# Linear algebra and quantum probability

William Slofstra

January 4, 2022 (version 0.8)

# Preface

This book originated as course notes for PMATH 343 “Mathematics of quantum information”, a 3rd year undergraduate pure math course at the University of Waterloo. I’m making it available online for anyone else who finds it useful. There’s a longer introduction covering what this book is about, but the brief version: this is an undergraduate textbook, covering advanced linear algebra (along with some basic matrix analysis) and quantum probability (the mathematical framework underlying quantum mechanics) for readers who want to learn quantum information and quantum computation. The book is from the “pure math” point of view: concepts are investigated using theorems and proofs, and we try to do linear algebra in a basis independent manner.

Hopefully it’s clear from this description that this is not a book on quantum mechanics. Quantum probability *is* the mathematical framework for quantum mechanics, but this book is about the mathematical aspects of this framework, not about how the framework is actually used. Also, aside from a few very basic things, this book doesn’t cover much about information or computation. If you’re primarily interested in quantum computing, you don’t need to start with this book; there are a number of good undergraduate textbooks where you can just jump in with only an introductory linear algebra course. In fact, most people working in the field just use the basis dependent approach to linear algebra. So it makes perfect sense to start elsewhere, and come back to this book if you find yourself asking mathematical questions like “why is the Kronecker product defined the way it is?” On the other hand, readers who know from the outset that they’d like to learn quantum computing *and* all the math behind it (this seems to describe most of the students who enroll in the class at Waterloo) can start here: after this book, you’ll be fluent in the mathematical language used in quantum computing, and ready to read other books or take other courses.

Most of the linear algebra concepts discussed in this book are widely used outside of quantum information as well. For readers primarily interested in other applications, quantum probability is a great way to be introduced to these concepts. One of the challenges in learning advanced linear algebra and matrix analysis is that many treatments of these subjects don't provide much in the way of motivation or context. A typical example is simultaneous diagonalization of commuting matrices. It's difficult to appreciate this important result on its own, but it's easy to see the significance when it's stated in terms of jointly measurable observables. Quantum probability provides a natural context for this and many other concepts.

A final note: there are several topics (e.g. quantum channels, the 1-norm on matrices) which fit well with the theme of the book, but which haven't been added yet. In that sense, the book is still incomplete. For getting the book to the current point, I need to thank the students and TAs (Adina Goldberg, Ehsaan Hossain, and Yuming Zhao) of the first several iterations of the course, along with David Gosset and Yangchen Zhou, for many suggestions and corrections.

# Contents

# Chapter 1

# Introduction

The basic story of quantum mechanics is that physics at very small scales looks very different from physics at human scales, and we have to dramatically change how we model physical scenarios at this scale.

From a mathematical point of view, quantum mechanics is a toolkit (a set of mathematical axioms) that provides a way to understand and model this type of physics. This toolkit is sometimes called *quantum probability* or *noncommutative probability*.

## 1.1 Probabilistic reasoning in physics

Recall that, for the basic axioms of probability, we start with a *sample space* $\Omega$. This is the space of *outcomes*, or *things that can happen* in a given situation. An *event* is a subset of $\Omega$, and a *probability distribution* is a function $p$ from the set of events to the interval $[0,1]$, satisfying certain axioms. When $\Omega$ is finite, a probability distribution is just a function $p : \Omega \to [0,1]$ such that

$$\sum_{x \in \Omega} p(x) = 1.$$

We say that $p(x)$ is *the probability of outcome $x$*.

There are two ways to think about what $p$ means:

- Frequentist interpretation: $\Omega =$ outcomes of some experiment that can be repreated many times, and

$$p(x) = \lim_{N \to +\infty} \frac{\text{number of times } x \text{ occurs in } N \text{ repetitions of the experiment}}{N}.$$

- Bayesian interpretation: $p(x)$ quantifies our best guess about how likely $x$ is to occur. In this interpretation, $p$ reflects our knowledge or information about the system.

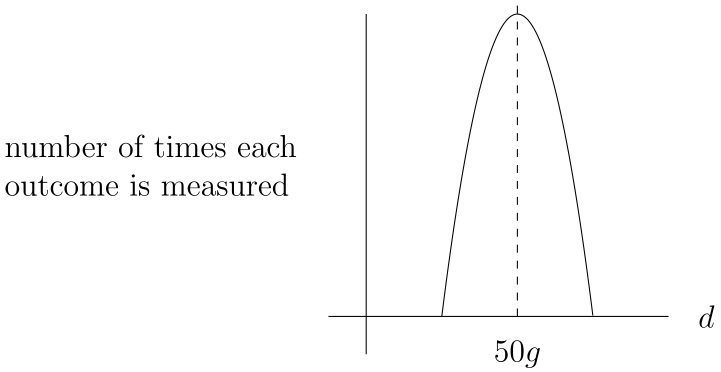
We commonly use probabilities when describing physical systems, and we have only limited knowledge about the system. For instance, in trying to describe the weather, we might say that the probability of snow tomorrow is 80%. (Here we are using the Bayesian interpretation of probability.)

At other times, it seems like we don't use probability when describing "classical" physics.

**Example 1.1.1.** *Question: How far does an object dropped straight down from a building fall in $t$ seconds?*

*Answer: $d = gt^2/2$ metres, where $g$ is the gravitational constant.*

In this example, we don't seem to need probability to describe the physical system. However, suppose we actually do an experiment where we drop an object and measure $d$ after $t = 10$ seconds. According to our model, the object should fall $50g$ metres. But when we do the experiment, it's unlikely that we'll get $50g$ exactly. Instead, if we repeat the experiment repeatedly, we'll get measurement outcomes clustered around $50g$:



Based on this picture, it seems like the formula $d = gt^2/2$ doesn't hold, and we should probably think of $d$ as a random variable. (A *random variable* is another standard concept from propbability theory. For a finite sample space $\Omega$, a random variable is just a function $f : \Omega \to \mathbb{R}$.) So why don't we include probability theory in the description of the physical system in our example? The reason is that we can typically resolve this situation by looking for hidden information or uncertainty in our physical picture. For instance, maybe the problem is that we are not measuring the distance $d$ at exactly $t = 10$ seconds;

each time we measure, we are actually measuring at some time $t$ randomly distributed around 10. If we think of $t$ as a random variable, then the formula $d = gt^2/2$ holds again, and the distribution of $t$ explains the distribution of $d$.

Of course, this isn't the only way that noise could enter our experiment. But in "classical" physical thinking, we can often explain this noise by looking for hidden information. So for instance, we might have to consider air resistance and currents in our formula, but if we just knew the location of every air molecule, we could calculate the distance travelled exactly. For this reason, we can often leave probability theory out when describing classical physical systems.

## 1.2 A measurement scenario

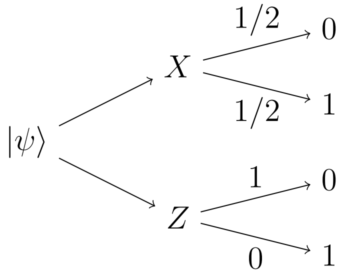
In quantum physics, there are phenomena which are intrinsically probabilistic. However, there is nothing in quantum physics which we can't describe with classical probability, if we use it correctly. So quantum probability is not a replacement for classical probability, but rather an add-on that helps us reason about and more efficiently describe certain situations.

To see why quantum probability might be helpful, consider a measurement scenario. Measurement is something that we will discuss a lot in this course. It can refer to any process where we uncover some information about a system, whether it's by making some complicated experiment in a lab, or revealing the result of a coinflip. In the measurement scenario we want to consider, suppose we have a physical system on which we can make one of two measurements, $X$ or $Z$. Each measurement results in one of two outcomes, 0 or 1. Suppose we always prepare this system according to a fixed procedure, leaving it in some state, which we will denote by $|\psi\rangle$.[1] When in state $|\psi\rangle$, we measure the system and discover that if we make measurement $Z$, we always get outcome 0, while if we make measurement $X$, we get 0 and 1 with equal probability.

How should we describe the state $|\psi\rangle$ of the system? We might think that $|\psi\rangle$ has two different properties, $X$ and $Z$. Since $Z$ is always 0, we can just say that the property $Z$ is equal to 0 after preparation. Since we can get either 0 or 1 from $X$, we can describe property $X$ as the uniform probability distribution on the set $\{0, 1\}$. This is shown in Figure 1.1.

Is this a good description? To check, we might try to measure both $X$ and $Z$. In this case, if we measure $Z$ first, then we find that our description is appropriate: we get 0 when we measure $Z$, and either 0 or 1 when we measure $X$, with probability $1/2$ each. This is shown on the left in Figure 1.2

[1] We'll explain this weird notation later.



$$\begin{array}{c}\underline{|\psi\rangle}\\[1em] Z=0\\[1em] X=\begin{pmatrix}1/2\\1/2\end{pmatrix}\begin{array}{c}0\\1\end{array}\end{array}$$

Figure 1.1: A naive description of $|\psi\rangle$

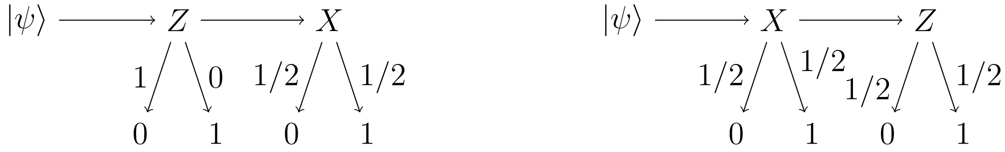


Figure 1.2: Measuring both $X$ and $Z$

However, to be careful, we also try measuring $X$ before $Z$. When we do this, we find that measuring $X$ has affected $Z$, and we now get $Z = 0$ and $Z = 1$ with equal probability as well.

The measurement scenario that we've described is a simplified version of what happens in a repeated Stern-Gerlach experiment, where we measure angular momentum along the $X$ and $Z$ axes. What we see is that $X$ and $Z$ satisfy an uncertainty principle: if we try to get information about $X$ by measuring it, we lose information about $Z$ (in short, if we're certain about $X$, we're uncertain about $Z$). Note that since measuring $X$ affects our knowledge about $Z$, to describe this process we must use probability theory.

Can we describe the physical system $|\psi\rangle$ (after preparation, but before any measurement) with classical probability theory? Certainly. We can define two joint probability distributions

$$p_{XZ} = \begin{array}{c}\\ \begin{pmatrix}1/4\\1/4\\1/4\\1/4\end{pmatrix}\end{array}\begin{array}{c}\underline{XZ}\\00\\01\\10\\11\end{array} \quad\text{and}\quad p_{ZX} = \begin{array}{c}\\ \begin{pmatrix}1/2\\1/2\\0\\0\end{pmatrix}\end{array}\begin{array}{c}\underline{ZX}\\00\\01\\10\\11\end{array},$$

one for when we measure $X$ first, and one for when we measure $Z$ first, and say that these two distributions together define the state $|\psi\rangle$.

While this works, it is both inconvenient and counterintuitive. First, we need a probability distribution for both orders of measurement. The problem gets even worse if we add a third measurement (we'd need at least 6 probability distributions) or allow repetitions of measurements (we'd need a probability distribution for every string like $XZXXZX\ldots$). Also, it's counterintuitive to have to describe the state of the system by referring to the order of measurements, before any measurement has been made. Who says we have to make a measurement at all?

Recall that a binary operation is commutative if $ab = ba$ for all $a, b$. Multiplication of numbers is commutative, while multiplication of matrices is not. The key problem in this measurement scenario is that measuring $X$ affects $Z$, so the two measurement processes do not *commute*. For this reason, we'd like to have a noncommutative probability theory, and this is what quantum probability provides. A quantum system meeting the above description could be described by a unit vector

$$\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \in \mathbb{C}^2.$$

In this description, the measurement operators would be described by matrices

$$X = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } Z = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

Note that $XZ \neq ZX$. In quantum probability, we think of matrices like this as random variables. When they do not commute, they satisfy an uncertainty principle (this is one of the things we will prove in this course).

To avoid being misleading, we should note that we don't have to look at a Stern-Gerlach experiment or other scenarios in quantum physics to find physical situations where measuring one quantity might affect another quantity. Quantum probability isn't a toolkit for modelling all such situations; it's a toolkit that's proven very effective for modelling quantum physics specifically. Still, thinking of quantum probability as noncommutative probability is a good starting point.

## 1.3 Quantum information

Computers have given us a very hands-on view of information, as something that can be stored or manipulated by a computing device. The collection of fields that study information in this sense is sometimes called *information science*, although there are other popular terms such as *informatics*. Computer science (which itself is split into many fields, such as algorithms, data structures, etc.), cryptography, and many other fields all fall under the umbrella of information science.

