2

Complex Vector Spaces

Philosophy is written in that great book which continually lies open before us (I mean the Universe). But one cannot understand this book until one has learned to understand the language and to know the letters in which it is written. It is written in the language of mathematics, and the letters are triangles, circles and other geometric figures. Without these means it is impossible for mankind to understand a single word; without these means there is only vain stumbling in a dark labyrinth.[1]

Galileo Galilei

Quantum theory is cast in the language of complex vector spaces. These are mathematical structures that are based on complex numbers. We learned all that we need about such numbers in Chapter 1. Armed with this knowledge, we can now tackle complex vector spaces themselves.

Section 2.1 goes through the main example of a (finite-dimensional) complex vector space at tutorial pace. Section 2.2 provides formal definitions, basic properties, and more examples. Each of Section 2.3 through Section 2.7 discusses an advanced topic.

Reader Tip. The reader might find some of this chapter to be "just boring math." If you are eager to leap into the quantum world, we suggest reading the first two or three sections before moving on to Chapter 3. Return to Chapter 2 as a reference when needed (using the index and the table of contents to find specific topics). ♡

[1] *... La filosofia é scritta in questo grandissimo libro che continuamente ci sta aperto innanzi a gli occhi (io dico l'universo), ma non si puo intendere se prima non s'impara a intender la lingua, e conoscer i caratteri, ne' quali é scritto. Egli é scritto in lingua matematica, e i caratteri sono triangoli, cerchi, ed altre figure geometriche, senza i quali mezi e impossibile a intenderne umanamente parola; senza questi e un aggirarsi vanamente per un'oscuro laberinto...* (Opere Il Saggiatore p. 171).

A small disclaimer is in order. The theory of complex vector spaces is a vast and beautiful subject. Lengthy textbooks have been written on this important area of mathematics. It is impossible to provide anything more than a small glimpse into the beauty and profundity of this topic in one chapter. Rather than "teaching" our reader complex vector spaces, we aim to cover the bare minimum of concepts, terminology, and notation needed in order to start quantum computing. It is our sincere hope that reading this chapter will inspire further investigation into this remarkable subject.

2.1 $\mathbb{C}^n$ AS THE PRIMARY EXAMPLE

The primary example of a complex vector space is the set of vectors (one-dimensional arrays) of a fixed length with complex entries. These vectors will describe the states of quantum systems and quantum computers. In order to fix our ideas and to see clearly what type of structure this set has, let us carefully examine one concrete example: the set of vectors of length 4. We shall denote this set as $\mathbb{C}^4 = \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$, which reminds us that each vector is an ordered list of four complex numbers.

A typical element of $\mathbb{C}^4$ looks like this:

$$\begin{bmatrix} 6-4i \\ 7+3i \\ 4.2-8.1i \\ -3i \end{bmatrix}. \tag{2.1}$$

We might call this vector V. We denote the jth element of V as $V[j]$. The top row is row number 0 (not 1);[2] hence, $V[1] = 7 + 3i$.

What types of operations can we carry out with such vectors? One operation that seems obvious is to form the **addition** of two vectors. For example, given two vectors of $\mathbb{C}^4$

$$V = \begin{bmatrix} 6-4i \\ 7+3i \\ 4.2-8.1i \\ -3i \end{bmatrix} \quad \text{and} \quad W = \begin{bmatrix} 16+2.3i \\ -7i \\ 6 \\ -4i \end{bmatrix}, \tag{2.2}$$

[2] Computer scientists generally start indexing their rows and columns at 0. In contrast, mathematicians and physicists tend to start indexing at 1. The difference is irrelevant. We shall generally follow the computer science convention (after all, this is a computer science text).

we can add them to form $V + W \in \mathbb{C}^4$ by adding their respective entries:

$$\begin{bmatrix} 6-4i \\ 7+3i \\ 4.2-8.1i \\ -3i \end{bmatrix} + \begin{bmatrix} 16+2.3i \\ -7i \\ 6 \\ -4i \end{bmatrix} = \begin{bmatrix} (6-4i)+(16+2.3i) \\ (7+3i)+(-7i) \\ (4.2-8.1i)+(6) \\ (-3i)+(-4i) \end{bmatrix} = \begin{bmatrix} 22-1.7i \\ 7-4i \\ 10.2-8.1i \\ -7i \end{bmatrix}. \tag{2.3}$$

Formally, this operation amounts to

$$(V+W)[j] = V[j] + W[j]. \tag{2.4}$$

Exercise 2.1.1 Add the following two vectors:

$$\begin{bmatrix} 5+13i \\ 6+2i \\ 0.53-6i \\ 12 \end{bmatrix} + \begin{bmatrix} 7-8i \\ 4i \\ 2 \\ 9.4+3i \end{bmatrix}. \tag{2.5}$$

■

The addition operation satisfies certain properties. For example, because the addition of complex numbers is commutative, addition of complex vectors is also **commutative**:

$$V + W = \begin{bmatrix} (6-4i)+(16+2.3i) \\ (7+3i)+(-7i) \\ (4.2-8.1i)+(6) \\ (-3i)+(-4i) \end{bmatrix} = \begin{bmatrix} 22-1.7i \\ 7-4i \\ 10.2-8.1i \\ -7i \end{bmatrix}$$

$$= \begin{bmatrix} (16+2.3i)+(6-4i) \\ (-7i)+(7+3i) \\ (6)+(4.2-8.1i) \\ (-4i)+(-3i) \end{bmatrix} = W + V. \tag{2.6}$$

Similarly, addition of complex vectors is also **associative**, i.e., given three vectors V, W, and X, we may add them as $(V + W) + X$ or as $V + (W + X)$. Associativity states that the resulting sums are the same:

$$(V + W) + X = V + (W + X). \tag{2.7}$$

Exercise 2.1.2 Formally prove the associativity property. ■

There is also a distinguished vector called **zero**:

$$\mathbf{0} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \tag{2.8}$$

which satisfies the following property: for all vectors $V \in \mathbb{C}^4$, we have

$$V + \mathbf{0} = V = \mathbf{0} + V. \tag{2.9}$$

Formally, $\mathbf{0}$ is defined as $\mathbf{0}[j] = 0$.

Every vector also has an **(additive) inverse** (or **negative**). Consider

$$V = \begin{bmatrix} 6 - 4i \\ 7 + 3i \\ 4.2 - 8.1i \\ -3i \end{bmatrix}. \tag{2.10}$$

There exists in $\mathbb{C}^4$ another vector

$$-V = \begin{bmatrix} -6 + 4i \\ -7 - 3i \\ -4.2 + 8.1i \\ 3i \end{bmatrix} \in \mathbb{C}^4 \tag{2.11}$$

such that

$$V + (-V) = \begin{bmatrix} 6 - 4i \\ 7 + 3i \\ 4.2 - 8.1i \\ -3i \end{bmatrix} + \begin{bmatrix} -6 + 4i \\ -7 - 3i \\ -4.2 + 8.1i \\ 3i \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \mathbf{0}. \tag{2.12}$$

In general, for every vector $W \in \mathbb{C}^4$, there exists a vector $-W \in C^4$ such that $W + (-W) = (-W) + W = \mathbf{0}$. $-W$ is called the **inverse** of W. Formally,

$$(-W)[j] = -(W[j]). \tag{2.13}$$

The set $\mathbb{C}^4$ with the addition, inverse operations, and zero such that the addition is associative and commutative, form something called an **Abelian group**.

What other structure does our set $\mathbb{C}^4$ have? Take an arbitrary complex number, say, $c = 3 + 2i$. Call this number a **scalar**. Take a vector

$$V = \begin{bmatrix} 6+3i \\ 0+0i \\ 5+1i \\ 4 \end{bmatrix}. \tag{2.14}$$

We can **multiply an element by a scalar** by multiplying the scalar with each entry of the vector; i.e.,

$$(3+2i) \cdot \begin{bmatrix} 6+3i \\ 0+0i \\ 5+1i \\ 4 \end{bmatrix} = \begin{bmatrix} 12+21i \\ 0+0i \\ 13+13i \\ 12+8i \end{bmatrix}. \tag{2.15}$$

Formally, for a complex number c and a vector V, we form $c \cdot V$, which is defined as

$$(c \cdot V)[j] = c \times V[j], \tag{2.16}$$

where the $\times$ is complex multiplication. We shall omit the $\cdot$ when the scalar multiplication is understood.

Exercise 2.1.3 Scalar multiply $8 - 2i$ with $\begin{bmatrix} 16+2.3i \\ -7i \\ 6 \\ 5-4i \end{bmatrix}$. ■

Scalar multiplication satisfies the following properties: for all $c, c_1, c_2 \in \mathbb{C}$ and for all $V,\ W \in \mathbb{C}^4$,

- $1 \cdot V = V$,
- $c_1 \cdot (c_2 \cdot V) = (c_1 \times c_2) \cdot V$,
- $c \cdot (V + W) = c \cdot V + c \cdot W$,
- $(c_1 + c_2) \cdot V = c_1 \cdot V + c_2 \cdot V$.

