(\mathbf{s})$ satisfies 1,2,3, $\text{span}(\mathbf{s})$ must be a subspace. ■

Theorem 1.8 *Basis Theorem*

If \mathbf{S} is a set of n linearly independent vectors in \mathbb{C}^n , then $\text{span}(\mathbf{S}) = \mathbb{C}^n$.

Definition 1.9 A **basis** of a subspace $M \subseteq \mathbb{C}^n$ is a set of vectors \mathbf{S} such that

1. \mathbf{S} is linearly independent.

2. $\text{span}(\mathbf{S}) = M$, or in plain English "S spans M" ◆

Definition 1.10 The **dimension** of a space is the number of vectors in it. ◆

Example 1.11 Standard basis of different complex vector spaces.

- Standard Basis for \mathbb{C}^2 : $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

- Standard Basis for \mathbb{C}^n : $\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$

◆

Exercise 1.12 (Vector Space Exercise) Below are some exercises designed to put the concepts in this section to work, in order to further reinforce learning.

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 .

$$\lambda |v\rangle = 1 \begin{bmatrix} 1 \\ -1 \end{bmatrix} + 1 \begin{bmatrix} i \\ 1 \end{bmatrix} - (1 + 200i) \begin{bmatrix} 0 \\ i \end{bmatrix} \quad (1.7)$$

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

$$\alpha |v_1\rangle + \beta |v_2\rangle + \gamma |v_3\rangle = \begin{bmatrix} 1+i \\ 200-i \end{bmatrix}, \quad \alpha = 1, \beta = 1, \gamma = ?$$

$$1 \begin{bmatrix} 1 \\ -1 \end{bmatrix} + 1 \begin{bmatrix} i \\ 1 \end{bmatrix} - \gamma \begin{bmatrix} 0 \\ i \end{bmatrix} = \begin{bmatrix} 1+i \\ 200-i \end{bmatrix} \quad \text{Choose alpha and beta to obtain } \begin{bmatrix} 1+i \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1+i \\ 0 \end{bmatrix} - \gamma \begin{bmatrix} 0 \\ i \end{bmatrix} = \begin{bmatrix} 1+i \\ 200-i \end{bmatrix} \quad \text{Now we must isolate } \gamma$$

$$\begin{bmatrix} 0 \\ \gamma * i \end{bmatrix} = \begin{bmatrix} 0 \\ -200+i \end{bmatrix} \quad \text{We now set the matrix as an equality}$$

$$\gamma * i = -200 + i$$

$$\gamma = -(1 + 200i)$$

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

Since we were able to create a linear combination of the vectors that satisfy the given vector, it is in $\text{Span}(S)$.

- (c) Describe $\text{Span}(S)$ geometrically.

$\text{Span}(S)$ is every possible vector $\in \mathbb{C}^2$

◆

Exercise 1.13 (Linear Independence Exercise) Find the condition under which the following two vectors are linearly independent.

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

$$\begin{bmatrix} x \\ y \\ 3 \end{bmatrix} = \alpha \begin{bmatrix} 2 \\ x - y \\ 1 \end{bmatrix} \tag{1.8}$$

First, we must make this linearly dependent so we know when x and y fail linear independence

$$\alpha = 3 \quad \rightarrow \quad \begin{bmatrix} x \\ y \\ 3 \end{bmatrix} = 3 \begin{bmatrix} 2 \\ x - y \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} x \\ y \\ 3 \end{bmatrix} = \begin{bmatrix} 6 \\ 3(x - y) \\ 3 \end{bmatrix}$$

Now we need to make this an equality to solve for x and y.

$$x = 6 \quad \rightarrow \quad y = 3(x - y)$$

$$y = 3x - 3y$$

$$4y = 18$$

$$y = 9/2(\text{or } 4.5)$$



Exercise 1.14 (Basis Exercise) Show that the set formed by the following vectors is a basis for \mathbb{C}^3

$$|V_1\rangle = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, |V_2\rangle = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, |V_3\rangle = \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}$$

There are two things we must prove in order for a set of vectors to form a basis: linear independence and an equal number of vectors as the dimension of the space.