The subfield of information science which is most focused on information is *information theory*, which is the quantitative study of information. In this field, information is what is gained when we measure some random variable, or otherwise learn the outcome of some random process. To get a taste for how this works, suppose we flip a coin and find out that it's heads. How much information have we gained? If the coin usually gives heads with probability $p(H) = 5/6$, then we've gained less information than if the coin usually gives heads with probability $p(H) = 1/2$. It turns out that it works well to quantify the amount of information gained when we learn outcome $x$ as $-\log_2 p(x)$, where $p(x)$ is the probability of outcome $x$. The *information* (or *Shannon entropy*) of a probability distribution $p$ is the expected information gained. For our coin flip, the amount of information is $I = -p(H)\log_2 p(H) - p(T)\log_2 p(T)$. When $p(H) = 1/2$, we get $I = 1$, while if $p(H) = 5/6$ we get $I \approx 0.263 < 1$. Information is measured in bits, so we would say that a fair coin (one with $p(H) = 1/2$) contains 1 bit of information.

One of the major insights of the last few decades is that the point of view of information science, in the broad sense, is very useful in understanding quantum mechanics. This connection goes the other way as well, in that the laws of quantum mechanics seem to have profound implications for information science. In particular, it seems like it might be possible to build quantum computers, which might be more powerful than classical computers. Large-scale efforts to build such a computer are now underway, although it remains to be seen whether they will be fully successful.

The field which combines information science and quantum mechanics is called *quantum information science*. Like information science, it contains many areas, including quantum algorithms, quantum cryptography, and quantum information theory. This course is about the mathematics used in quantum information, and specifically quantum probability and the core concepts of quantum information such as qubits, measurements, and quantum circuits. We won't have time to look at any of the applications of quantum information, such as algorithms or cryptography, but this course should leave you ready to take another course on these subjects, or read about them on your own.

## 1.4 Axioms and prerequisites

As mentioned above, quantum probability is a set of axioms that describe how to model physical scenarios. The axioms for a theory are the statements that we accept as true without proof. Giving a complete axiomatization of quantum mechanics is beyond the scope of this course. However, as a way of understanding what we accept as given, and what we need to prove, we will introduce some of the key axioms needed for quantum information. They are:

1. A physical system corresponds to a Hilbert space.

2. The state of a physical system corresponding to Hilbert space $H$ is given by a unit vector $v \in H$.

3. For every orthonormal basis in a Hilbert space, there is an associated measurement.

4. Time evolution is linear.

5. For every complete family of orthogonal projections, there is an associated measurement.

6. Let $H_1$ and $H_2$ be the Hilbert spaces of two physical systems. Then the Hilbert space of the joint system is the tensor product $H_1 \otimes H_2$.

The main goal of this course will be to explain what these axioms mean, and derive some of the important consequences of these axioms. Note that all of these axioms involve linear algebra. And indeed, linear algebra is central to quantum mechanics, to the point that this course could be considered a course in advanced linear algebra. We do assume knowledge of basic linear algebra in this course, although we review some of the key concepts in the next two chapters. In addition, it will be helpful to know some basic analysis, such as continuous functions, open and closed sets, and limits in normed vector spaces.

# Chapter 2

# Linear algebra

Since quantum probability is based on linear algebra, in this section we review some of the basic concepts. While most of the concepts should be familiar, we discuss some of the nuances that might not come up in a beginning linear algebra course. We also introduce two concepts, free vector spaces and dual spaces, which are sometimes omitted from such courses.

## 2.1 The basics

### 2.1.1 Vector spaces

Recall that we can do linear algebra over any field $\mathbb{F}$. In this course, we will assume that $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ so that operations like conjugation and absolute values are available. If $x \in \mathbb{C}$, then $\overline{x}$ will denote the complex conjugate, while if $x \in \mathbb{R}$, then we set $\overline{x} := x$. The main object of study in linear algebra are vector spaces:

**Definition 2.1.1.** *An $\mathbb{F}$-vector space is a tuple $(V, +, \cdot, 0)$, where $V$ is a set, $+ : V \times V \to V$, $\cdot : \mathbb{F} \times V \to V$, and $0 \in V$, such that for all $u, v, w \in V$, $r, s \in \mathbb{F}$,*

*(1)* $u + v = v + u$,

*(2)* $u + (v + w) = (u + v) + w$,

*(3)* $v + 0 = v$,

*(4) there is a unique element $-v \in V$ such that $v + (-v) = 0$,*

*(5)* $r \cdot (s \cdot v) = (rs) \cdot v$,

*(6)* $(r + s) \cdot v = r \cdot v + s \cdot v$,

*(7)* $r \cdot (u + v) = r \cdot u + r \cdot v$, *and*

*(8)* $1 \cdot u = u$.

**Example 2.1.2.** *Examples of vector spaces include:*

- *The space of column vectors* $\mathbb{F}^n$, $n \geq 0$.
- $M_{mn}\mathbb{F}$, *the space of* $m \times n$ *matrices over* $\mathbb{F}$, *with matrix addition and scalar multiplication.*
- *The set of functions* $\mathrm{Fun}(X, V)$ *from* $X$ *to* $V$, *where* $X$ *is a set and* $V$ *is an* $\mathbb{F}$*-vector space. For this vector space, if* $f, g \in \mathrm{Fun}(X, V)$ *and* $c \in \mathbb{F}$, *then* $cf + g$ *is the function with* $(cf + g)(x) = cf(x) + g(x)$ *for all* $x \in X$.

**Definition 2.1.3.** *A* ***basis*** $\mathcal{B}$ *of an* $\mathbb{F}$*-vector space is a subset which is both linearly independent and spanning. The* ***dimension*** $\dim V$ *of a vector space* $V$ *is the size of any basis.*

Every vector space has a basis, and all bases have the same size, so the dimension is well-defined. Bases can be infinite, in which case we say that $V$ is infinite-dimensional. In this course we'll occasionally work with infinite-dimensional vector spaces, but our focus will be on finite-dimensional spaces, and it will be safe to assume that all vector spaces are finite-dimensional unless otherwise noted.

**Example 2.1.4.** *The* ***standard basis*** *of* $\mathbb{F}^n$ *is the set* $\{e_1, \ldots, e_n\}$, *where* $e_i$ *is the vector with a* $1$ *in position* $i$, *and zeroes elsewhere. Hence* $\mathbb{F}^n$ *is* $n$*-dimensional.*

One of the nice things about the standard basis is that we have an order on the vectors in the basis: $e_1$ comes first, then $e_2$, and so on. So the standard basis is an example of an ordered basis:

**Definition 2.1.5.** *An* ***ordered basis*** *for a vector space* $V$ *is a sequence* $v_1, \ldots, v_n$ *such that the set* $\{v_1, \ldots, v_n\}$ *is a basis for* $V$.

The point of this definition is that, with sets, we don't keep track of order, so $\{v_1, v_2\}$ and $\{v_2, v_1\}$ would be the same set, whereas $v_1, v_2$ and $v_2, v_1$ would be different sequences if $v_1 \neq v_2$. Sometimes it's necessary to work with ordered bases rather than unordered bases, such as in the following definition:

**Definition 2.1.6.** *If $\mathcal{B} = \{w_1, \ldots, w_n\}$ is an ordered basis for $V$, where $\dim V = n$, then the **coordinate vector** $[v]_B$ of $v \in V$ is a vector $a \in \mathbb{F}^n$ such that $v = \sum_{i=1}^n a_i w_i$.*

Note that we still use set notation for ordered bases. Typically we won't draw a hard line between ordered and unordered bases, but rather just say "basis" for both, and leave it up to context as to which type of basis we mean.

**Example 2.1.7.** *If $\mathcal{B}$ is the standard basis of $\mathbb{F}^n$, then $[v]_{\mathcal{B}} = v$.*

**Example 2.1.8.** *If $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a basis for $V$, then $[v_i]_{\mathcal{B}} = e_i$, the $i$th standard basis vector for $\mathbb{F}^n$.*

We should mention one more basis that we'll use frequently:

**Example 2.1.9.** *Let $\mathbb{F}$ be a field, and suppose $m, n \geq 1$. For all $1 \leq i \leq m$ and $1 \leq j \leq n$, define $E_{ij}$ to be the element of $M_{mn}\mathbb{F}$ with a $1$ in the $ij$th position, and zeroes elsewhere. Then the set*

$$\{E_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$$

*is a basis for $M_{mn}\mathbb{F}$. Hence $M_{mn}\mathbb{F}$ is $mn$-dimensional.*

We have one more concept to recall concerning vector spaces:

**Definition 2.1.10.** *A **subspace** of a vector space $V$ is a non-empty subset $W$ of $V$ such that for all $s \in \mathbb{F}$ and $u, w \in W$, $su + w \in W$.*

Subspaces are vector spaces in their own right, and showing that a set is a subspace of a known vector space is often the easiest way to show that the set is a vector space.

### 2.1.2 Linear transformations

Vector spaces aren't the only object of study in linear algebra. We also look at linear transformations, which are functions between vector spaces which preserve the linear structure:

**Definition 2.1.11.** *An $\mathbb{F}$**-linear transformation** (also called an $\mathbb{F}$**-linear operator** or $\mathbb{F}$**-linear map**) between two $\mathbb{F}$-vector spaces $V$,$W$ is a function $T : V \to W$ such that*

$$T(sv + w) = sT(v) + T(w)$$

*for all $s \in \mathbb{F}$, $v, w \in V$.*

Let $V$ and $W$ be vector spaces. Two common examples of linear transformations are the zero map

$$0 : V \to W : v \mapsto 0_W,$$

and the identity map

$$\mathbb{1}_V : V \to V : v \mapsto v.$$

Another way to get linear transformations is from matrices. If $A \in M_{mn}\mathbb{F}$, then the function

$$\mathbb{F}^n \to \mathbb{F}^m : v \mapsto Av$$

is linear. It is a standard fact of linear algebra that if $T : \mathbb{F}^n \to \mathbb{F}^m$ is a linear transformation, then there is a unique matrix $A \in M_{mn}\mathbb{F}$ such that $T(v) = Av$ for all $v \in \mathbb{F}^n$. The matrix $A$ is called **the matrix of** $T$. More generally:

**Definition 2.1.12.** *Suppose $V$ and $W$ are vector spaces with bases $\mathcal{B}$ and $\mathcal{R}$ respectively. If $\dim V = n$ and $\dim W = m$, then the* ***coordinate matrix*** *$[T]_{\mathcal{R},\mathcal{B}}$ of a linear transformation $T : V \to W$ is the unique $m \times n$ matrix such that*

$$[T]_{\mathcal{R},\mathcal{B}}[v]_{\mathcal{B}} = [T(v)]_{\mathcal{R}}$$

*for all $v \in V$.*

**Example 2.1.13.** *Let $\mathcal{B}$ be the standard basis of $\mathbb{F}^n$, and $\mathcal{R}$ be the standard basis of $\mathbb{F}^m$. Then*

$$[T]_{\mathcal{R},\mathcal{B}}v = [T]_{\mathcal{R},\mathcal{B}}[v]_{\mathcal{B}} = [T(v)]_{\mathcal{R}} = T(v)$$

*for all $v \in \mathbb{F}^n$, so $[T]_{\mathcal{R},\mathcal{B}}$ is the matrix of $T$.*

**Example 2.1.14.** *If $\mathcal{B}, \mathcal{R}$ are bases of $V$, then the matrix $[\mathbb{1}]_{\mathcal{R},\mathcal{B}}$ is called the* ***change of basis matrix*** *from $\mathcal{B}$ to $\mathcal{R}$, since*

$$[\mathbb{1}]_{\mathcal{R},\mathcal{B}}[v]_{\mathcal{B}} = [\mathbb{1}(v)]_{\mathcal{R}} = [v]_{\mathcal{R}}.$$

Suppose we want to specify a linear transformation $T : V \to W$. If $V = \mathbb{F}^n$ and $W = \mathbb{F}^m$, then we can define $T$ by writing down its matrix (and as we'll see below, this works for arbitrary vector spaces as well after we pick a basis). However, there is another way to specify linear transformations that's very useful: we just pick a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ for $V$, and vectors $w_1, \ldots, w_n \in W$ that we want the vectors $v_i$ to map to. This is enough to specify $T$:

**Lemma 2.1.15.** *There is a unique linear transformation $T : V \to W$ such that $T(v_i) = w_i$ for all $1 \leq i \leq n$.*

Although we're skipping most of the proofs in this section, since everything should be review, we'll make an exception for this lemma.

*Proof.* Define $T$ by the formula $T(v) = \sum_i a_i w_i$, where $a = [v]_{\mathcal{B}}$. If $a = [v]_{\mathcal{B}}$, and $b = [w]_{\mathcal{B}}$, and $s \in \mathbb{F}$, then

$$\sum_i (sa_i + b_i)v_i = s\sum_i a_i v_i + \sum_i b_i v_i = sv + w,$$

so $[sv + w] = sa + b$. Hence

$$T(sv + w) = \sum_{i=1}^{n} (sa_i + b_i)w_i = s\sum_i a_i w_i + \sum_i b_i w_i = sT(v) + T(w),$$

so $T$ is linear. In addition, $[v_i]_{\mathcal{B}} = e_i$, so $T(v_i) = w_i$.