Exercise 2.1.4 Formally prove that $(c_1 + c_2) \cdot V = c_1 \cdot V + c_2 \cdot V$. ■

An Abelian group with a scalar multiplication that satisfies these properties is called a **complex vector space**.

Notice that we have been working with vectors of size 4. However, everything that we have stated about vectors of size 4 is also true for vectors of arbitrary size. So the set $\mathbb{C}^n$ for a fixed but arbitrary n also has the structure of a complex vector space. In fact, these vector spaces will be the primary examples we will be working with for the rest of the book.

Programming Drill 2.1.1 *Write three functions that perform the addition, inverse, and scalar multiplication operations for $\mathbb{C}^n$, i.e., write a function that accepts the appropriate input for each of the operations and outputs the vector.*

2.2 DEFINITIONS, PROPERTIES, AND EXAMPLES

There are many other examples of complex vector spaces. We shall need to broaden our horizon and present a formal definition of a complex vector space.

Definition 2.2.1 *A* **complex vector space** *is a nonempty set $\mathbb{V}$, whose elements we shall call vectors, with three operations*

- *Addition:* $+ : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{V}$
- *Negation:* $- : \mathbb{V} \longrightarrow \mathbb{V}$
- *Scalar multiplication:* $\cdot : \mathbb{C} \times \mathbb{V} \longrightarrow \mathbb{V}$

and a distinguished element called the **zero vector** $\mathbf{0} \in \mathbb{V}$ *in the set. These operations and zero must satisfy the following properties: for all $V, W, X \in \mathbb{V}$ and for all $c, c_1, c_2 \in \mathbb{C}$,*

(i) *Commutativity of addition:* $V + W = W + V$,
(ii) *Associativity of addition:* $(V + W) + X = V + (W + X)$,
(iii) *Zero is an additive identity:* $V + \mathbf{0} = V = \mathbf{0} + V$,
(iv) *Every vector has an inverse:* $V + (-V) = \mathbf{0} = (-V) + V$,
(v) *Scalar multiplication has a unit:* $1 \cdot V = V$,
(vi) *Scalar multiplication respects complex multiplication:*

$$c_1 \cdot (c_2 \cdot V) = (c_1 \times c_2) \cdot V, \tag{2.17}$$

(vii) *Scalar multiplication distributes over addition:*

$$c \cdot (V + W) = c \cdot V + c \cdot W, \tag{2.18}$$

(viii) *Scalar multiplication distributes over complex addition:*

$$(c_1 + c_2) \cdot V = c_1 \cdot V + c_2 \cdot V. \tag{2.19}$$

To recap, any set that has an addition operation, an inverse operation, and a zero element that satisfies Properties (i), (ii), (iii), and (iv) is called an **Abelian group**. If, furthermore, there is a scalar multiplication operation that satisfies all the properties, then the set with the operations is called a **complex vector space**.

Although our main concern is complex vector spaces, we can gain much intuition from real vector spaces.

Definition 2.2.2 *A* **real vector space** *is a nonempty set $\mathbb{V}$ (whose elements we shall call vectors), along with an addition operation and a negation operation. Most important, there is a scalar multiplication that uses $\mathbb{R}$ and not $\mathbb{C}$, i.e.,*

$$\cdot : \mathbb{R} \times \mathbb{V} \longrightarrow \mathbb{V}. \tag{2.20}$$

This set and these operations must satisfy the analogous properties of a complex vector space.

In plain words, a real vector space is like a complex vector space except that we only require the scalar multiplication to be defined for scalars in $\mathbb{R} \subset \mathbb{C}$. From the fact that $\mathbb{R} \subset \mathbb{C}$, it is easy to see that for every $\mathbb{V}$ we have $\mathbb{R} \times \mathbb{V} \subset \mathbb{C} \times \mathbb{V}$. If we have a given

$$\cdot : \mathbb{C} \times \mathbb{V} \longrightarrow \mathbb{V}, \tag{2.21}$$

then we can write

$$\mathbb{R} \times \mathbb{V} \hookrightarrow \mathbb{C} \times \mathbb{V} \longrightarrow \mathbb{V}. \tag{2.22}$$

We conclude that every complex vector space can automatically be given a real vector space structure.

Let us descend from the abstract highlands and look at some concrete examples.

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

Example 2.2.2 $\mathbb{C}^n$, the set of vectors of length n with complex entries, is also a real vector space because every complex vector space is also a real vector space. The operations are the same as those in Example 2.2.1. □

Example 2.2.3 $\mathbb{R}^n$, the set of vectors of length n with real number entries, is a real vector space. Notice that there is no obvious way to make this into a complex vector space. What would the scalar multiplication of a complex number with a real vector be? □

In Chapter 1, we discussed the geometry of $\mathbb{C} = \mathbb{C}^1$. We showed how every complex number can be thought of as a point in a two-dimensional plane. Things get more complicated for $\mathbb{C}^2$. Every element of $\mathbb{C}^2$ involves two complex numbers or four real numbers. One could visualize this as an element of four-dimensional space. However, the human brain is not equipped to visualize four-dimensional space. The most we can deal with is three dimensions. Many times throughout this text, we shall discuss $\mathbb{C}^n$ and then revert to $\mathbb{R}^3$ in order to develop an intuition for what is going on.

It pays to pause for a moment to take an in-depth look at the geometry of $\mathbb{R}^3$. Every vector of $\mathbb{R}^3$ can be thought of as a point in three-dimensional space or equivalently, as an arrow from the origin of $\mathbb{R}^3$ to that point. So the vector $\begin{bmatrix} 5 \\ -7 \\ 6.3 \end{bmatrix}$ shown in Figure 2.1 is 5 units in the x direction, -7 units in the y direction, and 6.3 units in the z direction.

Given two vectors $V = \begin{bmatrix} r_0 \\ r_1 \\ r_2 \end{bmatrix}$ and $V' = \begin{bmatrix} r'_0 \\ r'_1 \\ r'_2 \end{bmatrix}$ of $\mathbb{R}^3$, we may add them to form $\begin{bmatrix} r_0 + r'_0 \\ r_1 + r'_1 \\ r_2 + r'_2 \end{bmatrix}$. Addition can be seen as making a parallelogram in $\mathbb{R}^3$ where you attach the beginning of one arrow to the end of the other one. The result of the addition is

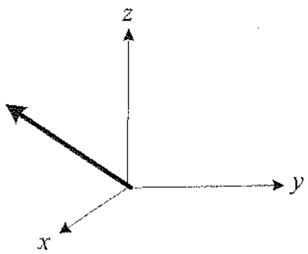

Figure 2.1. A vector in three dimensional space.

the composition of the arrows (see Figure 2.2). The reason that we can be ambiguous about which arrow comes first demonstrates the commutativity property of addition.

Given a vector $V = \begin{bmatrix} r_0 \\ r_1 \\ r_2 \end{bmatrix}$ in $\mathbb{R}^3$, we form the inverse $-V = \begin{bmatrix} -r_0 \\ -r_1 \\ -r_2 \end{bmatrix}$ by looking at the arrow in the opposite direction with respect to all dimensions (as in Figure 2.3).

And finally, the scalar multiplication of a real number r and a vector $V = \begin{bmatrix} r_0 \\ r_1 \\ r_2 \end{bmatrix}$ is $r \cdot V = \begin{bmatrix} rr_0 \\ rr_1 \\ rr_2 \end{bmatrix}$, which is simply the vector V stretched or shrunk by r (as in Figure 2.4).

It is useful to look at some of the properties of a vector space from the geometric point of view. For example, consider the property $r \cdot (V + W) = r \cdot V + r \cdot W$. This corresponds to Figure 2.5.

Exercise 2.2.1 Let $r_1 = 2$, $r_2 = 3$, and $V = \begin{bmatrix} 2 \\ -4 \\ 1 \end{bmatrix}$. Verify Property (vi), i.e., calculate $r_1 \cdot (r_2 \cdot V)$ and $(r_1 \times r_2) \cdot V$ and show that they coincide. ■

Exercise 2.2.2 Draw pictures in $\mathbb{R}^3$ that explain Properties (vi) and (viii) of the definition of a real vector space. ■

Let us continue our list of examples.

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

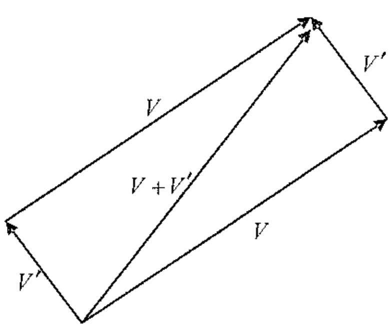

Figure 2.2. Vector addition.

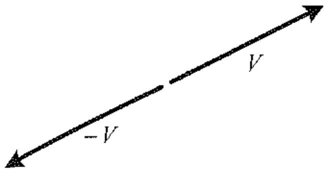

Figure 2.3. Inverse of a vector.