First we will prove linear independence:

1. Linear Independence Test

$$\begin{aligned} & \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 1 & -1 & 0 \end{bmatrix} \text{ First, we build augmented matrix} \\ \xrightarrow{R_2-R_3} & \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 1 & -1 & 0 \end{bmatrix} \\ \xrightarrow{R_3-R_1} & \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & 0 \end{bmatrix} \\ \xrightarrow{-1*R_2, -\frac{1}{2}*R_3} & \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\ \xrightarrow[\begin{smallmatrix} R_1-R_2 \\ R_1-R_3 \end{smallmatrix}]{R_1-R_2} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{aligned} \tag{1.9}$$

Thus, we have proved that if the only way to obtain the $[0]$ matrix is through $\lambda_1, \dots, \lambda_k = 0$ as mentioned in [Definition 1.4](#), we know that the vectors are **linearly independent**.

2. Dimension Test

Now we must prove that the dimension of the space is equal to the number of the vectors, and since we are working with \mathbb{C}^3 and we have $|V_1\rangle, |V_2\rangle, |V_3\rangle$ we know that our space has three dimensions and we have three vectors, therefore we have just proven that **the given set of vectors forms a basis for \mathbb{C}^3** . \blacklozenge

1.4 Inner/Outer Products, and Norms of Vectors

Definition 1.15 The **dual space of \mathbb{C}^n** (\mathbb{C}^{n*}) is a space of row vectors where there are n entries from \mathbb{C} . ♦

Definition 1.16 A **transpose** is an operation that every column into a row vector and vice versa without changing the order. ♦

Example 1.17 (Example of transpose operation)

$$|V\rangle^\dagger = \begin{bmatrix} 7 \\ 8i \\ \pi + 3i \\ 0 \end{bmatrix}^\dagger \quad (1.10)$$

$$\langle V| = [7 \quad 8i \quad \pi + 3i \quad 0] \quad (1.11)$$

It can be seen that the only difference between **1.10** and **1.11** is that we have converted the column to a row, this is accomplished through the **dagger** (\dagger) being applied to a matrix or vector. ♦

Definition 1.18 Given $|V\rangle, |W\rangle$, the **inner product** of $|V\rangle, |W\rangle$ is $\langle W|V\rangle$ which can also be written as $\langle W| * |V\rangle$.

It should be noted that the inner product of a bra and ket vector will always yield a constant. ♦

Example 1.19 (Example of an Inner Product on \mathbb{R}^n)

$$|V\rangle = \begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix}, |W\rangle = \begin{bmatrix} 5 \\ -2 \\ 1 \end{bmatrix} \quad (1.12)$$

$$\langle W|V\rangle = [5 \quad -2 \quad 1] \begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix} = 5 - 2 + 3 = 6 \quad (1.13)$$

It should be noted that the inner product on \mathbb{R}^n is just the usual dot product. ♦

Example 1.20 (Example of an Inner Product on \mathbb{C}^n)

$$|V\rangle = \begin{bmatrix} i \\ 1 \end{bmatrix}, |W\rangle = \begin{bmatrix} -i \\ -1 \end{bmatrix} \quad (1.14)$$

$$\langle W|V\rangle = [-i \quad -1] \begin{bmatrix} i \\ 1 \end{bmatrix} = 1 - 1 = 0 \quad (1.15)$$

*The inner product yielding 0 means that the two vectors are **orthogonal**.* ♦

Definition 1.21 The norm (or magnitude) of $|V\rangle \in \mathbb{C}^n$ is

$$\| |V\rangle \| := \sqrt{\langle V|V\rangle} \quad (1.16)$$

◆

Example 1.22 (Example of taking the norm of a complex vector)

$$v = [1, 1] \in \mathbb{R}^2$$

$$\| |V\rangle \| := \sqrt{[1 \quad 1] \begin{bmatrix} 1 \\ 1 \end{bmatrix}} = \sqrt{1+1} = \sqrt{2}$$

Two points of note:

1. Can $\langle W|V\rangle$ be complex? **YES**
2. Can $\langle V|V\rangle = \| |V\rangle \|^2 \in \mathbb{C}$? **YES**

◆

Definition 1.23 A set of nonzero vectors $S = \{|V_1\rangle, |V_2\rangle, \dots, |V_k\rangle\} \subseteq \mathbb{C}^n$ is called an **orthogonal set** if $\langle \mathbf{v}_i | \mathbf{v}_j \rangle = 0$ if $\mathbf{i} \neq \mathbf{j}$.

◆

Theorem 1.24 (Orthogonality and Linear Independence Theorem) *In this theorem, we will use what we have learned so far in order to gain a deeper understanding into the properties of orthogonality in a vector space.*

If $S = |V_1\rangle, \dots, |V_k\rangle$ is an orthogonal vector set of nonzero vectors in \mathbb{C}^n , then S is linearly independent.