Conversely, if $v \in V$ and $a = [v]_{\mathcal{B}}$, then $v = \sum_i a_i v_i$ by definition. So if $T' : V \to W$ is linear and $T'(v_i) = w_i$ for all $1 \leq i \leq n$, then $T'(v) = \sum_i a_i T'(v_i) = \sum_i a_i w_i = T(v)$ for all $v \in V$. So $T = T'$. □

Because $T$ is essentially defined by declaring $T(v_i) = w_i$, and then setting $T(\sum_i a_i v_i) = \sum_i a_i T(v_i)$, when we want to use this method of defining $T$, we say that we are **declaring $T$ on a basis, and then extending linearly**.

There are two subspaces associated with a linear transformation $T : V \to W$, the **kernel** or **nullspace**

$$\ker T := \{v \in V : T(v) = 0\} = T^{-1}(v) \subseteq V$$

and the **image**

$$\operatorname{Im} T := \{w \in W : \text{ there exists } v \in V \text{ such that } T(v) = w\} = T(V) \subseteq W.$$

One of the reasons these two subspaces are important is that they control whether a linear transformation is injective or surjective:

**Proposition 2.1.16.** *Let $T : V \to W$ be a linear transformation. Then:*

*(a) $T$ is injective (sometimes called one-to-one) if and only if $\ker T = 0$.*

*(b) $T$ is surjective (sometimes called onto) if and only if $\operatorname{Im} T = W$.*

### 2.1.3 Isomorphisms

Recall that a function $f : X \to Y$ between two sets is said to be bijective if it is both injective and surjective, and invertible if there is a function $g : Y \to X$ such that $f \circ g = \mathbb{1}_Y$ and $g \circ f = \mathbb{1}_X$, where $\mathbb{1}_X$ and $\mathbb{1}_Y$ are the identity functions $X \to X$ and $Y \to Y$ respectively. If $f$ is invertible, then the inverse function $g$ is unique, and is denoted by $f^{-1}$. It is a standard fact about functions that $f$ is invertible if and only if $f$ is bijective.

There is a special name for bijective (aka. invertible) linear transformations:

**Definition 2.1.17.** *An $\mathbb{F}$-linear transformation $T : V \to W$ is an **isomorphism** if $T$ is invertible. If there is an isomorphism $T : V \to W$, then we say that $V$ **is isomorphic to** $W$, and write $V \cong W$.*

**Example 2.1.18.** *The identity map $\mathbb{1} : V \to V$ is an isomorphism.*

Given an isomorphism $T : V \to W$, we can translate from $V$ to $W$ by applying $T$, and from $W$ to $V$ by applying $T^{-1}$. Since $T$ is linear, if we perform a vector operation $sv + w$, $s \in \mathbb{F}$ and $v, w \in V$, and translate to $W$ via $T$, then we get $T(sv+w) = sT(v)+T(w)$, which is the same operation applied to the translates $T(v)$ and $T(w)$ of $v$ and $w$. However, it's not immediately clear what happens if we try to translate a vector operation from $W$ to $V$ via $T^{-1}$, since $T^{-1}$ is just the inverse of $T$ as a function. Fortunately, it turns out that the inverse $T^{-1}$ of an invertible linear transformations $T$ is also linear. So if we perform a vector operation $sv + w$ on vectors $v, w \in W$ and translate to $V$ via $T^{-1}$, we get $T^{-1}(sv + w) = sT^{-1}(v) + T^{-1}(w)$, the same operation applied to $v$ and $w$. Combining the linearity of $T$ and $T^{-1}$, we see that we have two ways of doing vector operations in $V$. If we wanted to, say, add two vectors $v, w \in V$, we could take the sum $v + w$ in $V$ directly. Or we could translate to $T(v), T(w) \in W$, take the sum $T(v) + T(w) \in W$, and then translate back via $T^{-1}$. Since $T^{-1}(T(v) + T(w)) = T^{-1}T(v) + T^{-1}T(w) = v + w$, we get the same thing from either method.

The upshot of this is that, from the point of view of linear algebra, we can treat $\cong$ kind of like an equality sign. Of course, $V$ and $W$ might be very different as sets, but if $V \cong W$, then vector operations on the two sets are equivalent, in the sense that we can translate freely back and forth between the two. And from the point of view of linear algebra, the vector operations are all we care about, so we can regard $V$ and $W$ as being essentially the same vector space.

The isomorphism relation $\cong$ also behaves formally like an equality sign. Since the identity map is an isomorphism, $V \cong V$ for any vector space $V$.

And if $T : V \to W$ is an isomorphism, then $T^{-1} : W \to V$ is invertible and linear, so if $V \cong W$ then $W \cong V$. And finally, if $S : U \to V$ and $T : V \to W$ are isomorphisms, then $T \circ S : U \to W$ is an isomorphism, so if $U \cong V$ and $V \cong W$, then $U \cong W$. When a relation satisfies these three properties, we say that it is an equivalence relation, so $\cong$ is an equivalence relation on the class of vector spaces. We'll look at equivalence relations in more detail in a later chapter.

Since isomorphic vector spaces are essentially the same, if $T : V \to W$ is an isomorphism, and $\mathcal{B}$ is a basis for $V$, then $T(\mathcal{B}) := \{T(v) : v \in \mathcal{B}\}$ is a basis for $W$. It turns out that this property characterizes isomorphism:

**Proposition 2.1.19.** *Let $T : V \to W$ be a linear transformation. Then the following are equivalent:*

*(a) $T$ is an isomorphism.*

*(b) For every basis $\mathcal{B}$ of $V$, $T(\mathcal{B})$ is a basis of $W$.*

*(c) For some basis $\mathcal{B}$ of $V$, $T(\mathcal{B})$ is a basis of $W$.*

*As a result, if $V \cong W$, then $\dim V = \dim W$.*

**Example 2.1.20.** *Suppose $V$ and $W$ are $n$-dimensional vector spaces. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis for $V$, and $\mathcal{C} = \{w_1, \ldots, w_n\}$ be a basis for $W$. Define $T : V \to W$ by setting $T(v_i) = w_i$ and extending linearly. Then $T$ sends the basis $\mathcal{B}$ of $V$ to the basis $\mathcal{C}$ of $W$, so by Proposition 2.1.19, $T$ is an isomorphism. Since isomorphic vector spaces have the same dimension, we conclude that $V \cong W$ if and only if $\dim V = \dim W$.*

*Note that the isomorphism $T$ depends on the choice of $\mathcal{B}$ and $\mathcal{C}$. Changing either of them will change $T$. Unless $\dim V = \dim W = 0$, if $V \cong W$ then there are infinitely many isomorphisms between the two spaces. Often it's not very interesting to observe that $V \cong W$. Instead, we often ask that the isomorphism be natural in some way, as in Examples 2.1.18 or the upcoming examples 2.1.24 or 2.1.25. This is a concept we'll explore more deeply when we look at tensors.*

We can also understand isomorphisms in terms of matrices:

**Exercise 2.1.21.** *(a) Suppose $S : U \to V$ and $T : V \to W$ are linear transformations, and $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$ are bases of $U$, $V$, and $W$ respectively. Use the definition of the coordinate matrix to show that*

$$[T]_{\mathcal{D},\mathcal{C}}[S]_{\mathcal{C},\mathcal{B}} = [TS]_{\mathcal{D},\mathcal{B}}.$$

(b) *Let $V$ and $W$ be vector spaces with bases $\mathcal{B}$ and $\mathcal{C}$. Use part (a) to show that a linear transformation $T : V \to W$ is an isomorphism if and only if $[T]_{\mathcal{C},\mathcal{B}}$ is an invertible square matrix.*

(c) *Show in part (b) that if $T$ is an isomorphism, then $[T^{-1}]_{\mathcal{B},\mathcal{C}} = [T]^{-1}_{\mathcal{C},\mathcal{B}}$.*

We'll discuss one approach to Exercise 2.1.21 in the next section.

Since the identity map $\mathbb{1} : V \to V$ is an isomorphism, a change of basis matrix $[\mathbb{1}]_{\mathcal{R},\mathcal{B}}$ is an invertible matrix. It's interesting to look at what matrices can be change of basis matrices:

**Exercise 2.1.22.** *Let $\mathcal{B}$ be a basis for an $n$-dimensional vector space $V$, and let $A$ be an $n \times n$ invertible matrix. Show that there is a basis $\mathcal{C}$ for $V$ such that $A = [\mathbb{1}]_{\mathcal{B},\mathcal{C}}$, the change of basis matrix from $\mathcal{C}$ to $\mathcal{B}$.*

As a result of this exercise, we can think of an invertible $n \times n$ matrix in two ways: as the matrix in the standard basis of the isomorphism $\mathbb{F}^n \to \mathbb{F}^n : v \mapsto Av$, and as the change of basis matrix $[\mathbb{1}]_{\mathcal{B},\mathcal{C}}$ from some basis $\mathcal{C}$ to the standard basis $\mathcal{B}$. Having these two perspectives on invertible matrices can sometimes be useful.

### 2.1.4 Isomorphisms and diagrams

When first learning linear algebra, we typically focus on questions like "Is the given linear transformation invertible?" However, once we've mastered the basic concepts, our focus shifts and we con start to use these basic concepts as building blocks in more advanced concepts. This is especially true of isomorphisms. The idea of two spaces being equivalent is very powerful, and since isomorphisms turn up all over the place, we can use isomorphisms a lot. One of the most useful examples of an isomorphism is a map we've already looked at:

**Exercise 2.1.23.** *Let $\mathcal{B}$ be an ordered basis of an $\mathbb{F}$-vector space $V$ of dimension $n$. Then the coordinate map*

$$c_{\mathcal{B}} : V \to \mathbb{F}^n : v \mapsto [v]_{\mathcal{B}}$$

*is both linear and bijective, and hence is an isomorphism. The inverse of this map is the linear transformation*

$$c_{\mathcal{B}}^{-1} : \mathbb{F}^n \to V : a \mapsto \sum_{i=1}^{n} a_i v_i.$$

In other words, any $n$-dimensional vector space $V$ is equivalent to $\mathbb{F}^n$, at least if we're willing to pick an ordered basis. Of course, we don't always want to commit to a choice of basis, so an abstract vector space isn't necessarily the same thing as $\mathbb{F}^n$. But not having to commit to a particular choice of basis is really the only difference between abstract vector spaces and $\mathbb{F}^n$ (typically we think of $\mathbb{F}^n$ as coming with its standard basis).

Another helpful example to look at is the set of linear transformations

$$\mathrm{Lin}(V, W) := \{T : V \to W | T \text{ is linear } \}$$

between two vector spaces. The set $\mathrm{Lin}(V, W)$ is a subspace of the vector space $\mathrm{Fun}(V, W)$, and hence is a vector space under pointwise addition and scalar multiplication. If $V \cong V'$ and $W \cong W'$ then intuitively we should be able to replace $V$ with $V'$ and $W$ with $W'$. So that means that $\mathrm{Lin}(V, W)$ and $\mathrm{Lin}(V', W')$ should be equivalent spaces. To back that up, let's say that are isomorphisms are $S : V \to V'$ and $R : W \to W'$ respectively. Given a linear transformation $T : V \to W$, we have a bunch of maps between different spaces which we can arrange into the following diagram (ignoring the dotted line for the moment):

$$\begin{tikzcd}
V \arrow[r, bend left, "S"] \arrow[d, "T"'] & V' \arrow[l, bend left, "S^{-1}"] \arrow[d, dashed, "RTS^{-1}"] \\
W \arrow[r, bend left, "R"] & W' \arrow[l, bend left, "R^{-1}"]
\end{tikzcd} \tag{2.1.1}$$

Starting at $V'$, we can follow the arrows through $S^{-1}$, $T$, and $R$, to get the linear map $RTS^{-1} : V' \to W'$, which we put on the dotted line. Going in the other direction, if we were given a linear transformation $T' : V' \to W'$, we could follow the arrows again from $V$ through $S$, $T'$, and $R^{-1}$, to get a linear transformation $R^{-1}T'S : V \to W$. It's not hard to see that this gives a bijection between $\mathrm{Lin}(V, W)$ and $\mathrm{Lin}(V', W')$. In fact, we can go further:

**Exercise 2.1.24.** *Show that* $\mathrm{Lin}(V, W) \to \mathrm{Lin}(V', W') : T \mapsto RTS^{-1}$ *is an isomorphism.*

While it's not necessary to use the above diagram to prove this exercise, diagrams like this are very useful when we have a lot of linear transformations in play. One interesting property of this diagram is that if we pick two paths in the diagram with the same starting and ending space, then each path gives us the same linear transformation. For instance, if we start at $V$, and take $S$ followed by $RTS^{-1}$, we get $(RTS^{-1})S = RT : V \to W'$. If we take $T$ and then $R$, we get the same transformation. Diagrams with this property are said to be **commutative**. Commutative diagrams are one of the main tools in category theory. We won't get into formal category theory in this course[1], but we will use commutative diagrams and some other concepts from category theory informally when working with diagrams.