For a given $A \in \mathbb{C}^{m \times n}$, we denote the complex entry in the jth row and the kth column as $A[j,k]$ or $c_{j,k}$. We shall denote the jth row as $A[j,-]$ and the kth column as $A[-,k]$. Several times throughout the text we shall show the row and column numbers explicitly to the left and top of the square brackets:

$$A = \begin{array}{c} \\ \mathbf{0} \\ \mathbf{1} \\ \vdots \\ \boldsymbol{m-1} \end{array} \begin{array}{c} \begin{array}{cccc} \mathbf{0} & \mathbf{1} & \cdots & \boldsymbol{n-1} \end{array} \\ \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,n-1} \end{bmatrix} \end{array}. \tag{2.23}$$

The operations for $\mathbb{C}^{m \times n}$ are given as follows: Addition is

$$\begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,n-1} \end{bmatrix} + \begin{bmatrix} d_{0,0} & d_{0,1} & \cdots & d_{0,n-1} \\ d_{1,0} & d_{1,1} & \cdots & d_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ d_{m-1,0} & d_{m-1,1} & \cdots & d_{m-1,n-1} \end{bmatrix}$$

$$= \begin{bmatrix} c_{0,0}+d_{0,0} & c_{0,1}+d_{0,1} & \cdots & c_{0,n-1}+d_{0,n-1} \\ c_{1,0}+d_{1,0} & c_{1,1}+d_{1,1} & \cdots & c_{1,n-1}+d_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0}+d_{m-1,0} & c_{m-1,1}+d_{m-1,1} & \cdots & c_{m-1,n-1}+d_{m-1,n-1} \end{bmatrix}. \tag{2.24}$$

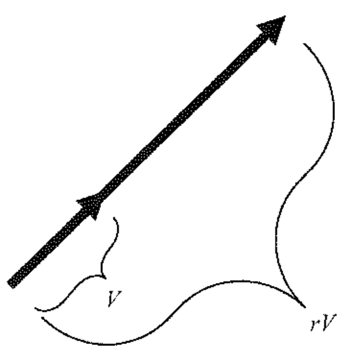

Figure 2.4. A real multiple of a vector.

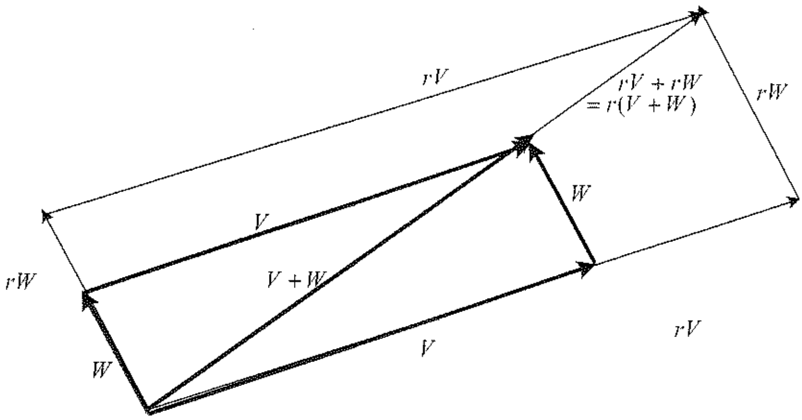

Figure 2.5. Scalar multiplication distributes over addition.

The inverse operation is given as

$$-\begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,n-1} \end{bmatrix} = \begin{bmatrix} -c_{0,0} & -c_{0,1} & \cdots & -c_{0,n-1} \\ -c_{1,0} & -c_{1,1} & \cdots & -c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ -c_{m-1,0} & -c_{m-1,1} & \cdots & -c_{m-1,n-1} \end{bmatrix}. \tag{2.25}$$

Scalar multiplication is given as

$$c \cdot \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,n-1} \end{bmatrix}$$

$$= \begin{bmatrix} c \times c_{0,0} & c \times c_{0,1} & \cdots & c \times c_{0,n-1} \\ c \times c_{1,0} & c \times c_{1,1} & \cdots & c \times c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c \times c_{m-1,0} & c \times c_{m-1,1} & \cdots & c \times c_{m-1,n-1} \end{bmatrix}. \tag{2.26}$$

Formally, these operations can be described by the following formulas:

For two matrices, $A, B \in \mathbb{C}^{m \times n}$, we add them as

$$(A + B)[j, k] = A[j, k] + B[j, k]. \tag{2.27}$$

The inverse of A is

$$(-A)[j, k] = -(A[j, k]). \tag{2.28}$$

The scalar multiplication of A with a complex number $c \in \mathbb{C}$ is

$$(c \cdot A)[j,k] = c \times A[j,k]. \tag{2.29}$$

Exercise 2.2.3 Let $c_1 = 2i$, $c_2 = 1+2i$, and $A = \begin{bmatrix} 1-i & 3 \\ 2+2i & 4+i \end{bmatrix}$. Verify Properties (vi) and (viii) in showing $\mathbb{C}^{2\times 2}$ is a complex vector space. ■

Exercise 2.2.4 Show that these operations on $\mathbb{C}^{m\times n}$ satisfy Properties (v), (vi), and (viii) of being a complex vector space. ■

Programming Drill 2.2.1 *Convert your functions from the last programming drill so that instead of accepting elements of $\mathbb{C}^n$, they accept elements of $\mathbb{C}^{m\times n}$.*

When $n = 1$, the matrices $\mathbb{C}^{m\times n} = \mathbb{C}^{m\times 1} = \mathbb{C}^m$, which we dealt with in Section 2.1. Thus, we can think of vectors as special types of matrices.

When $m = n$, the vector space $\mathbb{C}^{n\times n}$ has more operations and more structure than just a complex vector space. Here are three operations that one can perform on an $A \in \mathbb{C}^{n\times n}$:

- The **transpose** of A, denoted A^T, is defined as
$$A^T[j,k] = A[k,j]. \tag{2.30}$$
- The **conjugate** of A, denoted $\overline{A}$, is the matrix in which each element is the complex conjugate of the corresponding element of the original matrix,[3] i.e., $\overline{A}[j,k] = \overline{A[j,k]}$.
- The transpose operation and the conjugate operation are combined to form the **adjoint** or **dagger** operation. The adjoint of A, denoted as $A^\dagger$, is defined as $A^\dagger = (\overline{A})^T = \overline{(A^T)}$ or $A^\dagger[j,k] = \overline{A[k,j]}$.

Exercise 2.2.5 Find the transpose, conjugate, and adjoint of

$$\begin{bmatrix} 6-3i & 2+12i & -19i \\ 0 & 5+2.1i & 17 \\ 1 & 2+5i & 3-4.5i \end{bmatrix}. \tag{2.31}$$

■

These three operations are defined even when $m \neq n$. The transpose and adjoint are both functions from $\mathbb{C}^{m\times n}$ to $\mathbb{C}^{n\times m}$.

These operations satisfy the following properties for all $c \in \mathbb{C}$ and for all A, $B \in \mathbb{C}^{m\times n}$:

(i) Transpose is idempotent: $(A^T)^T = A$.
(ii) Transpose respects addition: $(A+B)^T = A^T + B^T$.
(iii) Transpose respects scalar multiplication: $(c \cdot A)^T = c \cdot A^T$.

[3] This notation is overloaded. It is an operation on complex numbers and complex matrices.

(iv) Conjugate is idempotent: $\overline{\overline{A}} = A$.
(v) Conjugate respects addition: $\overline{A + B} = \overline{A} + \overline{B}$.
(vi) Conjugate respects scalar multiplication: $\overline{c \cdot A} = \overline{c} \cdot \overline{A}$.
(vii) Adjoint is idempotent: $(A^\dagger)^\dagger = A$.
(viii) Adjoint respects addition: $(A + B)^\dagger = A^\dagger + B^\dagger$.
(ix) Adjoint relates to scalar multiplication: $(c \cdot A)^\dagger = \overline{c} \cdot A^\dagger$.

Exercise 2.2.6 Prove that conjugation respects scalar multiplication, i.e., $\overline{c \cdot A} = \overline{c} \cdot \overline{A}$. ■

Exercise 2.2.7 Prove Properties (vii), (viii), and (ix) using Properties (i) – (vi). ■

The transpose shall be used often in the text to save space. Rather than writing

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} \tag{2.32}$$

which requires more space, we write $[c_0, c_1, \cdots, c_{n-1}]^T$.