Proof. Let $c_1, \dots, c_k \in \mathbb{C}$ s.t. $c_1 |v_1\rangle, c_2 |v_2\rangle, \dots, c_k |v_k\rangle = |0\rangle$.

Goal: Show $c_1, \dots, c_k = 0$ using assumption S is orthogonal set.

Let $j \in \{1, \dots, k\}$, then

$$\begin{aligned} \langle v_j | (c_1 |v_1\rangle, \dots, c_k |v_k\rangle) &= \langle v_j | 0 \rangle \\ c_1 \langle v_j | v_1 \rangle + \dots + c_k \langle v_j | v_k \rangle & \\ c_j \langle v_j | v_j \rangle &= \text{Since } S \text{ is an orthogonal set} \end{aligned} \quad (1.17)$$

Since $\langle v_j | v_j \rangle$ can't possibly be 0 because we know that $j \neq 0$, it means that c_k must be zero, which as stated in the **Linear Independence Definition**, means that S is linearly independent. ■

Definition 1.25 A basis is **orthonormal** if two conditions are satisfied:

1. S is an orthogonal set of n unit vectors.
2. $\text{Span}(S) \in \mathbb{C}^n$

In plain English, an orthonormal basis is a basis in which there are exactly the number of vectors as the dimension of the space (from the basis definition) as well as all of those vectors being orthogonal to each other. ◆

Exercise 1.26 (Basis Practice) In this example, there will be multiple transformations completed to gain a better understanding of what a basis is, and what it means to be orthogonal.

1.

$$|b_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad |b_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \quad (1.18)$$

(a) Show that \mathcal{B} is an orthonormal basis for \mathbb{C}^2 .

i. Check orthogonality:

$$\langle b_1 | b_2 \rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = 1 - 1 = 0$$

These two vectors are orthogonal since their inner product is 0.

ii. Check that they are unit vectors: (is the norm one?)

$$\begin{aligned} \| |b_1\rangle \| &= \sqrt{\langle b_1 | b_1 \rangle} = \frac{1}{\sqrt{2}} \sqrt{1 + 1} = \frac{\sqrt{2}}{\sqrt{2}} = 1 \\ \| |b_2\rangle \| &= \sqrt{\langle b_2 | b_2 \rangle} = \frac{1}{\sqrt{2}} \sqrt{1^2 + (-1)^2} = \frac{\sqrt{2}}{\sqrt{2}} = 1 \end{aligned}$$

This means that, since the vectors are orthogonal and unit vectors, they are orthonormal, forming an orthonormal basis for \mathbb{C}^2 .

- (b) Find the coordinates of $|x\rangle = \begin{bmatrix} -2 \\ 1 \end{bmatrix}$ relative to basis \mathcal{B} (i.e. find the scalars such that...)

$$c_1, c_2 \in \mathbb{C} \text{ such that } c_1 |b_1\rangle + c_2 |b_2\rangle = |x\rangle$$

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

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

$$b_1, b_2 \text{ are orthogonal so } \langle b_1 | b_2 \rangle = 0 \text{ so}$$

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

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

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

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

$$b_1, b_2 \text{ are orthogonal so } \langle b_2 | b_1 \rangle = 0 \text{ so}$$

◆

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

$$c_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} -2 \\ 1 \end{bmatrix} = \frac{-3}{\sqrt{2}}$$

Definition 1.27 Define $P_i := |f_i\rangle \langle f_i|$ to be the **projection operator** onto $\text{span}(|f_i\rangle)$ ♦

Proposition 1.28 Let $\mathcal{B} = \{|f_1\rangle, \dots, |f_n\rangle\}$ be an orthonormal basis for \mathbb{C}^n then...

1. $P_i(|v\rangle) \in \text{span}(|f_i\rangle)$
2. $|v\rangle - P_i|v\rangle$ is orthogonal to $|f_i\rangle$
3. $P_i^2 = P_i * P_i = P_i$ Projection will still be the same.
4. $P_i P_j = 0$ shadow on one plane will be "nothing" in the perspective of another plane.
5. $P_i^\dagger = P_i$ self-adjoint
6. $\sum_{i=1}^n P_i = I_n$

Example 1.29 (Outer Product Example) Given $P_2 = \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$, what is $P_1 + P_2$

$$\begin{aligned}
 P_1 &= |f_1\rangle \langle f_1| \\
 &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} * \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \end{bmatrix} \\
 &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \\
 P_1 + P_2 &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \\
 &= \frac{1}{2} \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} \\
 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
 \end{aligned}$$

This is an interesting result, it shows that if you add all of the projections in a space you will get the identity matrix, proof available elsewhere as I am too lazy to type it out. ♦

Why is projection useful?: It allows us to find c_1, \dots, c_k for $|x\rangle = c_1 |f_1\rangle + \dots + c_k |f_k\rangle$ when all $|f\rangle$ are orthogonal to each other.