One special case where we often use the isomorphism in Exercise 2.1.24 when the isomorphisms are coordinate maps. Specifically, let $\mathcal{B}$ and $\mathcal{C}$ be bases for vector spaces $V$ and $W$ of dimension $n$ and $m$ respectively. Let

$$c_{\mathcal{B}} : V \to \mathbb{F}^n : v \mapsto [v]_{\mathcal{B}} \quad \text{and} \quad c_{\mathcal{C}} : W \to \mathbb{F}^m : w \mapsto [w]_{\mathcal{C}}$$

be the corresponding coordinate map. Setting $S = c_{\mathcal{B}}$ and $R = c_{\mathcal{C}}$ in the above diagram, we get

$$\begin{tikzcd}
V \arrow[r, bend left, "c_{\mathcal{B}}"] \arrow[d, "T"'] & \mathbb{F}^n \arrow[l, bend left, "c_{\mathcal{B}}^{-1}"] \arrow[d, "c_{\mathcal{C}} T c_{\mathcal{B}}^{-1}"] \\
W \arrow[r, bend left, "c_{\mathcal{C}}"] & \mathbb{F}^m \arrow[l, bend left, "c_{\mathcal{C}}^{-1}"]
\end{tikzcd}$$

(2.1.2)

As a linear transformation $\mathbb{F}^n \to \mathbb{F}^m$, $c_{\mathcal{C}} T c_{\mathcal{B}}^{-1}$ must be of the form $x \mapsto Ax$ for some matrix $A \in M_{mn}\mathbb{F}$. If we start with a vector $v \in V$, and apply $c_{\mathcal{B}}$ followed by $c_{\mathcal{C}} T c_{\mathcal{B}}^{-1}$, we get $Ac_{\mathcal{B}}(v) = A[v]_{\mathcal{B}}$. On the other hand, if we apply $T$ followed by $c_{\mathcal{C}}$, we get $c_{\mathcal{C}}T(v) = [T(v)]_{\mathcal{C}}$. Since we're supposed to get the same vector in $\mathbb{F}^m$ no matter what path we take, we must have $[T(v)]_{\mathcal{C}} = A[v]_{\mathcal{B}}$. In other words, $A = [T]_{\mathcal{C},\mathcal{B}}$, the coordinate matrix of $T$ with respect to $\mathcal{C}$ and $\mathcal{B}$. This is a very simple example of an argument by **diagram chasing**, so-called since we start with a vector $v$ in one of the vector spaces, and chase it around the diagram.

Given a matrix $A \in M_{mn}\mathbb{F}$, we can also go the other way in this diagram, filling in the arrow from $\mathbb{F}^n \to \mathbb{F}^m$ with the linear transformation

[1] It's not hard, we've just got other things to cover

$T' : \mathbb{F}^n \to \mathbb{F}^m : x \mapsto Ax$, and setting $T = c_{\mathcal{C}}^{-1} T' c_{\mathcal{B}}$. As you might expect, this method of going back and forth between linear transformation and matrix is an isomorphism as well:

**Exercise 2.1.25.** *Suppose $V, W$ are vector spaces with bases $\mathcal{B}$ and $\mathcal{R}$ respectively, where $\dim V = n$, and $\dim W = m$. Then the function*

$$\mathrm{Lin}(V, W) \to M_{mn}\mathbb{F} : T \mapsto [T]_{\mathcal{R},\mathcal{B}}$$

*is an isomorphism. In particular, the function $\mathrm{Fun}(\mathbb{F}^n, \mathbb{F}^m) \to M_{mn}\mathbb{F}$ which sends a linear transformation $\mathbb{F}^n \to \mathbb{F}^m$ to its matrix in the standard basis is an isomorphism.*

Since $\dim M_{mn}\mathbb{F} = mn$, this exercise implies that $\dim \mathrm{Lin}(V, W) = (\dim V)(\dim W)$.

To finish this section, we note that diagrams don't have to be squares. For instance, one way to prove part (a) of Exercise 2.1.21 is using the diagram

$$\begin{tikzcd}
U \arrow[r, "c_{\mathcal{B}}"] \arrow[d, "S"'] & \mathbb{F}^n \arrow[d, "c_{\mathcal{C}} S c_{\mathcal{B}}^{-1}"] \\
V \arrow[r, "c_{\mathcal{C}}"] \arrow[d, "T"'] & \mathbb{F}^m \arrow[d, "c_{\mathcal{D}} T c_{\mathcal{C}}^{-1}"] \\
W \arrow[r, "c_{\mathcal{D}}"] & \mathbb{F}^k
\end{tikzcd}$$

where $n = \dim U$, $m = \dim V$, and $k = \dim W$.

## 2.2 Free vector spaces

**Definition 2.2.1.** *Let $X$ be a finite set and $\mathbb{F}$ be a field. The **free vector space spanned by $X$ over $\mathbb{F}$** is the vector space of formal sums*

$$\mathbb{F}X := \left\{ \sum_{x \in X} c_x \left| x \right\rangle : c_x \in \mathbb{F} \text{ for all } x \in X \right\},$$

*with the operations*

$$\sum_{x\in X} c_x \left|x\right\rangle + \sum_{x\in X} d_x \left|x\right\rangle := \sum_{x\in X}(c_x + d_x) \left|x\right\rangle$$

*and*

$$s \cdot \sum_{x\in X} c_x \left|x\right\rangle := \sum_{x\in X} sc_x \left|x\right\rangle .$$

The idea behind free vector spaces is that we can make a vector space from any set $X$ by just declaring the elements of $X$ to be basis vectors. Thus given $x, y \in X$, we can talk about vectors like $x + 11y$ or $3x$. This works great if $X$ is a set of symbols like $X = \{\vec{i}, \vec{j}, \vec{k}\}$. Vectors in $\mathbb{R}^3$ are often written this way. For instance $3\vec{i} - \vec{j} + 7\vec{k}$ would refer to the vector $(3, -1, 7)$. However, this notation does not work so well if $X$ is a set like $\{0, 1, 2\}$. The expression $3 \cdot 0 - 1 + 7 \cdot 2$ looks like 13, not like a vector in a three-dimensional vector space. To get around this notational problem, we write $\left|x\right\rangle$ for the element of $\mathbb{F}X$ corresponding to $x \in X$. This is our first encounter with **Dirac notation**. We'll use this notation in a variety of ways in this course.

**Example 2.2.2.** *If $X = \{0, \ldots, n\}$, then the elements of $\mathbb{C}X$ are linear combinations*

$$\sum_{i=0}^{n} c_i \left|i\right\rangle, c_0, \ldots, c_n \in \mathbb{C}.$$

*For instance, if $n = 1$, we might write*

$$-\left|0\right\rangle + 2\left|1\right\rangle + 2(5\left|0\right\rangle - 3\left|1\right\rangle) = 9\left|0\right\rangle - 4\left|1\right\rangle .$$

Note that if $c_x = 0$ in an element $\sum c_x \left|x\right\rangle$ of $\mathbb{F}X$, then we usually drop $\left|x\right\rangle$ from the formal expression. For instance, in the above example, $\left|0\right\rangle$ by itself would refer to the formal sum $1\left|0\right\rangle + 0\left|1\right\rangle$, so $c_0 = 1$ and $c_1 = 0$.

**Proposition 2.2.3.** *$\mathbb{F}X$ is a vector space, and the set $\{\left|x\right\rangle, x \in X\}$ is a basis for $\mathbb{F}X$.*

*Proof.* Choose an order $X = \{x_1, \ldots, x_n\}$ of the elements of $X$. Then the formal sums $\sum_{i=1}^{n} c_i \left|x_i\right\rangle$ can be thought of as vectors $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in \mathbb{F}^n$, so $\mathbb{F}X$ is a vector space for the same reason $\mathbb{F}^n$ is. In this correspondence, $\left|x_i\right\rangle$ corresponds to the $i$th standard basis vector $e_i$, so $\{\left|x_i\right\rangle : i = 1, \ldots, n\}$ is a basis. □

This proof shows that if $|X| = n$, then $\mathbb{F}X \cong \mathbb{F}^n$. However, this requires us to pick an order on $X$. Part of the point of defining $\mathbb{F}X$ is that we don't need to pick such an order. However, when $X$ has a natural order, such as when $X = \{0, \ldots, n-1\}$, we will often think of $\mathbb{F}X$ and $\mathbb{F}^n$ as being identical. When $X$ doesn't have an order, we can still identify $\mathbb{F}X$ with a more concrete space as follows:

**Exercise 2.2.4.** *Show that if $X$ is a finite set, then $\mathbb{F}X \cong \mathrm{Fun}(X, \mathbb{F})$.*

By Exercise 2.2.4, we could use $\mathrm{Fun}(X, \mathbb{F})$ as the definition of $\mathbb{F}X$ if we wanted. The basic idea, a list of numbers indexed by a set $X$, is essentially the same.

This changes if $X$ is an infinite set. To be concrete, let's take $X = \mathbb{N} = \{1, 2, 3, \ldots\}$. Then $\mathbb{F}X$ should clearly include the formal sums

$$|1\rangle + |2\rangle + \ldots + |n\rangle$$

for any $n \geq 1$. However infinite formal sums like

$$|1\rangle + |2\rangle + \ldots + |n\rangle + \ldots$$

are less clear. We actually end up excluding these, with the reasoning that $\mathbb{F}X$ is the space of formal linear combinations of elements of $X$, and linear combinations are always finite. So for infinite sets we end up making the definition:

**Definition 2.2.5.** *Let $X$ be a set, and $\mathbb{F}$ a field. Then the free vector space $\mathbb{F}X$ is the vector space of formal sums*

$$\mathbb{F}X := \left\{ \sum_{x \in X} c_x \, |x\rangle : c_x \in \mathbb{F} \textit{ for all } x \in X, \textit{ and } c_x = 0 \textit{ for all but finitely many } x \in X \right\},$$

*and operations defined as in 2.2.1.*

**Exercise 2.2.6.** *Let $X$ be a set and $\mathbb{F}$ a field. Show that*

$$\{ f \in \mathrm{Fun}(X, \mathbb{F}) : f^{-1}(\mathbb{F} \setminus \{0\}) \textit{ is finite } \} \tag{2.2.1}$$

*is a subspace of* $\mathrm{Fun}(X, \mathbb{F})$.

The subspace in Equation (2.2.1) is known as the space of **finitely supported functions**. We could use this subspace as the definition of $\mathbb{F}X$ for arbitrary sets $X$ if we wanted to, and as in the finite case, this shows that $\mathbb{F}X$ is a vector space.

Another use for free vector spaces is for linearizing functions:

**Proposition 2.2.7.** *Suppose $\mathbb{F}$ is a field, $X$ is a set, and $W$ is an $\mathbb{F}$-vector space. If $f : X \to W$ is a function, then there is a unique linear map $T : \mathbb{F}X \to W$ sending $T\,|x\rangle = f(x)$ for all $x \in X$.*

*Proof.* Since $\{|x\rangle : x \in X\}$ is a basis for $\mathbb{F}X$, we can define $T$ by setting $T\,|x\rangle = f(x)$, and then extending linearly. Uniqueness of $T$ also follows from Lemma 2.1.15. □

In particular, if $X$ and $Y$ are sets, and $f : X \to Y$ is a function, then there is a unique linear function $T : \mathbb{F}X \to \mathbb{F}Y$ such that $T\,|x\rangle = |f(x)\rangle$.

## 2.3 Dual spaces

Although $\mathbb{F}$ denotes the field of scalars, $\mathbb{F}$ can also be thought of as the one-dimensional $\mathbb{F}$-vector space $\mathbb{F}^1$, or equivalently as the space $M_{11}\mathbb{F}$ of $1 \times 1$ matrices. The standard basis of $\mathbb{F}$ consists of single standard basis vector $e_1$, which is really just the element $1 \in \mathbb{F}$. As a special case of Example 2.1.7, we see that $[x]_{\{1\}} = x$ for all $x \in \mathbb{F}$.

If we plug $\mathbb{F}$ in as the codomain in $\mathrm{Lin}(V, \mathbb{F})$, we get an interesting space: elements $f \in \mathrm{Lin}(V, \mathbb{F})$ send vectors $v \in V$ to scalars $f(v) \in \mathbb{F}$.

**Definition 2.3.1.** *If $V$ is an $\mathbb{F}$-vector space, then the space $\mathrm{Lin}(V, \mathbb{F})$ of linear functions $V \to \mathbb{F}$ is called the **dual space** of $V$, and is denoted by $V^*$. Elements of $V^*$ are sometimes called **linear functionals** on $V$.*

Since we pretty much always want to work with the standard basis on $\mathbb{F}$, given a basis $\mathcal{B}$ for $V$, we let $[f]_{\mathcal{B}} := [f]_{\{1\},\mathcal{B}}$ for all $f \in V^*$. Note that if $V$ is $n$-dimensional, then $[f]_{\mathcal{B}} \in M_{1n}\mathbb{F}$, which is the space of $1 \times n$ row vectors. This is interesting, because we know that if $v \in V$, then $[v]_{\mathcal{B}} \in \mathbb{F}^n$, which we defined as the space of $n \times 1$ column vectors. According to the rules of matrix multiplication, row vectors and column vectors of the same dimension can be multiplied together to get an element of $M_{11}\mathbb{F} = \mathbb{F}$. So the product $[f]_{\mathcal{B}} \cdot [v]_{\mathcal{B}}$ seems to be another way to get a scalar by pairing up $f$ and $v$. However, if we apply the definition of the coordinate matrix for $f$, we see that

$$[f]_{\{1\},\mathcal{B}} \cdot [v]_{\mathcal{B}} = [f(v)]_{\{1\}} = f(v),$$

so this product $[f]_{\mathcal{B}}[v]_{\mathcal{B}}$ is just another way to get $f(v)$. So to summarize, if we pick a basis $\mathcal{B}$ for $V$, then $V$ is isomorphic to the space of column vectors $\mathbb{F}^n$, $V^*$ is isomorphic to the space of $1 \times n$ row vectors, and the "dual pairing" $(f, v) \mapsto f(v)$ corresponds to matrix multiplication of these vectors.