When $m = n$, there is another binary operation that is used: **matrix multiplication**. Consider the following two 3-by-3 matrices:

$$A = \begin{bmatrix} 3+2i & 0 & 5-6i \\ 1 & 4+2i & i \\ 4-i & 0 & 4 \end{bmatrix}, \quad B = \begin{bmatrix} 5 & 2-i & 6-4i \\ 0 & 4+5i & 2 \\ 7-4i & 2+7i & 0 \end{bmatrix}. \tag{2.33}$$

We form the matrix product of A and B, denoted $A \star B$. $A \star B$ will also be a 3-by-3 matrix. $(A \star B)[0, 0]$ will be found by multiplying each element of the 0th row of A with the corresponding element of the 0th column of B. We then sum the results:

$$\begin{aligned} (A \star B)[0, 0] &= ((3+2i) \times 5) + (0 \times 0) + ((5-6i) \times (7-4i)) \\ &= (15+10i) + (0) + (11-62i) = 26-52i. \end{aligned} \tag{2.34}$$

The $(A \star B)[j, k]$ entry can be found by multiplying each element of $A[j, -]$ with the appropriate element of $B[-, k]$ and summing the results. So,

$$(A \star B) = \begin{bmatrix} 26-52i & 60+24i & 26 \\ 9+7i & 1+29i & 14 \\ 48-21i & 15+22i & 20-22i \end{bmatrix}. \tag{2.35}$$

Exercise 2.2.8 Find $B \star A$. Does it equal $A \star B$? ■

Matrix multiplication is defined in a more general setting. The matrices do not have to be square. Rather, the number of columns in the first matrix must be the same as the number of rows in the second one. Matrix multiplication is a binary operation

$$\star : \mathbb{C}^{m\times n} \times \mathbb{C}^{n\times p} \longrightarrow \mathbb{C}^{m\times p}. \tag{2.36}$$

Formally, given A in $\mathbb{C}^{m\times n}$ and B in $\mathbb{C}^{n\times p}$, we construct $A \star B$ in $\mathbb{C}^{m\times p}$ as

$$(A \star B)[j,k] = \sum_{h=0}^{n-1} (A[j,h] \times B[h,k]). \tag{2.37}$$

When the multiplication is understood, we shall omit the $\star$.

For every n, there is a special n-by-n matrix called the **identity matrix**,

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}, \tag{2.38}$$

that plays the role of a unit of matrix multiplication. When n is understood, we shall omit it.

Matrix multiplication satisfies the following properties: For all A, B, and C in $\mathbb{C}^{n\times n}$,

(i) Matrix multiplication is associative: $(A \star B) \star C = A \star (B \star C)$.
(ii) Matrix multiplication has I_n as a unit: $I_n \star A = A = A \star I_n$.
(iii) Matrix multiplication distributes over addition:

$$A \star (B + C) = (A \star B) + (A \star C), \tag{2.39}$$

$$(B + C) \star A = (B \star A) + (C \star A). \tag{2.40}$$

(iv) Matrix multiplication respects scalar multiplication:

$$c \cdot (A \star B) = (c \cdot A) \star B = A \star (c \cdot B). \tag{2.41}$$

(v) Matrix multiplication relates to the transpose:

$$(A \star B)^T = B^T \star A^T. \tag{2.42}$$

(vi) Matrix multiplication respects the conjugate:

$$\overline{A \star B} = \overline{A} \star \overline{B}. \tag{2.43}$$

(vii) Matrix multiplication relates to the adjoint:

$$(A \star B)^\dagger = B^\dagger \star A^\dagger. \tag{2.44}$$

Notice that commutativity is *not* a basic property of matrix multiplication. This fact will be very important in quantum mechanics.

Exercise 2.2.9 Prove Property (v) in the above list. ■

Exercise 2.2.10 Use A and B from Equation (2.33) and show that $(A \star B)^{\dagger} = B^{\dagger} \star A^{\dagger}$. ■

Exercise 2.2.11 Prove Property (vii) from Properties (v) and (vi). ■

Definition 2.2.3 *A complex vector space* $\mathbb{V}$ *with a multiplication* $\star$ *that satisfies the first four properties is called a* **complex algebra**.

Programming Drill 2.2.2 *Write a function that accepts two complex matrices of the appropriate size. The function should do matrix multiplication and return the result.*

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

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

Programming Drill 2.2.3 *Write a function that accepts a vector and a matrix and outputs the vector resulting from the "action."*

We return to our list of examples.

Example 2.2.5 $\mathbb{C}^{m\times n}$, the set of all m-by-n matrices (two-dimensional arrays) with complex entries, is a real vector space. (Remember: Every complex vector space is also a real vector space.) □

Example 2.2.6 $\mathbb{R}^{m\times n}$, the set of all m-by-n matrices (two-dimensional arrays) with real entries, is a real vector space. □

Definition 2.2.4 *Given two complex vector spaces* $\mathbb{V}$ *and* $\mathbb{V}'$, *we say that* $\mathbb{V}$ *is a* **complex subspace** *of* $\mathbb{V}'$ *if* $\mathbb{V}$ *is a subset of* $\mathbb{V}'$ *and the operations of* $\mathbb{V}$ *are restrictions of operations of* $\mathbb{V}'$.

Equivalently, $\mathbb{V}$ is a complex subspace of $\mathbb{V}'$ if $\mathbb{V}$ is a subset of the set $\mathbb{V}'$ and

(i) $\mathbb{V}$ is closed under addition: For all V_1 and V_2 in $\mathbb{V}$, $V_1 + V_2 \in \mathbb{V}$.
(ii) $\mathbb{V}$ is closed under scalar multiplication: For all $c \in \mathbb{C}$ and $V \in \mathbb{V}$, $c \cdot V \in \mathbb{V}$.

[4] This might seem reminiscent of computer graphics. In fact, there is a vague relationship that we shall see when we discuss the Bloch sphere (in Chapter 5) and unitary matrices.

It turns out that being closed under addition and multiplication implies that $\mathbb{V}$ is also closed under inverse and that $\mathbf{0} \in \mathbb{V}$.

Example 2.2.7 Consider the set of all vectors of $\mathbb{C}^9$ with the second, fifth, and eighth position elements being 0:

$$[c_0, c_1, 0, c_3, c_4, 0, c_6, c_7, 0]^T. \tag{2.45}$$

It is not hard to see that this is a complex subspace of $\mathbb{C}^9$. We shall see in a few moments that this subspace is the "same" as $\mathbb{C}^6$. □

Example 2.2.8 Consider the set $Poly_n$ of polynomials of degree n or less in one variable with coefficients in $\mathbb{C}$.

$$P(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n. \tag{2.46}$$

$Poly_n$ forms a complex vector space. □

For completeness, let us go through the operations. Addition is given as

$$\begin{aligned} P(x) + Q(x) &= (c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n) + (d_0 + d_1 x + d_2 x^2 + \cdots + d_n x^n) \\ &= (c_0 + d_0) + (c_1 + d_1)x + (c_2 + d_2)x^2 + \cdots + (c_n + d_n)x^n. \end{aligned} \tag{2.47}$$

Negation is given as

$$-P(x) = -c_0 - c_1 x - c_2 x^2 - \cdots - c_n x^n. \tag{2.48}$$

Scalar multiplication by $c \in \mathbb{C}$ is given as

$$c \cdot P(x) = c \times c_0 + c \times c_1 x + c \times c_2 x^2 + \cdots + c \times c_n x^n. \tag{2.49}$$

Exercise 2.2.12 Show that $Poly_n$ with these operations satisfies the properties of being a complex vector space. ■

Exercise 2.2.13 Show that $Poly_5$ is a complex subspace of $Poly_7$. ■

Example 2.2.9 Polynomials in one variable of degree n or less with coefficients in $\mathbb{C}$ also form a real vector space. □

Example 2.2.10 Polynomials in one variable of degree n or less with coefficients in $\mathbb{R}$

$$P(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_n x^n \tag{2.50}$$

form a real vector space. □

Definition 2.2.5 *Let $\mathbb{V}$ and $\mathbb{V}'$ be two complex vector spaces. A* **linear map** *from $\mathbb{V}$ to $\mathbb{V}'$ is a function $f : \mathbb{V} \longrightarrow \mathbb{V}'$ such that for all $V,\ V_1,\ V_2 \in \mathbb{V}$, and $c \in \mathbb{C}$,*

(i) *f respects the addition: $f(V_1 + V_2) = f(V_1) + f(V_2)$,*
(ii) *f respects the scalar multiplication: $f(c \cdot V) = c \cdot f(V)$.*

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

Computer scientists usually store a polynomial as the array of its coefficients, i.e., a polynomial with $n+1$ complex coefficients is stored as an $n+1$ vector. So it is not surprising that $Poly_n$ is the "same" as $\mathbb{C}^{n+1}$. We will now formulate what it means for two vector spaces to be the "same."