Theorem 1.30 (The Gram Schmidt Process) *Let $|b_1\rangle, \dots, |b_k\rangle$ be the basis for a subspace M in \mathbb{C}^n . Define the set of vectors $|f_1\rangle, \dots, |f_k\rangle$ as follows:*

Step 1:

Define $|f_1\rangle := |b_1\rangle$.

Step $i+1$:

for $i = 1:k-1$

$$|f_{i+1}\rangle := |b_{i+1}\rangle - \left(\sum_{j=1}^i \frac{|f_j\rangle \langle f_j|}{\langle f_j | f_j \rangle} \right) |b_{i+1}\rangle = |b_{i+1}\rangle - \left(\sum_{j=1}^i \frac{\langle f_j | b_{i+1} \rangle}{\langle f_j | f_j \rangle} \right) |f_j\rangle \quad (1.19)$$

Done

Now normalization step

for $i = 1 : k$

$$|f_i\rangle := \frac{1}{\| |f_i\rangle \|} |f_i\rangle \quad (1.20)$$

Done, now we know that $|f_1\rangle, \dots, |f_k\rangle$ is a orthonormal basis for M

A special thank you for Dr. Hamidi and Dr. Ismert for giving this psuedocode function for Gram Schmidt, I have pulled from it heavily in this page as it is the best way to explain this code.

2 Matrices and Linear Transformations

2.1 Matrices

This section assumes a basic knowledge of matrix operations, and should be a basic overview.

Definition 2.1 $M_{mn}(\mathbb{C})$ = set of all $m \times n$ matrices with complex entries. \blacklozenge

Definition 2.2 $M_n(\mathbb{C}) \equiv M_{nn}(\mathbb{C})$ meaning that it is just a square matrix with $n \times n$ size. \blacklozenge

Example 2.3 (Pauli Matrices)

$$\begin{aligned}\sigma_x &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ \sigma_y &= \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \\ \sigma_z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\end{aligned} \in M_2 \quad (2.21)$$

*These three matrices are called the **Pauli matrices** the basic matrices we will use for quantum computations in the future.* \blacklozenge

Definition 2.4 The **Identity Matrix** (I_n) is the matrix M_n whose columns are the standard basis $|e_1\rangle, \dots, |e_n\rangle$ for \mathbb{C}_n .

$$I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (2.22) \quad \blacklozenge$$

Theorem 2.5 M_n has a well defined matrix multiplication, in general, if $A \in M_{mn}, B \in M_{nk}$.

The matrix $AB = [A|b_1\rangle \dots A|b_k\rangle]$

Example 2.6 (Pauli Matrices in action) For this example, we will be scaling the σ_y Pauli matrix.

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 0 & -3i \\ i & 0 \end{bmatrix} = [1|a_1\rangle \quad 3|a_2\rangle] \quad (2.23)$$

This shows that in general, multiplying a row matrix by a diagonal matrix will scale the row matrix by the respective diagonal matrix value. \blacklozenge

2.2 Eigenvectors and Eigenvalues

2.2.1 Eigenvalues/Eigenvectors

Definition 2.7 An **eigenvalue** for $A \in M_n$ is a complex number $\lambda \in \mathbb{C}$ such that there is a nonzero vector $|x\rangle \in \mathbb{C}^n$ satisfying

$$A|x\rangle = \lambda|x\rangle \quad (2.24)$$

◆

Definition 2.8 A matrix $A \in M_n$ is **diagonalizable** if and only if:

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

◆

Example 2.9 Consider:

$$A = \begin{bmatrix} I_2 & 0 \\ 0 & \sigma_y \end{bmatrix} \equiv \begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \end{bmatrix} \quad (2.25)$$

1. Get eigenvalues and some normalized eigenvectors:

$$\begin{aligned} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix} - \begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{bmatrix} \\ &= \begin{bmatrix} 1-\lambda & 0 & 0 & 0 \\ 0 & 1-\lambda & 0 & 0 \\ 0 & 0 & \lambda & -i \\ 0 & 0 & i & -\lambda \end{bmatrix} \\ &= (1-\lambda)(1-\lambda)[\lambda^2 - 1] = 0 \\ &\lambda = 1, 1, 1, -1 \end{aligned} \quad (2.26)$$