As we see from the above paragraph, $\dim V^* = \dim V$. Given a basis $\mathcal{B}$ for $V$, we can define a nice basis for $V^*$.

**Proposition 2.3.2.** *Suppose $\mathcal{B} = \{x_1, \ldots, x_n\}$ is a basis for $V$. Then there is a unique basis $\{x^1, \ldots, x^n\}$ for $V^*$ such that $x^i(x_j) = \delta_{ij}$, where $\delta_{ij}$ is the Kronecker delta.*[2]

The basis $\{x^1, \ldots, x^n\}$ is called the **Kronecker dual basis to $\mathcal{B}$**.

*Proof #1 — exercise.* For each $1 \leq i \leq n$, define a linear transformation $x^i : V \to \mathbb{F}$ by setting $x^i(x_j) = \delta_{ij}$, and extending linearly. We leave it as an exercise to show that $\{x^1, \ldots, x^n\}$ is a basis (since $\dim V^* = n$, is enough to either show spanning or linear independence). □

*Proof #2.* Let $f_i$ denote the row vector in $M_{1n}\mathbb{F}$ with a 1 in position $i$, and zeroes elsewhere. Then $\{f_1, \ldots, f_n\}$ is a basis for $M_{1n}\mathbb{F}$. Pick a basis $\mathcal{B}$ for $V$, and let $c$ be the isomorphism $V^* \to M_{1n}\mathbb{F} : f \mapsto [f]_{\mathcal{B}}$. Let $x^i := c^{-1}(f_i)$. Then

$$x^i(x_j) = [x^i]_{\mathcal{B}}[x_j]_{\mathcal{B}} = c(x^i)[x_j]_{\mathcal{B}} = f_i \cdot e_j = \delta_{ij}.$$

□

As spaces of the same dimension, $V \cong V^*$. However, this is one of those cases where we don't have a natural map between the two spaces. The best that we can do is to pick a basis $\mathcal{B} = \{x_1, \ldots, x_n\}$, let $\{x^1, \ldots, x^n\}$ be the Kronecker dual basis to $\mathcal{B}$, and then take the isomorphism $V \to V^*$ which sends $x_i \mapsto x^i$ for all $1 \leq i \leq n$. Unfortunately, this still depends on the choice of basis:

**Exercise 2.3.3.** *Find an example of a vector space $V$, and two bases $\mathcal{B}_1$ and $\mathcal{B}_2$ for $V$, such that if $\mathcal{B}_i = \{x_{i1}, \ldots, x_{in}\}$, $\{x_i^1, \ldots, x_i^n\}$ is the dual basis to $\mathcal{B}_i$, and $T_i : V \to V^*$ is the isomorphism sending $x_{ij} \mapsto x_i^j$, then $T_1 \neq T_2$.*

A related note is point is that, although these isomorphisms send $x_i$ to the dual vector $x^i$, we can't define $x^i$ without having the whole basis $x_1, \ldots, x_n$.

**Exercise 2.3.4.** *Find vectors $x_1, x_2, x_2' \in \mathbb{F}^2$ such that $\{x_1, x_2\}$ and $\{x_1, x_2'\}$ are bases for $\mathbb{F}^2$, but where vector $x^1$ in the dual basis $\{x^1, x^2\}$ to $\{x_1, x_2\}$ is different from the vector $y^1$ in the dual basis $\{y^1, y^2\}$ to $\{x_1, x_2'\}$.*

Nonetheless, the isomorphism we get from the Kronecker dual basis still has some nice features:

[2] The Kronecker delta $\delta_{ij}$ is 1 if $i = j$, and otherwise is 0. So this is a way of saying that $x^i(x_j) = 1$ if $i = j$, and $x^i(x_j) = 0$ if $i \neq j$.

**Exercise 2.3.5.** *Let $\mathcal{B} = \{x_1, \ldots, x_n\}$ be a basis for an $n$-dimensional space $V$, and let $\mathcal{B}' = \{x^1, \ldots, x^n\}$ be the Kronecker dual basis. Consider the coordinate maps*

$$c_{\mathcal{B}} : V \to \mathbb{F}^n : v \mapsto [v]_{\mathcal{B}}, c_{\mathcal{B}'} : V^* \to \mathbb{F}^n : f \mapsto [f]_{\mathcal{B}'}, \text{ and } \widehat{c}_{\mathcal{B}} : V^* \to M_{1n} : f \mapsto [f]_{\mathcal{B}}.$$

*(Be careful with the difference between $c_{\mathcal{B}'}$ and $\widehat{c}_{\mathcal{B}}$, as the notation is similar. $[f]_{\mathcal{B}'}$ is the coordinate vector with respect to the basis $\mathcal{B}'$, while $[f]_{\mathcal{B}} = [f]_{\{1\},\mathcal{B}}$ is the coordinate matrix of $f$.) Finally, let $T$ be the isomorphism $V \to V^*$ sending $x_i \mapsto x^i$ for all $1 \leq i \leq n$.*

$$\begin{tikzcd}
V \arrow[r, "c_{\mathcal{B}}"] \arrow[d, "T"'] & \mathbb{F}^n \arrow[d, "\widehat{c}_{\mathcal{B}} T c_{\mathcal{B}}^{-1}"] \\
V^* \arrow[ur, "c_{\mathcal{B}'}"] \arrow[r, "\widehat{c}_{\mathcal{B}}"] & M_{1n}\mathbb{F}
\end{tikzcd} \tag{2.3.1}$$

(a) *Show that $T = c_{\mathcal{B}'}^{-1} c_{\mathcal{B}}$, and use this to conclude that $\widehat{c}_{\mathcal{B}} T c_{\mathcal{B}}^{-1} = \widehat{c}_{\mathcal{B}} c_{\mathcal{B}'}^{-1}$.*

(b) *Show that $\widehat{c}_{\mathcal{B}} T c_{\mathcal{B}}^{-1}(v) = v^T$ for all $v \in \mathbb{F}^n$, where $v^T$ is the transpose of $v$.*

# Chapter 3

# Hilbert spaces

Now that we've reviewed some linear algebra, we come to our first axiom of quantum probability.

**Axiom 1.** *A physical system corresponds to a Hilbert space.*

The term physical system refers to any region or system we might analyze in the physical world. Knowing that a physical system has a corresponding Hilbert space is useless on its own, but it does tell us one thing: we need to review Hilbert spaces before we proceed. So that's what we'll do in this chapter. Since it doesn't take any extra work, we'll actually cover inner product spaces over $\mathbb{R}$ or $\mathbb{C}$.

## 3.1 Sesquilinear forms

An inner product space is an $\mathbb{F}$-vector space with a positive definite sesquilinear form. For this definition, it is important that $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. If $x \in \mathbb{C}$, we say that $x > 0$ if $\overline{x} = x$ (so $x \in \mathbb{R}$ considered as a subfield of $\mathbb{C}$) and $x > 0$ as an element of $\mathbb{R}$.

**Definition 3.1.1.** *Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. A function $\langle , \rangle : V \times V \to \mathbb{F}$ is called a **sesquilinear form** if*

$$\langle su + v, w\rangle = \overline{s}\langle u, w\rangle + \langle v, w\rangle \text{ and } \langle u, sv + w\rangle = s\langle u, v\rangle + \langle u, w\rangle.$$

*for all $s \in \mathbb{C}$, $u, v, w \in V$.*

*A **hermitian form** is a sesquilinear form $\langle , \rangle$ such that*

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

*for all $u, v \in V$.*

*A **positive semidefinite form** is a hermitian form $\langle , \rangle$ such that*

$$\langle u, u \rangle \geq 0$$

*for all $u \in V$. A positive semidefinite form $\langle , \rangle$ is **positive definite** (or an **inner product**) if*

$$\langle u, u \rangle = 0 \text{ if and only if } u = 0$$

*for all $u \in V$.*

It's worth comparing sesquilinear forms to the related concept of bilinear forms:

**Definition 3.1.2.** *A function $\langle , \rangle : V \times V \to \mathbb{F}$ is called a **bilinear form** if*

$$\langle su + v, w \rangle = s\langle u, w \rangle + \langle v, w \rangle \text{ and } \langle u, sv + w \rangle = s\langle u, v \rangle + \langle u, w \rangle.$$

*for all $s \in \mathbb{F}$, $u, v, w \in V$.*

*A **symmetric form** is a bilinear form $\langle , \rangle$ such that*

$$\langle u, v \rangle = \langle v, u \rangle$$

*for all $u, v \in V$.*

When $\mathbb{F} = \mathbb{R}$, $\overline{x} = x$, and hence sesquilinear and bilinear forms are the same. In fact, normally the term "sesquilinear form" is only used for $\mathbb{F} = \mathbb{C}$ and other fields with a nontrivial involution. A sesquilinear form over $\mathbb{R}$ would just be called a bilinear form, and a hermitian form would be called a symmetric form. However, we'll use sesquilinear form and hermitian form for both $\mathbb{R}$ and $\mathbb{C}$ to avoid having to state results twice.

**Example 3.1.3.** *The **standard inner product** on $\mathbb{F}^n$ is $\langle x, y \rangle = \sum_{i=1}^n \overline{x_i} y_i$. This inner product may also be denoted by $x \cdot y$, although this notation is most common when $\mathbb{F} = \mathbb{R}$.*

While sesquilinear forms and bilinear forms are the same over $\mathbb{R}$, they are different over $\mathbb{C}$.

**Exercise 3.1.4.** *The standard bilinear form on $\mathbb{C}^n$ is defined by $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$ (another way to write this is $\langle x, y \rangle = x^T y$, where $x^T$ is the transpose of $y$). For any $n \geq 2$, show that there is non-zero vector $x \in \mathbb{C}^n$ with $\langle x, x \rangle = 0$.*

We'll come back to bilinear forms when we consider tensor products.

We can define other sesquilinear forms on $\mathbb{F}^n$ using matrices, although we need some more definitions:

**Definition 3.1.5.** *If $M$ is an $m \times n$ matrix, then the* ***conjugate-transpose*** *of $M$ is the $n \times m$ matrix $M^*$ with $M^*_{ij} = \overline{M_{ji}}$. A matrix $M \in M_{nn}(\mathbb{F})$ is said to be*

- ***hermitian*** *if $M^* = M$,*
- ***positive semidefinite*** *if it is hermitian and $x^* M x \geq 0$ for all $x \in \mathbb{F}^n$, and*
- ***positive definite*** *if it is hermitian and $x^* M x > 0$ for all $x \in \mathbb{F}^n \setminus \{0\}$.*

When $\mathbb{F} = \mathbb{R}$, $M^* = M^T$, the transpose of $M$, and a matrix satisfying $M^T = M$ is usually called a **symmetric matrix**, rather than a hermitian matrix. As with forms, we use hermitian matrix when working over both $\mathbb{R}$ and $\mathbb{C}$ to avoid stating results twice. Recall that $(AB)^T = B^T A^T$, and it is not hard to see that $(AB)^* = B^* A^*$ as well. Also, the formula for the standard inner product on $\mathbb{F}^n$ can be written as $\langle x, y \rangle = x^* y$. This is generalized in the following lemma:

**Lemma 3.1.6.** *Let $M$ be an $n \times n$ matrix over $\mathbb{F}$. Then*

$$\langle x, y \rangle := x^* M y$$

*is a sesquilinear form on $\mathbb{F}^n$. Furthermore, $\langle , \rangle$ is hermitian (resp. positive semidefinite, positive definite) if and only if $M$ is hermitian (resp. positive semidefinite, positive definite).*

*Proof.* We leave it as an exercise to show that $\langle , \rangle$ is sesquilinear. The form $\langle , \rangle$ is hermitian if and only if

$$x^* M y = \langle x, y \rangle = \overline{\langle y, x \rangle} = \overline{y^* M x} = (y^* M x)^* = x^* M^* y$$

for all $x, y \in \mathbb{F}^n$. So if $M^* = M$ then $\langle , \rangle$ is hermitian. Conversely, if $\langle , \rangle$ is hermitian, then setting $x = e_i$, $y = e_j$, we see that $M_{ij} = M^*_{ji}$ for all $i, j$, so $M = M^*$. The fact that $\langle , \rangle$ is positive semidefinite (resp. positive definite) if and only if $M$ is positive semidefinite (resp. positive definite) follows immediately from Definition 3.1.5. □

Taking $M$ to be the identity map in Lemma 3.1.6 gives the standard inner product. It turns out that every sesquilinear form comes from a matrix in this way:

**Definition 3.1.7.** *Let $\langle , \rangle$ be a sesquilinear form on a vector space $V$, and let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis for $V$ (so $\dim V = n$). The* ***matrix of $\langle , \rangle$ with respect to $\mathcal{B}$*** *is the $n \times n$ matrix $M$ such that $M_{ij} = \langle v_i, v_j \rangle$.*

**Example 3.1.8.** *Suppose $M$ is an $n \times n$ matrix over $\mathbb{F}$, and use $M$ to define a sesquilinear form $\langle , \rangle$ on $\mathbb{F}^n$ via $\langle x, y\rangle = x^* M y$. If $\mathcal{B} = \{e_1, \dots, e_n\}$ is the standard basis for $\mathbb{F}^n$, then*

$$\langle e_i, e_j \rangle = e_i^* M e_j = M_{ij},$$

*so the matrix of $\langle , \rangle$ is just $M$.*

There really isn't standard notation for the matrix of $\langle , \rangle$ with respect to $\mathcal{B}$. The obvious suggestion would be $[\langle , \rangle]_{\mathcal{B}}$, but that's a lot of brackets.