Definition 2.2.6 *Two complex vector spaces* $\mathbb{V}$ *and* $\mathbb{V}'$ *are* **isomorphic** *if there is a one-to-one onto linear map* $f : \mathbb{V} \longrightarrow \mathbb{V}'$. *Such a map is called an* **isomorphism**. *When two vector spaces are isomorphic, it means that the names of the elements of the vector spaces are renamed but the structure of the two vector spaces are the same. Two such vector spaces are "essentially the same" or "the same up to isomorphism."*

Exercise 2.2.14 Show that all real matrices of the form

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix} \tag{2.51}$$

comprise a real subspace of $\mathbb{R}^{2\times 2}$. Then show that this subspace is isomorphic to $\mathbb{C}$ via the map $f : \mathbb{C} \longrightarrow \mathbb{R}^{2\times 2}$ that is defined as

$$f(x+iy) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}. \tag{2.52}$$

■

Example 2.2.11 Consider the set $Func(\mathbb{N}, \mathbb{C})$ of functions from the natural numbers $\mathbb{N}$ to the complex numbers $\mathbb{C}$. Given two functions $f : \mathbb{N} \longrightarrow \mathbb{C}$ and $g : \mathbb{N} \longrightarrow \mathbb{C}$, we may add them to form

$$(f+g)(n) = f(n) + g(n). \tag{2.53}$$

The additive inverse of f is

$$(-f)(n) = -(f(n)). \tag{2.54}$$

The scalar multiple of $c \in \mathbb{C}$ and f is the function

$$(c \cdot f)(n) = c \times f(n). \tag{2.55}$$

Because the operations are determined by their values at each of their "points" in the input, the constructed functions are said to be constructed **pointwise**. □

Exercise 2.2.15 Show that $Func(\mathbb{N}, \mathbb{C})$ with these operations forms a complex vector space. ■

Example 2.2.12 We can generalize $Func(\mathbb{N}, \mathbb{C})$ to other sets of functions. For any $a < b$ in $\mathbb{R}$, the set of functions from the interval $[a, b] \subseteq \mathbb{R}$ to $\mathbb{C}$ denoted $Func([a, b], \mathbb{C})$ is a complex vector space. □

Exercise 2.2.16 Show that $Func(\mathbb{N}, \mathbb{R})$ and $Func([a, b], \mathbb{R})$ are real vector spaces. ■

Example 2.2.13 There are several ways of constructing new vector spaces from existing ones. Here we see one method and Section 2.7 describes another. Let $(\mathbb{V}, +, -, \mathbf{0}, \cdot)$ and $(\mathbb{V}', +', -', \mathbf{0}', \cdot')$ be two complex vector spaces. We construct a new complex vector space $(\mathbb{V} \times \mathbb{V}', +'', -'', \mathbf{0}'', \cdot'')$ called the **Cartesian product**[5] or the **direct sum** of $\mathbb{V}$ and $\mathbb{V}'$. The vectors are ordered pairs of vectors $(V, V') \in \mathbb{V} \times \mathbb{V}'$. Operations are performed pointwise:

$$(V_1, V_1') +'' (V_2, V_2') = (V_1 + V_2, V_1' +' V_2'), \tag{2.56}$$

$$-''(V, V') = (-V, -'V'), \tag{2.57}$$

$$\mathbf{0}'' = (\mathbf{0}, \mathbf{0}'), \tag{2.58}$$

$$c \cdot'' (V, V') = (c \cdot V, c \cdot' V'). \tag{2.59}$$

□

Exercise 2.2.17 Show that $\mathbb{C}^m \times \mathbb{C}^n$ is isomorphic to $\mathbb{C}^{m+n}$. ■

Exercise 2.2.18 Show that $\mathbb{C}^m$ and $\mathbb{C}^n$ are each a complex subspace of $\mathbb{C}^m \times \mathbb{C}^n$. ■

2.3 BASIS AND DIMENSION

A basis of a vector space is a set of vectors of that vector space that is special in the sense that all other vectors can be uniquely written in terms of these basis vectors.

Definition 2.3.1 *Let $\mathbb{V}$ be a complex (real) vector space. $V \in \mathbb{V}$ is a* **linear combination** *of the vectors $V_0, V_1, \ldots, V_{n-1}$ in $\mathbb{V}$ if V can be written as*

$$V = c_0 \cdot V_0 + c_1 \cdot V_1 + \cdots + c_{n-1} \cdot V_{n-1} \tag{2.60}$$

for some $c_0, c_1, \ldots, c_{n-1}$ in $\mathbb{C}$ ($\mathbb{R}$).

Let us return to $\mathbb{R}^3$ for examples.

[5] A note to the meticulous reader: Although we used $\times$ for the product of two complex numbers, here we use it for the Cartesian product of sets and the Cartesian product of vector spaces. We feel it is better to overload known symbols than to introduce a plethora of new ones.

Example 2.3.1 As

$$3\begin{bmatrix} 5 \\ -2 \\ 3 \end{bmatrix} + 5\begin{bmatrix} 0 \\ 1 \\ 4 \end{bmatrix} - 4\begin{bmatrix} -6 \\ 1 \\ 0 \end{bmatrix} + 2.1\begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 45.3 \\ -2.9 \\ 31.1 \end{bmatrix}, \tag{2.61}$$

we say that

$$[45.3, -2.9, 31.1]^T \tag{2.62}$$

is a linear combination of

$$\begin{bmatrix} 5 \\ -2 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 4 \end{bmatrix}, \begin{bmatrix} -6 \\ 1 \\ 0 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix}. \tag{2.63}$$

□

Definition 2.3.2 *A set* $\{V_0, V_1, \ldots, V_{n-1}\}$ *of vectors in* $\mathbb{V}$ *is called* **linearly independent** *if*

$$\mathbf{0} = c_0 \cdot V_0 + c_1 \cdot V_1 + \cdots + c_{n-1} \cdot V_{n-1} \tag{2.64}$$

implies that $c_0 = c_1 = \cdots = c_{n-1} = 0$. *This means that the only way that a linear combination of the vectors can be the zero vector is if all the* c_j *are zero.*

It can be shown that this definition is equivalent to saying that for any nonzero $V \in \mathbb{V}$, there are *unique* coefficients $c_0, c_1, \ldots, c_{n-1}$ in $\mathbb{C}$ such that

$$V = c_0 \cdot V_0 + c_1 \cdot V_1 + \cdots + c_{n-1} \cdot V_{n-1}. \tag{2.65}$$

The set of vectors are called linearly independent because each of the vectors in the set $\{V_0, V_1, \ldots, V_{n-1}\}$ cannot be written as a combination of the others in the set.

Example 2.3.2 The set of vectors

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\} \tag{2.66}$$

is linearly independent because the only way that

$$\mathbf{0} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = x\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + y\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + z\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \tag{2.67}$$

can occur is if $0 = x$, $0 = x + y$, and $0 = x + y + z$. By substitution, we see that $x = y = z = 0$. □

Example 2.3.3 The set of vectors

$$\left\{\begin{bmatrix}1\\1\\1\end{bmatrix},\begin{bmatrix}0\\1\\1\end{bmatrix},\begin{bmatrix}2\\-1\\-1\end{bmatrix}\right\} \tag{2.68}$$

is not linearly independent (called **linearly dependent**) because

$$\mathbf{0}=\begin{bmatrix}0\\0\\0\end{bmatrix}=x\begin{bmatrix}1\\1\\1\end{bmatrix}+y\begin{bmatrix}0\\1\\1\end{bmatrix}+z\begin{bmatrix}2\\-1\\-1\end{bmatrix} \tag{2.69}$$

can happen when $x = 2$, $y = -3$, and $z = -1$. □

Exercise 2.3.1 Show that the set of vectors

$$\left\{\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}3\\0\\2\end{bmatrix},\begin{bmatrix}1\\-4\\-4\end{bmatrix}\right\} \tag{2.70}$$

is not linearly independent. ■

Definition 2.3.3 *A set* $\mathcal{B} = \{V_0, V_1, \ldots, V_{n-1}\} \subseteq \mathbb{V}$ *of vectors is called a* **basis** *of a (complex) vector space* $\mathbb{V}$ *if both*

(i) *every,* $V \in \mathbb{V}$ *can be written as a linear combination of vectors from* $\mathcal{B}$ *and*
(ii) $\mathcal{B}$ *is linearly independent.*

Example 2.3.4 $\mathbb{R}^3$ has a basis

$$\left\{\begin{bmatrix}1\\1\\1\end{bmatrix},\begin{bmatrix}0\\1\\1\end{bmatrix},\begin{bmatrix}0\\0\\1\end{bmatrix}\right\}. \tag{2.71}$$

□

Exercise 2.3.2 Verify that the preceding three vectors are in fact a basis of $\mathbb{R}^3$. ■

There may be many sets that each form a basis of a particular vector space but there is also a basis that is easier to work with called the **canonical basis** or the **standard basis**. Many of the examples that we will deal with have canonical basis. Let us look at some examples of canonical basis.

- $\mathbb{R}^3$:

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

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

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

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

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

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

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

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

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

- $Poly_n$: The canonical basis is formed by the following set of monomials:

$$1, x, x^2, \ldots, x^n. \tag{2.77}$$

- $Func(\mathbb{N}, \mathbb{C})$: The canonical basis is composed of a countably infinite[6] number of functions f_j $(j = 0, 1, 2, \ldots)$, where f_j is defined as

$$f_j(n) = \begin{cases} 1, & \text{if } j = n, \\ 0, & \text{otherwise.} \end{cases} \tag{2.78}$$

The definition previously given of a finite linear combination can easily be generalized to an infinite linear combination. It is not hard to see that any function $f \in Func(\mathbb{N}, \mathbb{C})$ can be written as the infinite sum

$$f = \sum_{j=0}^{\infty} c_j \cdot f_j, \tag{2.79}$$

where $c_j = f(j)$. It is also not hard to see that these functions are linearly independent. Hence they form a basis for $Func(\mathbb{N}, \mathbb{C})$.