2. Now plug in eigenvalue and find eigenvector:

$$\begin{aligned}
A|e_1\rangle &= |e_1\rangle \\
A|e_2\rangle &= |e_2\rangle \\
A - \lambda * I &= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -i \\ 0 & 0 & i & -1 \end{bmatrix} \\
&\xrightarrow{R_4 + iR_3} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & i \\ 0 & 0 & 0 & 0 \end{bmatrix} \\
&\xrightarrow[-1R_1]{R_1 \leftrightarrow R_3} \begin{bmatrix} 0 & 0 & 1 & -i \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}
\end{aligned}$$

Now we must use this and transfer it into an equation to solve for x_3, x_4

$$x_3 = ix_4$$

Choose $x_4 = 1$

$$|x\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ i \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ i \end{bmatrix} \quad (2.27)$$

These first two arrays are just chosen because there are no x_1, x_2 values in the eigenvector array, so we choose two unit vectors.

3. Finally, normalize the vector.

$$|x\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ i \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 1 \\ i \end{bmatrix}$$

4. Final answer

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} * i \\ 0 & 0 & \frac{1}{\sqrt{2}} * i & \frac{1}{\sqrt{2}} \end{bmatrix}, D = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

◆

2.2.2 Eigenvectors and Eigenvalues Big Picture

1. Self-Adjoint (Hermitian)

$A \in M_n$ is Hermitian if

$$\begin{aligned} A^\dagger &= A \\ \sigma_x^\dagger &= \sigma_x \\ \sigma_y^\dagger &= \sigma_y \\ \sigma_z^\dagger &= \sigma_z \end{aligned} \tag{2.28}$$

Additionally, all Hermitian matrices are diagonalizable, meaning their eigenvalues form an orthonormal basis.

2. Normal Matrices

$$A * A^\dagger = A^\dagger * A \leftrightarrow \text{eigenvectors form orthonormal basis} \tag{2.29}$$

3. Positive semi-definite matrix M_n is:

$$\begin{aligned} \forall |x\rangle \in \mathbb{C}^n, \text{ we have} \\ \langle x|A|x\rangle \geq 0 \text{ where } A|x\rangle = y \end{aligned} \tag{2.30}$$

4. (Unitary Matrices) The following are all equivalent:

- $U \in M_n$ is unitary
- $U^\dagger = U^{-1}$ or $(U^{-1} * U = U * U^{-1} = I_n)$
- $U * U^\dagger = I_n$ or $U^\dagger * U = I_n$ *note: U^\dagger not always equal to U , but they are normal.*
- The column of U form an orthonormal basis for \mathbb{C}^n .
- $\forall |x\rangle, |y\rangle \in \mathbb{C}^n$ and $\langle U_x|U_y\rangle = \langle x|y\rangle$ meaning unitary matrices are rotation matrices.

3 Introduction to Quantum Theory

Now that we have laid out the mathematical framework necessary to understand this subject, it is time to lay out the physics necessary to complete the basis (no pun intended) for Quantum Information Theory.

3.1 Quantum Theory Axioms

These axioms are humans attempts at creating rules and methods of abstractions to describe and understand

3.1.1 Axiom 1.1: A vector state x is a unit vector in a complex Hilbert space.

We want to figure out the photon's (particle) polarization, to figure this out we are going to shoot it at a vertically polarized filter. Classically, $|x\rangle$ should be polarized \uparrow or \rightarrow , if this is the case we expect two outcomes:

1. If $|x\rangle$ goes through filter, then $|x\rangle$ is \uparrow .
2. If $|x\rangle$ is deflected, then $|x\rangle$ is \rightarrow .

3.1.2 Axiom 1.2: Linear combinations (or superposition) of the physical states are allowed to act as x vectors.

Physical States (Choices made by humans to describe quantum mechanics):

$$\uparrow = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \rightarrow = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Something of note, these two vectors form a basis for \mathbb{C}^2 and all combinations are:

$$|x\rangle = \alpha \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \beta \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ where } \|\alpha\|^2 + \|\beta\|^2 = 1$$

To keep track of this choice, we make the matrix $A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ representing vertically polarized filter.

Another note, the e-vals of that matrix are $|v\rangle, |h\rangle$.