**Lemma 3.1.9.** *If $\langle , \rangle$ is a sesquilinear form on $V$, and $M$ is the matrix of $\langle , \rangle$ with respect to a basis $\mathcal{B}$ for $V$, then*

$$\langle x, y \rangle = [x]_{\mathcal{B}}^* M [y]_{\mathcal{B}}.$$

*Furthermore, $M$ is the unique matrix satisfying this equation.*

*Proof.* Let $\mathcal{B} = \{v_1, \dots, v_n\}$, and set $a = [x]_{\mathcal{B}}$ and $b = [y]_{\mathcal{B}}$. By definition, $x = \sum_{i=1}^n a_i v_i$, and $y = \sum_{i=1}^n b_i v_i$. So

$$\langle x, y \rangle = \langle \sum_{i=1}^n a_i v_i, \sum_{j=1}^n b_j v_j \rangle = \sum_{1 \le i,j \le n} \overline{a_i} b_j \langle v_i, v_j \rangle = \sum_{i1 \le i,j \le n} \overline{a_i} M_{ij} b_j = a^* M b.$$

Now suppose that $\langle x, y \rangle = [x]_{\mathcal{B}}^* M' [y]_{\mathcal{B}}$ for all $x, y \in V$. Since the coordinate map $x \mapsto [x]_{\mathcal{B}}^*$ is an isomorphism, this is the same thing as saying that $v^* M w = v^* M' w$ for all $v, w \in \mathbb{F}^n$, which implies that $v^*(M - M')w = 0$ for all $v, w \in \mathbb{F}^n$. If we take $v$ and $w$ to be the standard basis vectors $e_i$ and $e_j$, we get that $(M - M')_{ij} = 0$. Since this holds for all $i, j$, we get that $M = M'$. □

We've seen that we can define a sesquilinear form on $\mathbb{F}^n$ by specifying an $n \times n$ matrix, but what about defining forms on abstract vector spaces $V$? We can do this by choosing a linear map to a space where we already have a sesquilinear form:

**Proposition 3.1.10.** *Let $T : V \to W$ be a linear map, and let $\langle , \rangle_W$ be a sesquilinear form on $W$. Define $\langle , \rangle_V$ by*

$$\langle v, w \rangle_V := \langle Tv, Tw \rangle_W$$

*for all $v, w \in V$. Then $\langle , \rangle_V$ is a sesquilinear form on $V$. Furthermore:*

- *if $\langle , \rangle_W$ is hermitian then $\langle , \rangle_V$ is hermitian;*

- *if $\langle , \rangle_W$ is positive semidefinite then $\langle , \rangle_V$ is positive semidefinite; and*
- *if $\langle , \rangle_W$ is positive definite and $T$ is injective then $\langle , \rangle_V$ is positive definite.*

*Proof.* We leave sesquilinearity as an exercise.

If $\langle , \rangle_W$ is hermitian, then

$$\langle v, w\rangle_V = \langle Tv, Tw\rangle_W = \overline{\langle Tw, Tv\rangle_W} = \overline{\langle w, v\rangle_V}$$

for all $v, w \in V$. If in addition $\langle , \rangle_W$ is positive-semidefinite then

$$\langle v, v\rangle_V = \langle Tv, Tv\rangle_W \geq 0$$

for all $v \in V$. Finally if $T$ is injective and $\langle , \rangle_W$ is positive-definite, then $Tv \neq 0$ for all $v \in V \setminus 0$, so

$$\langle v, v\rangle_V = \langle Tv, Tv\rangle_W > 0$$

for all $v \in V \setminus 0$. □

The form $\langle , \rangle_V$ defined in Proposition 3.1.10 is called the **pullback** of $\langle , \rangle_W$ to $V$ along $T$.

Putting together what we know so far gives a strong connection between forms and matrices:

**Theorem 3.1.11.** *Let $M$ be an $n \times n$ matrix over $\mathbb{F}$, and let $\mathcal{B}$ a basis for an $n$-dimensional vector space $V$. Then*

$$\langle x, y\rangle := [x]_{\mathcal{B}}^* M [y]_{\mathcal{B}}$$

*is a sesquilinear form on $V$. Furthermore, $M$ is the matrix of $\langle , \rangle$ with respect to $\mathcal{B}$, and $\langle , \rangle$ is hermitian (resp. positive semidefinite, positive definite) if and only if $M$ is hermitian (resp. positive semidefinite, positive definite).*

*Proof.* Let $\langle , \rangle'$ be the form on $\mathbb{F}^n$ defined by $\langle v, w\rangle' = v^* M w$, and let $c_{\mathcal{B}}$ be the isomorphism $V \to \mathbb{F}^n : v \mapsto [v]_{\mathcal{B}}$. Then

$$\langle x, y\rangle = [x]_{\mathcal{B}}^* M [y]_{\mathcal{B}} = \langle c_{\mathcal{B}}(x), c_{\mathcal{B}}(y)\rangle'$$

is the pullback of $\langle , \rangle'$ through $c_{\mathcal{B}}$. By Lemma 3.1.6 and Proposition 3.1.10, $\langle , \rangle$ is a sesquilinear form, and will be hermitian (resp. positive semidefinite, positive definite) if $M$ is hermitian (resp. positive semidefinite, positive definite). By Lemma 3.1.9, $M$ is the matrix of $\langle , \rangle$.

Going the other way,

$$\langle v, w\rangle' = \langle c_{\mathcal{B}}(c_{\mathcal{B}}^{-1}(v)), c_{\mathcal{B}}(c_{\mathcal{B}}^{-1}(w))\rangle' = \langle c_{\mathcal{B}}^{-1}(v), c_{\mathcal{B}}^{-1}(w)\rangle,$$

so $\langle , \rangle'$ is the pullback of $\langle , \rangle$ through $c_{\mathcal{B}}^{-1}$.[1] By Proposition 3.1.10, if $\langle , \rangle$ is hermitian (resp. positive semidefinite, positive definite) then $\langle , \rangle'$ will be hermitian (resp. positive semidefinite, positive definite), and hence $M$ will be hermitian (resp. positive semidefinite, positive definite) by Lemma 3.1.6. □

**Corollary 3.1.12.** *Let $\mathcal{B}$ be a basis for an $n$-dimensional vector space $V$. Then the map taking a sesquilinear form on $V$ to its matrix with respect to $\mathcal{B}$ is a bijection between sesquilinar forms on $V$ and the spaces of matrices $M_{nn}\mathbb{F}$. Furthermore, this bijection identifies hermitian (resp. positive semidefinite, positive definite) forms with hermitian (resp. positive semidefinite, positive definite) matrices.*

*Proof.* Let $\mathcal{F}$ be the set of sesquilinear forms on $V$, and let $\phi : \mathcal{F} \to M_{nn}\mathbb{F}$ be the function such that $\phi(\langle , \rangle)$ is the matrix of $\langle , \rangle$ with respect to $\mathcal{B}$. Let $\psi : M_{nn}\mathbb{F} \to \mathcal{F}$ be the function taking a matrix $M$ to the sesquilinear form $\langle x, y \rangle = [x]_{\mathcal{B}}^* M [y]_{\mathcal{B}}$. By Theorem 3.1.11, $M$ is the matrix of $\psi(M)$, and hence $\phi(\psi(M)) = M$. And by Lemma 3.1.9, $M = \psi(\phi(M))$. So $\phi$ and $\psi$ are inverses. The correspondence between hermitian, positive semidefinite, and positive definite forms and matrices follows immediately from Theorem 3.1.11. □

We won't need it, but we can upgrade this bijection to an isomorphism:

**Exercise 3.1.13.** *Let $\mathcal{B}$ be a basis for an $n$-dimensional vector space $V$.*

*(a) Show that the set of sesquilinear forms is a subspace of* $\mathrm{Fun}(V \times V, \mathbb{F})$, *and hence is a vector space with the pointwise operations.*

*(b) Show that the bijection in Corollary 3.1.12 is an isomorphism between the space of sesquilinear forms and $M_{nn}\mathbb{F}$.*

So far we've looked at the matrix of a form with respect to a single basis. However, it's natural to wonder what happens if we change the basis. In fact, there is a very nice change of basis formula:

**Exercise 3.1.14.** *Let $\langle , \rangle$ be a sesquilinear form on a vector space $V$, and let $M_i$ be the matrix of $\langle , \rangle$ with respect to basis $\mathcal{B}_i$, $i = 1, 2$. Show that*

$$M_2 = [\mathbb{1}]_{\mathcal{B}_1,\mathcal{B}_2}^* \ M_1 \ [\mathbb{1}]_{\mathcal{B}_1,\mathcal{B}_2}$$

[1] This is a general pattern that happens with isomorphisms $T : V \to W$. If we pull back a form $\langle , \rangle_W$ on $W$ to a form $\langle , \rangle_V$ on $V$, then $\langle , \rangle_W$ will end up being the pullback of $\langle , \rangle_V$ through $T^{-1}$.

## 3.2 Inner product spaces

Now we can define Hilbert spaces. Recall that an inner product is another term for a positive-definite sesquilinear form.

**Definition 3.2.1.** *A (finite-dimensional)* ***inner product space*** *is a pair $(H, \langle , \rangle)$ where $H$ is a (finite-dimensional) $\mathbb{F}$-vector space, $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, and $\langle , \rangle$ is an inner product on $H$. A* ***Hilbert space*** *is another name for an inner product space over $\mathbb{C}$, while an inner product space over $\mathbb{R}$ is also known as a* ***Euclidean space****.*

There is also a very nice theory of infinite-dimensional Hilbert spaces. Since we're focusing on the finite-dimensional case, we'll use "Hilbert space" to mean "finite-dimensional Hilbert space" in this course. But outside this course, Hilbert spaces are usually defined to include the infinite-dimensional case. In addition, note that we usually write $H$ instead of $(H, \langle , \rangle)$ when referring to an inner product space, and use $\langle , \rangle$ or $\langle , \rangle_H$ to refer to the given inner product on $H$. This only makes sense when the inner product is clear from context; otherwise we have to identity the inner product explicitly.

**Definition 3.2.2.** *A basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ for an inner product space $H$ is an* ***orthonormal basis*** *if $\langle v_i, v_j \rangle = \delta_{ij}$ for all $i = 1, \ldots, n$, where $\delta_{ij}$ is the Kronecker delta.*

The reason we're interested in orthonormal bases is the following fundamental identity:

**Lemma 3.2.3.** *Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be an orthonormal basis for an inner product space $H$. Then*

$$x = \sum_{i=1}^{n} \langle v_i, x \rangle v_i \text{ for all } x \in H.$$

*In other words, $[x]_{\mathcal{B}}$ is the vector $a \in \mathbb{F}^n$ with $a_i = \langle v_i, x \rangle$.*

*Proof.* Since $\mathcal{B}$ is a basis, $x = \sum a_i v_i$ for $a = [x]_{\mathcal{B}}$. So

$$\langle v_i, x \rangle = \langle v_i, \sum_{j=1}^{n} a_j v_j \rangle = \sum_{j=1}^{n} a_j \langle v_i, v_j \rangle = a_i.$$

□

The orthogonality condition in the definition of orthonormal basis can actually be useful in checking that a set of vectors is a basis:

**Lemma 3.2.4.** *Let $H$ be an inner product space. If $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a set of vectors in $H$ such that $\langle v_i, v_j \rangle = \delta_{ij}$ for all $i, j = 1, \ldots, n$, then $\{v_1, \ldots, v_n\}$ is linearly independent. In particular, if $\dim V = n$, then $\mathcal{B}$ is an orthonormal basis.*

Finally, every inner product has an orthonormal basis:

**Lemma 3.2.5.** *If $H$ is an inner product space, then $H$ has an orthonormal basis, and we can always find an orthonormal basis by applying the Gram-Schmidt algorithm to a given basis.*

For the proofs of Lemmas 3.2.4 and 3.2.5, we refer to a linear algebra course (note that the proofs for for $\mathbb{F} = \mathbb{R}$ and $\mathbb{F} = \mathbb{C}$ are exactly the same).