- (For the calculus-savvy reader.) $Func([a, b], \mathbb{C})$: The canonical basis is composed of an uncountably infinite number of functions f_r for $r \in [a, b] \subseteq \mathbb{R}$, which is defined as

$$f_r(x) = \begin{cases} 1, & \text{if } r = x, \\ 0, & \text{otherwise.} \end{cases} \tag{2.80}$$

These functions are linearly independent. Analogous to the last countable discrete summation given in Equation (2.79), we may write any function $f \in Func([a, b], \mathbb{C})$ as an integral:

$$f = \int_a^b c_r \cdot f_r, \tag{2.81}$$

where $c_r = f(r)$. Hence the f_r form a basis for $Func([a, b], \mathbb{C})$.

It is easy to construct a basis for a Cartesian product of two vector spaces. If $\mathcal{B} = \{V_0, V_1, \ldots, V_{m-1}\}$ is a basis for $\mathbb{V}$ and $\mathcal{B}' = \{V'_0, V'_1, \ldots, V'_{m-1}\}$ is a basis for $\mathbb{V}'$, then $\mathcal{B} \bigcup \mathcal{B}' = \{V_0, V_1, \ldots, V_{m-1}, V'_0, V'_1, \ldots, V'_{m-1}\}$ is a basis of $\mathbb{V} \times \mathbb{V}'$.

Let us look at $\mathbb{R}^3$ carefully. There is the canonical basis:

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}. \tag{2.82}$$

[6] If the reader does not know the difference between "countably" and "uncountably" infinite, fear not. These notions do not play a major role in the tale we are telling. We shall mostly stay within the finite world. Suffice it to state that an infinite set is countable if the set can be put in a one-to-one correspondence with the set of natural numbers $\mathbb{N}$. A set is uncountably infinite if it is infinite and cannot be put into such a correspondence.

There are, however, many other bases of $\mathbb{R}^3$, e.g.,

$$\mathcal{B}_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}, \tag{2.83}$$

$$\mathcal{B}_2 = \left\{ \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ -2 \\ 0 \end{bmatrix} \right\}. \tag{2.84}$$

It is no coincidence that all these bases have the same number of vectors.

Proposition 2.3.1 For every vector space, every basis has the same number of vectors.

Definition 2.3.4 *The* **dimension** *of a (complex) vector space is the number of elements in a basis of the vector space.*

This coincides with the usual use of the word "dimension." Let us run through some of our examples:

- $\mathbb{R}^3$, as a real vector space, is of dimension 3.
- In general, $\mathbb{R}^n$ has dimension n as a real vector space.
- $\mathbb{C}^n$ has dimension n as a complex vector space.
- $\mathbb{C}^n$ is of dimension $2n$ as a real vector space because every complex number is described by two real numbers.
- $Poly_n$ is isomorphic to $\mathbb{C}^{n+1}$; it is not hard to see that the dimension of $Poly_n$ is also $n+1$.
- $\mathbb{C}^{m\times n}$: the dimension is mn as a complex vector space.
- $Func(\mathbb{N}, \mathbb{C})$ has countably infinite dimension.
- $Func([a, b], \mathbb{C})$ has uncountably infinite dimension.
- The dimension of $\mathbb{V} \times \mathbb{V}'$ is the dimension of $\mathbb{V}$ plus the dimension of $\mathbb{V}'$.

The following proposition will make our lives easier:

Proposition 2.3.2 Any two complex vector spaces that have the same dimension are isomorphic. In particular, for each n, there is essentially only one complex vector space that is of dimension n: $\mathbb{C}^n$.

(It is easy to see why this is true. Let $\mathbb{V}$ and $\mathbb{V}'$ be any two vector spaces with the same dimension. Every $V \in \mathbb{V}$ can be written in a unique way as a linear combination of basis vectors in $\mathbb{V}$. Taking those unique coefficients and using them as coefficients for the linear combination of the basis elements of any basis of $\mathbb{V}'$ gives us a nice isomorphism from $\mathbb{V}$ to $\mathbb{V}'$.)

Because we will be concentrating on finite-dimensional vector spaces, we only concern ourselves with $\mathbb{C}^n$.

Sometimes we shall use more than one basis for a single vector space.

Example 2.3.5 Consider the basis

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ -3 \end{bmatrix}, \begin{bmatrix} -2 \\ 4 \end{bmatrix} \right\} \tag{2.85}$$

of $\mathbb{R}^2$. The vector $V = \begin{bmatrix} 7 \\ -17 \end{bmatrix}$ can be written as

$$\begin{bmatrix} 7 \\ -17 \end{bmatrix} = 3 \begin{bmatrix} 1 \\ -3 \end{bmatrix} - 2 \begin{bmatrix} -2 \\ 4 \end{bmatrix}. \tag{2.86}$$

The coefficients for V with respect to the basis $\mathcal{B}$ are 3 and -2. We write this as $V_{\mathcal{B}} = \begin{bmatrix} 3 \\ -2 \end{bmatrix}$. If $\mathcal{C}$ is the canonical basis of $\mathbb{R}^2$, then

$$\begin{bmatrix} 7 \\ -17 \end{bmatrix} = 7 \begin{bmatrix} 1 \\ 0 \end{bmatrix} - 17 \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{2.87}$$

i.e., $V_{\mathcal{C}} = V = \begin{bmatrix} 7 \\ -17 \end{bmatrix}$.

Let us consider another basis of $\mathbb{R}^2$:

$$\mathcal{D} = \left\{ \begin{bmatrix} -7 \\ 9 \end{bmatrix}, \begin{bmatrix} -5 \\ 7 \end{bmatrix} \right\}. \tag{2.88}$$

What are the coefficients of V with respect to $\mathcal{D}$? What is $V_{\mathcal{D}}$? A **change of basis matrix** or a **transition matrix** from basis $\mathcal{B}$ to basis $\mathcal{D}$ is a matrix $M_{\mathcal{D}\leftarrow\mathcal{B}}$ such that for any matrix V, we have

$$V_{\mathcal{D}} = M_{\mathcal{D}\leftarrow\mathcal{B}} \star V_{\mathcal{B}}. \tag{2.89}$$

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

$$M_{\mathcal{D}\leftarrow\mathcal{B}} = \begin{bmatrix} 2 & -\frac{3}{2} \\ -3 & \frac{5}{2} \end{bmatrix}. \tag{2.90}$$

So

$$V_{\mathcal{D}} = M_{\mathcal{D}\leftarrow\mathcal{B}} V_{\mathcal{B}} = \begin{bmatrix} 2 & -\frac{3}{2} \\ -3 & \frac{5}{2} \end{bmatrix} \begin{bmatrix} 3 \\ -2 \end{bmatrix} = \begin{bmatrix} 9 \\ -14 \end{bmatrix}. \tag{2.91}$$

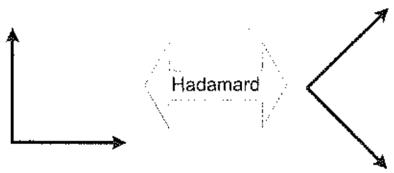

Figure 2.6. The Hadamard matrix as a transition between two bases.

Checking, we see that

$$\begin{bmatrix} 7 \\ -17 \end{bmatrix} = 9 \begin{bmatrix} -7 \\ 9 \end{bmatrix} - 14 \begin{bmatrix} -5 \\ 7 \end{bmatrix}. \tag{2.92}$$

□

Given two bases of a finite-dimensional vector space, there are standard algorithms to find a transition matrix from one to the other. (We will not need to know how to find these matrices.)

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

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \tag{2.93}$$

to this other basis

$$\left\{ \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \right\} \tag{2.94}$$

is the **Hadamard matrix**:

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

Exercise 2.3.3 Show that H times itself gives you the identity matrix. ■

Because H multiplied by itself gives the identity matrix, we observe that the transition back to the canonical basis is also the Hadamard matrix. We might envision these transitions as in Figure 2.6.

It turns out that the Hadamard matrix plays a major role in quantum computing.

In physics, we are often faced with a problem in which it is easier to calculate something in a noncanonical basis. For example, consider a ball rolling down a ramp as depicted in Figure 2.7.

The ball will not be moving in the direction of the canonical basis. Rather it will be rolling downward in the direction of $+45°$, $-45°$ basis. Suppose we wish to calculate when this ball will reach the bottom of the ramp or what is the speed of the ball. To do this, we change the problem from one in the canonical basis to one in the other basis. In this other basis, the motion is easier to deal with. Once we have

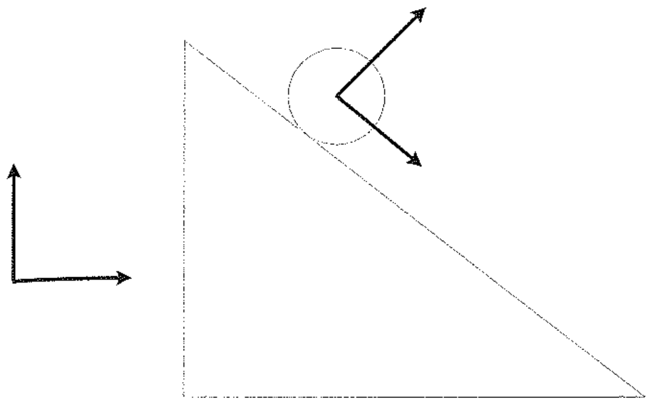

Figure 2.7. A ball rolling down a ramp and the two relevant bases.

completed the calculations, we change our results into the more understandable canonical basis and produce the desired answer. We might envision this as the flowchart shown in Figure 2.8.