Example 3.1 $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ might be a nice to represent a horizontally polarized filter. ◆

3.1.3 Axiom 2: Observable

An observable of a state $|x\rangle$ corresponds to a Hermitian matrix A . $|x\rangle$ is in state $|u\rangle$, an e-vect for A with probability $|\langle u|x\rangle|^2$

Definition 3.2 Expectation value of A (or mean value) of observable associated to A after measurements with respect to many copies of $|\psi\rangle$ is **the weighted average of the expected outcomes**.

$$\langle A \rangle_\psi = \sum_{i=1}^n |\langle u_i | \psi \rangle|^2$$

$$|\psi\rangle = \sum_{i=1}^n c_i |u_i\rangle \text{ where } u_i \text{ is an e-basis from A}$$

◆

3.1.4 Axiom 3: The time dependence of a state is governed by the Schrödinger equation

$$i\hbar \frac{\delta |\psi\rangle}{\delta t} = H |\psi\rangle \quad (3.31)$$

\hbar is reduced Planck's constant

H is Hermitian matrix corresponding to energy of the system **Hamiltonian**.

When H is time invariant (constant), the Schrödinger equation becomes:

$$|\psi(t)\rangle = e^{\frac{-itH}{\hbar}} |\psi(0)\rangle \quad (3.32)$$

3.2 More Introductory Quantum Concepts

Now that the basic framework of what a quantum state is, it is now time to apply these concepts and build on them to further characterize what a quantum system is, and why it is important to us. Prepare yourself, because we are jumping right into an example applying the previous axioms to characterize a *real world* quantum system.

Example 3.3 Consider a physical system with Hamiltonian $H = \frac{\hbar}{2}\omega\sigma_x$ and suppose $|\psi(0)\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ (The first column of σ_z .)

- Find the wave function $|\psi(t)\rangle, t > 0$, which by the Shrödinger equation is:

$$\begin{aligned}
 |\psi(t)\rangle &= \exp \frac{-itH}{\hbar} * |\psi\rangle \\
 &= \exp \left(i \left(\frac{-t}{\hbar} \right) \left(\frac{\hbar}{2} \omega \sigma_x \right) \right) \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\
 &= \exp i \left(\frac{t}{2} \omega \right) \sigma_x \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{where } \frac{t}{2} \omega \text{ is } \alpha \\
 &= \exp i(\alpha) \sigma_x \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\
 &= \left[\cos\left(\frac{t}{2}\omega\right) I + i \sin\left(\frac{t}{2}\omega\right) \sigma_x \right] \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\
 &= \begin{bmatrix} \cos\left(\frac{t}{2}\omega\right) & i \sin\left(\frac{t}{2}\omega\right) \\ i \sin\left(\frac{t}{2}\omega\right) & \cos\left(\frac{t}{2}\omega\right) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\
 |\psi(t)\rangle &= \begin{bmatrix} \cos\left(\frac{\omega t}{2}\right) \\ i \sin\left(\frac{\omega t}{2}\right) \end{bmatrix}
 \end{aligned} \tag{3.33}$$

- Find the probability for the system to have outcome +1 upon measurement of σ_z

$$\begin{aligned}
 P_2 |\psi(t)\rangle &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \cos\left(\frac{\omega t}{2}\right) \\ i \sin\left(\frac{\omega t}{2}\right) \end{bmatrix} = \begin{bmatrix} \cos\left(\frac{\omega t}{2}\right) \\ 0 \end{bmatrix} \\
 P_{\downarrow}(t) &= \left| \cos \frac{\omega t}{2} \right|^2 = \cos^2 \frac{\omega t}{2}
 \end{aligned} \tag{3.34}$$

As you can see, we have picked off the cos out of ψ and in order to compute the probability distribution of the wave, we square the final answer, this will look familiar to a probability and statistics class topic of expected values and distributions (because it is... Wow! never thought it would be useful again)

- Find the probability for the system to have outcome -1 upon measurement of σ_z

$$P_2 |\psi(t)\rangle = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \cos(\frac{\omega t}{2}) \\ i \sin \frac{\omega t}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ i \sin \frac{\omega t}{2} \end{bmatrix} \quad (3.35)$$

$$P_{\downarrow}(t) = |i \sin \frac{\omega t}{2}|^2 = \sin^2 \frac{\omega t}{2} \quad \blacklozenge$$

Same thing as the one above, but notice that this one is picking out the sin in ψ instead using the other diagonal term in the P matrix.

- Find the expectation value under many measurements of σ_z :