Orthonormal bases can also be characterized in terms of the matrix of the inner product:

**Proposition 3.2.6.** *Let $\mathcal{B}$ be a basis of an inner product space $H$. Then the following are equivalent:*

*(a) $\mathcal{B}$ is an orthonormal basis.*

*(b) The matrix of $\langle , \rangle_{\mathcal{H}}$ with respect to $\mathcal{B}$ is equal to $\mathbb{1}_n$, the $n \times n$ identity matrix.*

*(c) $\langle v, w \rangle_H = [v]_{\mathcal{B}}^*[w]_{\mathcal{B}}$ for all $v, w \in H$.*

*Proof.* The equivalence of parts (a) and (b) is an easy exercise. Parts (b) and (c) are equivalent by Lemma 3.1.9. □

Combining part (b) with Lemma 3.2.5 shows that for every inner product space, there is a basis $\mathcal{B}$ such that the basis of $\langle , \rangle$ with respect to $\mathcal{B}$ is the identity matrix. Also, part (c) of Proposition 3.2.6 provides another reason to work with orthonormal bases, as they simplify the calculation of the inner product. Finally, combining Proposition 3.2.6 with Theorem 3.1.11 leads to one of the easiest ways to define an inner product on a vector space $V$: pick a basis and declare it to be orthonormal.

**Corollary 3.2.7.** *For any basis $\mathcal{B}$ of a vector space $V$, there is a unique inner product $\langle , \rangle$ such that $\mathcal{B}$ is orthonormal.*

*Proof.* By Theorem 3.1.11 and Corollary 3.1.12, there is a unique sesquilinear form $\langle , \rangle$ on $V$ whose matrix with respect to $\mathcal{B}$ is the identity matrix. Since the standard inner product on $\mathbb{F}^n$ is positive definite, $\langle , \rangle$ will be positive definite on $V$. Finally, by Proposition 3.2.6, $\langle , \rangle$ is the unique inner product making $\mathcal{B}$ orthonormal (since this is the same as having the identity matrix as its matrix with respect to $\mathcal{B}$). □

We can use Corollary 3.2.7 to turn free vector spaces into free Hilbert spaces.

**Definition 3.2.8.** *The free Hilbert space $\mathbb{F}X$ is the Hilbert space we get from the free vector space $\mathbb{F}X$ by declaring the basis $\{|x\rangle : x \in X\}$ to be orthonormal.*

In the context of quantum information, it's quite common to write vectors as $|v\rangle$ rather than $v$, and write the inner product between $v$ and $w$ as $\langle v|w\rangle$.

If we use this notation in the free Hilbert space setting, we can say that the inner product is defined by setting $\langle x|y\rangle = \delta_{xy}$ for all $x, y \in X$. If

$$|v\rangle = \sum_{x \in X} c_x |x\rangle \text{ and } |w\rangle = \sum_{x \in X} d_x |x\rangle$$

then $\langle v|w\rangle = \sum_{x \in X} \overline{c_x} d_x$.

## 3.3 Normed spaces

**Definition 3.3.1.** *A **norm** on an $\mathbb{F}$-vector space $V$ is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ such that for all $v, w \in V$, $s \in \mathbb{F}$,*

*(1) $\|v + w\| \leq \|v\| + \|w\|$,*

*(2) $\|s \cdot v\| = |s|\|v\|$, and*

*(3) $\|v\| = 0$ if and only if $v = 0$.*

**Exercise 3.3.2.** *Let $V = \mathbb{C}^n$. Then*

$$\|v\|_1 := \sum_{i=1}^{n} |v_i| \text{ and } \|v\|_\infty := \max_{i=1,\ldots,n} |v_i|$$

*define norms on $V$, called the 1-norm and the $\infty$-norm respectively.*

**Definition 3.3.3.** *A **normed vector space** is a pair $(V, \|\cdot\|)$, where $V$ is a vector space and $\|\cdot\|$ is a norm on $V$.*

As with Hilbert spaces, we'll typically write $V$ for a normed space rather than writing out the pair $(V, \|\cdot\|)$, and as long as the norm is clear from context, we'll use $\|\cdot\|$ or $\|\cdot\|_V$ for the norm on $V$.

The reason we bring up normed spaces is that an inner product $\langle , \rangle$ can be turned into a norm $\|\cdot\|$ via the formula $\|x\| = \sqrt{\langle x, x, \rangle}$. That $\|\cdot\|$ is indeed a norm follows from the famous Cauchy-Schwarz inequality. Interestingly, this inequality actually holds for positive semidefinite forms, not just positive definite forms.

**Proposition 3.3.4** (Cauchy-Schwarz inequality)**.** *Let $\langle , \rangle$ be a positive semidefinite form on a vector space $V$, and define $\|v\| := \sqrt{\langle v, v\rangle}$. Then*

$$|\langle u, v\rangle| \leq \|u\|\|v\|.$$

Since $\langle , \rangle$ is only positive semidefinite, we can't rely on $\|v\|$ being nonzero, and hence some of the standard proofs won't work. However, one of the standard proofs does work.

*Proof.* We give the proof for $\mathbb{F} = \mathbb{C}$, which is the most complicated case. If one of $\|u\|$ or $\|v\|$ is non-zero, then we can use one of the standard proofs from a linear algebra course. So that just leaves the case $\|u\| = \|v\| = 0$, for which we want to show that $\langle u, v\rangle = 0$. To see this, observe that

$$0 \leq \langle u + v, u + v\rangle = 2\,\mathrm{Re}\langle u, v\rangle$$

(using the identity that $\alpha + \overline{\alpha} = 2\,\mathrm{Re}\,\alpha$) and

$$0 \leq \langle u - v, u - v\rangle = -2\,\mathrm{Re}\langle u, v\rangle,$$

so $\mathrm{Re}\langle u, v\rangle = 0$. For the imaginary part, we have that

$$0 \leq \langle u + iv, u + iv\rangle = -2\,\mathrm{Im}\langle u, v\rangle$$

(using the identity $i(\alpha - \overline{\alpha}) = -2\,\mathrm{Im}\,\alpha$) and

$$0 \leq \langle u - iv, u - iv\rangle = 2\,\mathrm{Im}\langle u, v\rangle,$$

so $\mathrm{Im}\langle u, v\rangle = 0$. □

**Exercise 3.3.5.** *Prove the Cauchy-Schwarz inequality, assuming that one of $\|v\|$ or $\|w\|$ is non-zero.*

**Corollary 3.3.6.** *If $\langle , \rangle$ is an inner product on a vector space $V$, then the function $\|v\| = \sqrt{\langle v, v\rangle}$ is a norm.*

*Proof.* That $\|v\| = 0$ if and only if $v = 0$ follows from positive definiteness of $\langle , \rangle$. That $\|sv\| = |s|\|v\|$ is obvious. That leaves the triangle inequality:

$$\begin{aligned}\|x+y\|^2 &= \langle x+y, x+y\rangle = \langle x,x\rangle + \langle y,x\rangle + \langle x,y\rangle + \langle y,y\rangle, \\ &= \|x\|^2 + \|y\|^2 + 2\operatorname{Re}\langle x,y\rangle \leq \|x\|^2 + \|y\|^2 + 2|\langle x,y\rangle| \\ &\leq \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| = (\|x\| + \|y\|)^2\end{aligned}$$

for all $x, y \in V$, where the last inequality follows from the Cauchy-Schwarz inequality. □

**Definition 3.3.7.** *An inner product space $H$ is regarded as a normed space with norm $\|x\| = \sqrt{\langle x, x\rangle}$.*

This means that we can use the notation $\|\cdot\|$ freely in an inner product space, as long as the underlying inner product is clear from context.

**Example 3.3.8.** *A **unit vector** in a Hilbert space is a vector $v$ with $\|v\| = 1$. If $v$ is a non-zero vector, then $\|v\| \neq 0$, and $v/\|v\|$ will be a unit vector.*

## 3.4 Isomorphisms

**Definition 3.4.1.** *Let $H_1, H_2$ be inner product spaces. A linear transformation $T : H_1 \to H_2$ is an isomorphism of inner product spaces if $T$ is an isomorphism of vector spaces (i.e. an invertible linear transformation) and*

$$\langle Tv, Tw\rangle_{H_2} = \langle v, w\rangle_{H_1} \tag{3.4.1}$$

*for all $v, w \in H_1$.*

Condition (3.4.1) is equivalent to saying that $\langle , \rangle_{H_1}$ is the pullback of $\langle , \rangle_{H_2}$ through $T$. Of course, this is equivalent to saying that $\langle , \rangle_{H_2}$ is the pullback of $\langle , \rangle_{H_1}$ through $T^{-1}$.

The matrix version of being an isomorphism of inner product spaces is being unitary:

**Definition 3.4.2.** *A matrix $U \in M_{nn}(\mathbb{F})$ is **unitary** if any of the following equivalent conditions hold:*

*(1)* $(Ux)^*(Uy) = x^*y$ *for all* $x, y \in \mathbb{F}^n$.

*(2)* $U^*U = \mathbb{1}$.

*(3)* $UU^* = \mathbb{1}$.

*(4) The columns of $U$ are an orthonormal basis of $\mathbb{F}^n$ with respect to the standard inner product.*

Note that unitary matrices $U$ are invertible, with $U^{-1} = U^*$. As with a lot of our other terminology, the term "unitary matrix" is normally reserved for matrices over $\mathbb{F} = \mathbb{C}$. When $\mathbb{F} = \mathbb{R}$, the equivalent term is **orthogonal matrix**. Once again, we use "unitary matrix" in both cases to save time.

It's not difficult to see that the conditions in Definition 3.4.2 are equivalent. For instance, to see that (1) implies (2), note that

$$(Ux)^*(Uy) = x^*U^*Uy,$$

and if $x^*U^*Uy = x^*y$ for all $x, y \in \mathbb{F}^n$, then taking $x = e_i$, $y = e_j$, implies that $(U^*U)_{ij} = e_i^* e_j = \delta_{ij}$, so $U^*U = \mathbb{1}$.

**Exercise 3.4.3.** *Finish the proof that conditions (1)-(4) in Definition 3.4.2 are equivalent.*

**Proposition 3.4.4.** *Let $\mathcal{B}_i$ be orthonormal bases for inner product spaces $\mathcal{H}_i$, $i = 1, 2$, and let $T : \mathcal{H}_1 \to \mathcal{H}_2$ be a linear transformation. Then the following are equivalent:*

*(a) $T$ is an isomorphism of inner product spaces.*

*(b) $[T]_{\mathcal{B}_2,\mathcal{B}_1}$ is unitary.*

*(c) $T(\mathcal{B}_1)$ is an orthonormal basis of $\mathcal{H}_2$.*

*Proof.* If (a) holds, then $T$ is an isomorphism, and in particular $[T]_{\mathcal{B}_2,\mathcal{B}_1}$ is a square matrix. Conversely, if $[T]_{\mathcal{B}_2,\mathcal{B}_1}$ is unitary, then it is invertible, and hence $T$ is an isomorphism. Because $\mathcal{B}_1$ and $\mathcal{B}_2$ are orthonormal, Proposition 3.2.6 implies that

$$\langle u, v\rangle_{H_1} = [u]_{\mathcal{B}_1}^*[v]_{\mathcal{B}_1} \text{ and}$$
$$\langle Tu, Tv\rangle = [Tu]_{\mathcal{B}_2}^*[Tv]_{\mathcal{B}_2} = ([T]_{\mathcal{B}_2,\mathcal{B}_1}[u]_{\mathcal{B}_1})^*([T]_{\mathcal{B}_2,\mathcal{B}_1}[v]_{\mathcal{B}_1})$$

for all $u, v \in \mathcal{H}_1$. Because the coordinate map is an isomorphism, we conclude that

$$\langle u, v\rangle_{H_1} = \langle Tu, Tv\rangle_{H_2} \text{ for all } u, v \in H_1$$

if and only if

$$x^*y = ([T]_{\mathcal{B}_2,\mathcal{B}_1}x)^*([T]_{\mathcal{B}_2,\mathcal{B}_1}y) \text{ for all } x, y \in \mathbb{F}^n.$$

Hence (a) and (b) are equivalent.

For condition (c), we show that (a) implies (c) and (c) implies (b). Let $\mathcal{B}_1 = \{v_1, \ldots, v_n\}$. If (a) holds then $T$ is an isomorphism of vector spaces, so by Proposition 2.1.19, $T(\mathcal{B}_1)$ is a basis for $\mathcal{H}_2$. To see that this basis is orthonormal, we use the identity

$$\langle T(v_i), T(v_j)\rangle_{H_2} = \langle v_i, v_j\rangle_{H_1} = \delta_{ij}.$$

So (c) holds.