Throughout this text, we shall go from one basis to another basis, perform some calculations, and finally revert to the original basis. The Hadamard matrix will frequently be the means by which we change the basis.

2.4 INNER PRODUCTS AND HILBERT SPACES

We will be interested in complex vector spaces with additional structure. Recall that a state of a quantum system corresponds to a vector in a complex vector space. A need will arise to compare different states of the system; hence, there is a need to compare corresponding vectors or measure one vector against another in a vector space.

Consider the following operation that we can perform with two vectors in $\mathbb{R}^3$:

$$\left\langle \begin{bmatrix} 5 \\ 3 \\ -7 \end{bmatrix}, \begin{bmatrix} 6 \\ 2 \\ 0 \end{bmatrix} \right\rangle = [5, 3, -7] \star \begin{bmatrix} 6 \\ 2 \\ 0 \end{bmatrix} = (5 \times 6) + (3 \times 2) + (-7 \times 0) = 36. \tag{2.96}$$

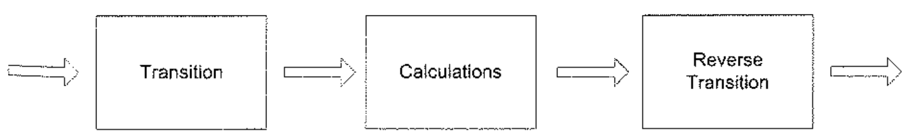

Figure 2.8. Problem-solving flowchart.

In general, for any two vectors $V_1 = [r_0, r_1, r_2]^T$ and $V_2 = [r'_0, r'_1, r'_2]^T$ in $\mathbb{R}^3$, we can form a real number by performing the following operation:

$$\langle V_1, V_2 \rangle = V_1^T \star V_2 = \sum_{j=0}^{2} r_j r'_j. \tag{2.97}$$

This is an example of an inner product of two vectors. An inner product in a complex (real) vector space is a binary operation that accepts two vectors as inputs and outputs a complex (real) number. This operation must satisfy certain properties spelled out in the following:

Definition 2.4.1 *An* **inner product** *(also called a* **dot product** *or* **scalar product***) on a complex vector space* $\mathbb{V}$ *is a function*

$$\langle -, - \rangle : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{C} \tag{2.98}$$

that satisfies the following conditions for all V, V_1, V_2, *and* V_3 *in* $\mathbb{V}$ *and for a* $c \in \mathbb{C}$:

(i) *Nondegenerate:*

$$\langle V, V \rangle \geq 0, \tag{2.99}$$

$$\langle V, V \rangle = 0 \text{ if and only if } V = \mathbf{0} \tag{2.100}$$

(i.e., the only time it "degenerates" is when it is 0).

(ii) *Respects addition:*

$$\langle V_1 + V_2, V_3 \rangle = \langle V_1, V_3 \rangle + \langle V_2, V_3 \rangle, \tag{2.101}$$

$$\langle V_1, V_2 + V_3 \rangle = \langle V_1, V_2 \rangle + \langle V_1, V_3 \rangle. \tag{2.102}$$

(iii) *Respects scalar multiplication:*

$$\langle c \cdot V_1, V_2 \rangle = c \times \langle V_1, V_2 \rangle, \tag{2.103}$$

$$\langle V_1, c \cdot V_2 \rangle = \overline{c} \times \langle V_1, V_2 \rangle. \tag{2.104}$$

(iv) *Skew symmetric:*

$$\langle V_1, V_2 \rangle = \overline{\langle V_2, V_1 \rangle}. \tag{2.105}$$

An inner product on real vector space $\langle\ ,\ \rangle : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{R}$ must satisfy the same properties. Because any $r \in \mathbb{R}$ satisfies $\overline{r} = r$, Properties (iii) and (iv) are simpler for a real vector space.

Definition 2.4.2 *A* **(complex) inner product space** *is a (complex) vector space along with an inner product.*

Let us list some examples of inner product spaces.

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

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

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

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

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

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

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

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

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

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

- $Func(\mathbb{N}, \mathbb{C})$:

$$\langle f, g \rangle = \sum_{j=0}^{\infty} \overline{f(j)} g(j). \tag{2.111}$$

- $Func([a,b], \mathbb{C})$:

$$\langle f, g \rangle = \int_a^b \overline{f(t)} g(t)\, dt. \tag{2.112}$$

Exercise 2.4.1 Let $V_1 = [2,1,3]^T$, $V_2 = [6,2,4]^T$, and $V_3 = [0,-1,2]^T$. Show that the inner product in $\mathbb{R}^3$ respects the addition, i.e., Equations (2.101) and (2.102). ■

Exercise 2.4.2 Show that the function $\langle\ ,\ \rangle : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ given in Equation (2.106) satisfies all the properties of being an inner product on $\mathbb{R}^n$. ■

Exercise 2.4.3 Let $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$, and $C = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}$. Show that the inner product in $\mathbb{R}^{2\times 2}$ respects addition (Equations (2.101) and (2.102)) with these matrices. ■

Exercise 2.4.4 Show that the function given for pairs of real matrices satisfies the inner product properties and converts the real vector space $\mathbb{R}^{n\times n}$ to a real inner product space. ■

Programming Drill 2.4.1 *Write a function that accepts two complex vectors of length n and calculates their inner product.*

The inner product of a complex vector with itself is a real number. We can observe this from the property that for all V_1, V_2, an inner product must satisfy

$$\langle V_1, V_2 \rangle = \overline{\langle V_2, V_1 \rangle}. \tag{2.113}$$

It follows that if $V_2 = V_1$, then we have

$$\langle V_1, V_1\rangle = \overline{\langle V_1, V_1\rangle}; \tag{2.114}$$

hence it is real.

Definition 2.4.3 *For every complex inner product space* $\mathbb{V}, \langle -, -\rangle$, *we can define a* **norm** *or* **length** *which is a function*

$$|\ \ |: \mathbb{V} \longrightarrow \mathbb{R} \tag{2.115}$$

defined as $|V| = \sqrt{\langle V, V\rangle}$.

Example 2.4.1 In $\mathbb{R}^3$, the norm of vector $[3, -6, 2]^T$ is

$$\left|\begin{bmatrix} 3 \\ -6 \\ 2 \end{bmatrix}\right| = \sqrt{\left\langle \begin{bmatrix} 3 \\ -6 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ -6 \\ 2 \end{bmatrix} \right\rangle} = \sqrt{3^2 + (-6)^2 + 2^2} = \sqrt{49} = 7. \tag{2.116}$$

□

Exercise 2.4.5 Calculate the norm of $[4 + 3i, 6 - 4i, 12 - 7i, 13i]^T$. ■

Exercise 2.4.6 Let $A = \begin{bmatrix} 3 & 5 \\ 2 & 3 \end{bmatrix} \in \mathbb{R}^{2\times 2}$. Calculate the norm $|A| = \sqrt{\langle A, A\rangle}$. ■

In general, the norm of the vector $[x, y, z]^T$ is

$$\left|\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right| = \sqrt{\left\langle \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \begin{bmatrix} x \\ y \\ z \end{bmatrix} \right\rangle} = \sqrt{x^2 + y^2 + z^2}. \tag{2.117}$$

This is the Pythagorean formula for the length of a vector. The intuition one should have is that the norm of a vector in any vector space is the length of the vector.

From the properties of an inner product space, it follows that a norm has the following properties for all $V, W \in \mathbb{V}$ and $c \in \mathbb{C}$:

(i) Norm is nondegenerate: $|V| > 0$ if $V \neq \mathbf{0}$ and $|\mathbf{0}| = 0$.
(ii) Norm satisfies the **triangle inequality**: $|V + W| \leq |V| + |W|$.
(iii) Norm respects scalar multiplication: $|c \cdot V| = |c| \times |V|$.

Programming Drill 2.4.2 *Write a function that calculates the norm of a given complex vector.*

Given a norm, we can proceed and define a distance function.

Definition 2.4.4 *For every complex inner product space* $(\mathbb{V}, \langle\ ,\ \rangle)$, *we can define a* **distance function**

$$d(\ ,\ ) : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{R}, \tag{2.118}$$

where

$$d(V_1, V_2) = |V_1 - V_2| = \sqrt{\langle V_1 - V_2, V_1 - V_2\rangle}. \tag{2.119}$$

Exercise 2.4.7 Let $V_1 = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}$ and $V_2 = \begin{bmatrix} 2 \\ 2 \\ -1 \end{bmatrix}$. Calculate the distance between these two vectors. ∎

The intuition is that $d(V_1, V_2)$ is the distance from the end of vector V_1 to the end of vector V_2. From the properties of an inner product space, it is not hard to show that a distance function has the following properties for all $U, V, W \in \mathbb{V}$:

(i) Distance is nondegenerate: $d(V, W) > 0$ if $V \neq W$ and $d(V, V) = 0$.
(ii) Distance satisfies the **triangle inequality**: $d(U, V) \leq d(U, W) + d(W, V)$.
(iii) Distance is symmetric: $d(V, W) = d(W, V)$.

Programming Drill 2.4.3 *Write a function that calculates the distance of two given complex vectors.*

Definition 2.4.5 *Two vectors* V_1 *and* V_2 *in an inner product space* $\mathbb{V}$ *are* **orthogonal** *if* $\langle V_1, V_2\rangle = 0$.

The picture to keep in mind is that two vectors are orthogonal if they are perpendicular to each other.

Definition 2.4.6 *A basis* $\mathcal{B} = \{V_0, V_1, \ldots, V_{n-1}\}$ *for an inner product space* $\mathbb{V}$ *is called an* **orthogonal basis** *if the vectors are pairwise orthogonal to each other, i.e.,* $j \neq k$ *implies* $\langle V_j, V_k\rangle = 0$. *An orthogonal basis is called an* **orthonormal basis** *if every vector in the basis is of norm 1, i.e.,*

$$\langle V_j, V_k\rangle = \delta_{j,k} = \begin{cases} 1, & \text{if } j = k, \\ 0, & \text{if } j \neq k. \end{cases} \tag{2.120}$$

$\delta_{j,k}$ *is called the* **Kronecker delta function**.

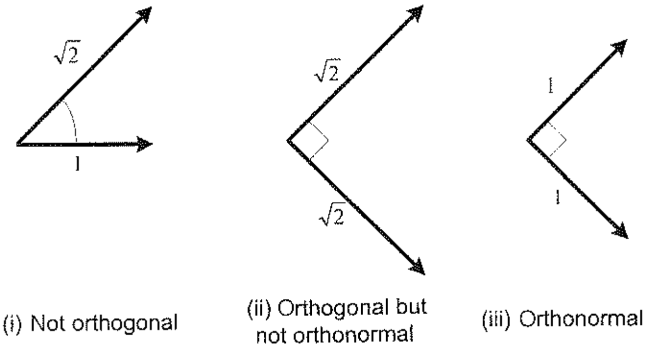

Figure 2.9. Three bases for $\mathbb{R}^2$.

Example 2.4.2 Consider the three bases for $\mathbb{R}^2$ shown in Figure 2.9. Formally, these bases are

$$\text{(i)} \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

$$\text{(ii)} \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix},$$

$$\text{(iii)} \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

□

In $\mathbb{R}^3$, the standard inner product $\langle V, V' \rangle = V^T V'$ can be shown to be equivalent to

$$\langle V, V' \rangle = |V||V'| \cos\theta, \tag{2.121}$$

where θ is the angle between V and V'. When $|V'| = 1$, this equation reduces to

$$\langle V, V' \rangle = |V| \cos\theta. \tag{2.122}$$

Exercise 2.4.8 Let $V = [3, -1, 0]^T$ and $V' = [2, -2, 1]^T$. Calculate the angle θ between these two vectors. ■

Elementary trigonometry teaches us that when $|V'| = 1$, the number $\langle V, V' \rangle$ is the length of the projection of V onto the direction of V' (Figure 2.10).

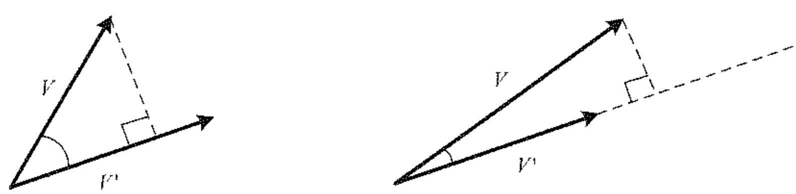

Figure 2.10. The projection of V onto V'.

$\langle V, V' \rangle \cdot V'$ is the vector V' extended (or reduced) to meet the projection of V onto V'.

What does this mean in terms of $\mathbb{R}^3$? Let $V = [r_0, r_1, r_2]^T$ be any vector in $\mathbb{R}^3$. Let E_0, E_1, and E_2 be the canonical basis of $\mathbb{R}^3$. Then

$$V = \begin{bmatrix} r_0 \\ r_1 \\ r_2 \end{bmatrix} = \langle E_0, V \rangle \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \langle E_1, V \rangle \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \langle E_2, V \rangle \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}. \tag{2.123}$$

In general, for any $V \in \mathbb{R}^n$,

$$V = \sum_{j=0}^{n-1} \langle E_j, V \rangle E_j. \tag{2.124}$$

We shall use the intuition afforded by $\mathbb{R}^3$ and $\mathbb{R}^n$ to understand this type of decomposition of vectors into sums of canonical vectors for other vector spaces.

Proposition 2.4.1 In $\mathbb{C}^n$, we also have that any V can be written as

$$V = \langle E_0, V \rangle E_0 + \langle E_1, V \rangle E_1 + \cdots + \langle E_{n-1}, V \rangle E_{n-1}. \tag{2.125}$$

It must be stressed that this is true for any orthonormal basis, not just the canonical one.

In $Func(\mathbb{N}, \mathbb{C})$ for an arbitrary function $g : \mathbb{N} \longrightarrow \mathbb{C}$ and for a canonical basis function $f_j : \mathbb{N} \longrightarrow \mathbb{C}$, we have

$$\langle f_j, g \rangle = \sum_{k=0}^{\infty} \overline{f_j(k)} g(k) = 1 \times g(j) = g(j). \tag{2.126}$$

And so any $g : \mathbb{N} \longrightarrow \mathbb{C}$ can be written as

$$g = \sum_{k=0}^{\infty} (\langle f_k, g \rangle f_k). \tag{2.127}$$

Reader Tip. The following definitions will not be essential for us, but we include them so that the reader will be able to understand other texts. In our text, there is no reason to worry about them because we are restricting ourselves to finite-dimensional inner product spaces and they automatically satisfy these properties. ♡

Definition 2.4.7 *Within an inner product space* $\mathbb{V}$, $\langle\ ,\ \rangle$ *(with the derived norm and a distance function), a sequence of vectors* $V_0, V_1, V_2, \ldots$ *is called a* **Cauchy sequence** *if for every* $\epsilon > 0$*, there exists an* $N_0 \in \mathbb{N}$ *such that*

$$\text{for all } m, n \geq N_0, \quad d(V_m, V_n) \leq \epsilon. \tag{2.128}$$

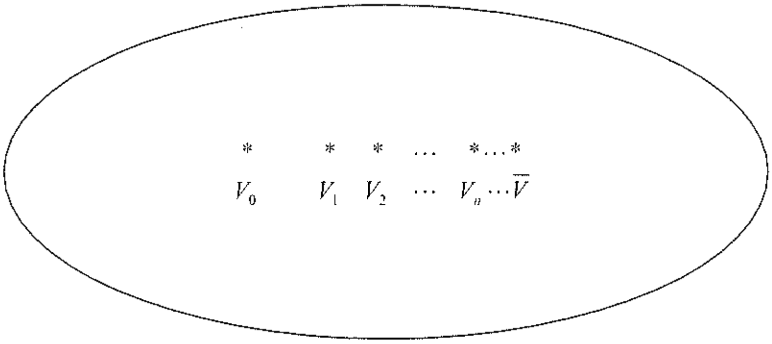

Figure 2.11. Completeness for a complex inner product space.

Definition 2.4.8 *A complex inner product space is called* **complete** *if for any Cauchy sequence of vectors $V_0, V_1, V_2, \ldots$, there exists a vector $\bar{V} \in \mathbb{V}$ such that*

$$\lim_{n\to\infty} |V_n - \bar{V}| = 0. \tag{2.129}$$

The intuition behind this is that a vector space with an inner product is complete if any sequence accumulating somewhere converges to a point (Figure 2.11).

Definition 2.4.9 *A* **Hilbert space** *is a complex inner product space that is complete.*

If completeness seems like an overly complicated notion, fear not. We do not have to worry about completeness because of the following proposition (which we shall not prove).

Proposition 2.4.2 Every inner product on a *finite*-dimensional complex vector space is automatically complete; hence, every finite-dimensional complex vector space with an inner product is automatically a Hilbert space.

Quantum computing in our text will only deal with finite-dimensional vector spaces and so we do not have to concern ourselves with the notion of completeness. However, in the culture of quantum mechanics and quantum computing, you will encounter the words "Hilbert space," which should no longer cause any anxiety.

2.5 EIGENVALUES AND EIGENVECTORS

Example 2.5.1 Consider the simple 2-by-2 real matrix

$$\begin{bmatrix} 4 & -1 \\ 2 & 1 \end{bmatrix}. \tag{2.130}$$

Notice that

$$\begin{bmatrix} 4 & -1 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix} = 3\begin{bmatrix} 1 \\ 1 \end{bmatrix}. \tag{2.131}$$