Conversely, if (c) holds, let $\mathcal{B}' = T(\mathcal{B}_1) = \{T(v_1), \ldots, T(v_n)\}$. The $i$th column of $[T]_{\mathcal{B}',\mathcal{B}_1}$ is

$$[T]_{\mathcal{B}',\mathcal{B}_1} e_i = [T]_{\mathcal{B}',\mathcal{B}_1}[v_i]_{\mathcal{B}_1} = [T(v_i)]_{\mathcal{B}'} = e_i,$$

so $[T]_{\mathcal{B}',\mathcal{B}_1}$ is the identity matrix. Since the identity matrix is unitary, and $\mathcal{B}'$ is an orthonormal basis for $H_2$, (b) holds. □

Recall that we can think of invertible matrices either as the coordinate matrices of isomorphisms, or as change of basis matrices. The same is true of unitary matrices: we can think of them either as the coordinate matrices of isomorphisms of inner product spaces, or as change of basis matrices between orthonormal bases:

**Exercise 3.4.5.** *Let $\mathcal{B}$ be an orthonormal basis of an inner product space $H$ of dimension $n$.*

*(a) Show that if $\mathcal{R}$ is another basis for $H$, then $\mathcal{R}$ is orthonormal if and only if $[\mathbb{1}]_{\mathcal{B},\mathcal{R}}$ is unitary.*

*(b) Show that if $U$ is a unitary $n \times n$ matrix, then there is a basis $\mathcal{R}$ such that $U = [\mathbb{1}]_{\mathcal{B},\mathcal{R}}$.*

## 3.5 Dual spaces and Dirac notation

Recall from the previous chapter that if $V$ is a vector space with basis $\{v_1, \ldots, v_n\}$, we get an isomorphism $V \to V^*$ mapping $v_i \mapsto v^i$, where $\{v^1, \ldots, v^n\}$ is the dual basis. This isomorphism depends on the choice of basis.

For inner product spaces $H$, there is another way to map $H \to H^*$. The only caveat is that this mapping is antilinear rather than linear.

**Definition 3.5.1.** *Let $V$ and $W$ be $\mathbb{F}$-vector spaces. A function $T : V \to W$ is* ***antilinear*** *if $T(sv + w) = \overline{s}T(v) + T(w)$ for all $s \in \mathbb{F}$, $v, w \in V$.*

*An* ***antilinear isomorphism*** *is an antilinear map which is a bijection.*

If $\mathbb{F} = \mathbb{R}$, then antilinear and linear maps are the same. For $\mathbb{F} = \mathbb{C}$, if we're willing to change the spaces involved a bit, then an antilinear map can be regarded as a linear map:

**Exercise 3.5.2.** *(a) Given a $\mathbb{C}$-vector space $(V, +, \cdot)$, define a new scalar multiplication $\circ$ on $V$ by*

$$c \circ v = \overline{c} \cdot v,$$

*where $\cdot$ is the scalar multiplication operation from $V$. Let $\overline{V} = (V, +, \circ)$. Show that $\overline{V}$ is a vector space.*

*(b) Show that a function $T : V \to W$ is antilinear if and only if $T$ is linear when considered as a function from $\overline{V} \to W$.*

*(c) Show that an antilinear function $T : V \to W$ is an isomorphism if and only if for every (resp. some) basis $\mathcal{B}$ of $V$, $T(\mathcal{B})$ is a basis of $W$.*

This means that the theory of antilinear maps is essentially the same as the theory of linear maps.

**Theorem 3.5.3.** *Let $H$ be an inner product space, and for $v \in H$, define*

$$f_v : H \to \mathbb{F} : w \mapsto \langle v, w \rangle.$$

*Then*

*(1) $f_v$ is linear, and hence belongs to $H^*$.*

*(2) The function*

$$H \to H^* : v \mapsto f_v$$

*is an antilinear isomorphism.*

*(3) If $\mathcal{B}$ is an orthonormal basis for $H$, then $[f_v]_{\mathcal{B}} = [v]^*_{\mathcal{B}} \in M_{1n}\mathbb{F}$.*

Before starting the proof, note that the map $v \mapsto f_v$ is antilinear because (by the definition of sesquilinearity) $\langle , \rangle$ is antilinear in its first argument. If we try to switch the formula around and set $f_v(w) = \langle w, v \rangle$, then the map $v \mapsto f_v$ would be linear, but $f_v$ itself would be antilinear, and hence wouldn't be an element of $H^*$.

*Proof of Theorem 3.5.3.* (1) is obvious from the definition of sesquilinearity. For (3), observe that if $w \in H$, then

$$[v]^*_{\mathcal{B}}[w]_{\mathcal{B}} = \langle v, w \rangle = [f_v(w)]_{\{1\}}.$$

So $[v]^*_{\mathcal{B}}$ satisfies the defining equation for $[f_v]_{\mathcal{B}} = [f_v]_{\{1\},\mathcal{B}}$, proving (3).

Now we can use (3) to prove (2). Let $c_{\mathcal{B}} : H \to \mathbb{F}^n : w \mapsto [w]_{\mathcal{B}}$ and $\hat{c}_{\mathcal{B}} : H^* \to M_{1n}\mathbb{F} : f \mapsto [f]_{\mathcal{B}}$ be the coordinate isomorphisms. It should be clear that the map $\phi : \mathbb{F}^n \to M_{1n} : x \mapsto x^*$ is an antilinear isomorphism. By (3),

$$f_v = \hat{c}_{\mathcal{B}}^{-1}([v]^*_{\mathcal{B}}) = \hat{c}_{\mathcal{B}}^{-1}(\phi([v]_{\mathcal{B}})) = \hat{c}_{\mathcal{B}}^{-1}\phi(c_{\mathcal{B}}(v)),$$

so the map sending $v \mapsto f_v$ is $\hat{c}_{\mathcal{B}}^{-1} \circ \phi \circ c_{\mathcal{B}}$. To finish the proof, we can use the following exercise:

**Exercise 3.5.4.** *Let $V_1, V_2, V_3, V_4$ be vector spaces, and suppose $S_1 : V_1 \to V_2$ and $S_2 : V_3 \to V_4$ are linear isomorphisms, and $T : V_2 \to V_3$ is an antilinear isomorphism. Show that $S_2 \circ T \circ S_1$ is an antilinear isomorphism.*

□

**Example 3.5.5.** *Let $H = \mathbb{F}^n$ with the standard inner product, so the standard basis $\mathcal{B}$ is an orthonormal basis. Identity $H^*$ with $M_{1n}\mathbb{F}$ using the standard basis. By the theorem, the map $H \to H^* : v \mapsto f_v$ just sends $v \mapsto v^*$, since $[v]_{\mathcal{B}} = v$.*

Let $H$ be an inner product space. Given a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ for $H$, we now have two ways of writing down a basis for $H^*$. We can take the Kronecker dual basis $\{v^1, \dots, v^n\}$, which is the unique basis with $v^i(v_j) = \delta_{ij}$. Or we can use the fact that, just like linear isomorphisms, antilinear isomorphisms send bases to bases, and take $\{f_{v_1}, \dots, f_{v_n}\}$, where $f_v$ is defined as in Theorem 3.5.3. When is the Kronecker dual basis equal to the basis we get from the inner product? Well, every element of $H^*$ is determined by its values on the basis $\mathcal{B}$, so $f_{v_i} = v^i$ if and only if $f_{v_i}(v_j) = v^i(v_j) = \delta_{ij}$ for all $1 \leq j \leq n$. Since $f_{v_i}(v_j) = \langle v_i, v_j \rangle$, we get:

**Lemma 3.5.6.** *The Kronecker dual basis $\{v^1, \dots, v^n\}$ is equal to the basis $\{f_{v_1}, \dots, f_{v_n}\}$ if and only if $\mathcal{B}$ is orthonormal.*

This means that when $\mathcal{B} = \{v_1, \dots, v_n\}$ is orthonormal, the antilinear isomorphism $H \to H^* : v \mapsto f_v$ sends $v_i \mapsto v^i$, just like the linear isomorphism $H \to H^*$ we previously studied. In fact, if $\mathbb{F} = \mathbb{R}$ then these are the same map. However, when $\mathbb{F} = \mathbb{C}$ there is an important difference: by making the map antilinear, we get a mapping $H \to H^*$ that depends only on the choice of inner product, not on the specific orthonormal bases we choose.

**Exercise 3.5.7.** *Let $\{e_1, e_2\}$ be the standard basis for $H = \mathbb{C}^2$, and let $\{e^1, e^2\}$ be the dual basis. Find an orthonormal basis $\{f_1, f_2\}$ for $\mathbb{C}^2$ (in the standard* *inner product), such that the linear transformation $H \to H^* : f_i \mapsto f^i$ does not send $e_1 \mapsto e^1$ (and hence is different from the linear transformation $H \to H^* : e_i \mapsto e^i$).*

*In contrast, show for your example that the two antilinear maps $H \to H^*$ sending $e_i \mapsto e^i$ and $f_i \mapsto f^i$ are the same.*

We can also use the antilinear isomorphism $v \mapsto f_v$ to define an inner product on $H^*$:

**Exercise 3.5.8.** *Let $H$ be an inner space, and for $v \in H$, let $f_v : H \to H : w \mapsto \langle v, w \rangle$.*

*(a) Show that $\langle f_v, f_w \rangle := \langle w, v \rangle$ defines an inner product on the dual space $H^*$.*

*(b) Suppose $\mathcal{B}$ is a basis for $H$, and let $\mathcal{B}'$ be the basis $\{f_v : v \in \mathcal{B}\}$ for $H^*$. Show that $\mathcal{B}'$ is orthonormal for the inner product defined in part (a) if and only if $\mathcal{B}$ is orthonormal in $H$.*

If $T$ is the map $H \to H^* : v \mapsto f_v$, then the inner product in part (a) of Exercise 3.5.8 can be rewritten as $\langle f, g \rangle = \langle T^{-1}(g), T^{-1}(f) \rangle$ for $f, g \in H^*$. So this inner product on $H^*$ is like the pullback along the isomorphism $T^{-1} : H^* \to H$, except that we have to to use $\langle T^{-1}(g), T^{-1}(f) \rangle$ instead of $\langle T^{-1}(f), T^{-1}(g) \rangle$ to account for the fact that $T$ is antilinear instead of linear. Part (b) shows that this inner product is also the unique inner product we get by declaring $\{f_v : v \in \mathcal{B}\}$ to be an orthonormal basis for $H^*$, where $\mathcal{B}$ is an orthonormal basis for $H$. In particular, if we define the inner product on $H^*$ by choosing an orthonormal basis for $H$ like this, then the inner product we get doesn't depend on the choice of basis.

We haven't properly explained Dirac notation yet. So far, we've used the symbols $|x\rangle$ to distinguish the elements of $X$ from the basis vectors corresponding to the elements of $X$ in the free vector space $\mathbb{F}X$. As mentioned above, in a Hilbert space $H$ we often write vectors as $|v\rangle$ rather than $v$, and the inner product as $\langle v|w \rangle$. With this notation, we can write the linear function $f_v : H \to \mathbb{F} : w \mapsto \langle v, w \rangle$ as $|w\rangle \mapsto \langle v|w \rangle$.

**Definition 3.5.9.** *Let $|v\rangle \in H^*$. Then the function $|w\rangle \mapsto \langle v|w \rangle$ is denoted by $\langle v|$. The symbol $|v\rangle$ is called a **ket**, the symbol $\langle v|$ is called a **bra**, and the inner product $\langle v|w \rangle$ is called the **bra-ket**, or bracket, of $v$ and $w$.*

In Dirac notation, the function $v \mapsto f_v$ in Theorem 3.5.3 simply sends $|w\rangle$ to $\langle w|$. It's quite handy to have this notation, as the other notation we use here, $f_v$, isn't exactly standard, meaning we have to define $f_v$ every time we want to use it. It's important to remember though that the map $|v\rangle \mapsto \langle v|$ is antilinear, rather than linear:

**Example 3.5.10.** *If* $|\psi\rangle = |0\rangle + i\,|1\rangle \in \mathbb{C}\{0,1\}$, *then* $\langle\psi| = \langle 0| - i\,\langle 1|$.

In Dirac notation, the inner product on $H^*$ is $\langle \langle v|\,, \langle w| \rangle = \langle w|v\rangle$.

# Chapter 4

# Quantum registers

## 4.1 States and measurement in a basis

In the previous chapter, we introduced our first axiom of quantum probability: physical systems correspond to Hilbert spaces. In this chapter, we'll add two more axioms that will help us use this first axiom. The first tells us how to describe the state of a physical system.

**Axiom 2.** *The state of a physical system corresponding to Hilbert space $H$ is given by a unit vector $v \in H$.*

As mentioned previously, we often denote this vector using Dirac notation as $|v\rangle$. We will use the term **state** as synonymous with unit vector. The set of states on a Hilbert space $H$ will be denoted by $S(H)$.

Note that we make a distinction between system and state. For example, we might think of a collection of air molecules as a physical system. The state of the system would be the position and velocity of each molecule. Note that the state changes in time, while the system remains unchanged. Another example is a computer. The computer hardware is the physical system, and the contents of memory is the state of the computer. We often keep this example in mind when thinking about physical systems from an information theory point of view.

The second axiom has to do with measurement. We'll think of measurement as an abstract physical process that returns some outcome. It's helpful to picture a measurement as a black box with a screen and a red button. When we press the button, the measurement is performed and the result appears on the screen. We don't necessarily know what result will appear, but what can appear will depend on how we design the box—if we designed the screen to show a number, we won't see a letter. Hence there is some set of possible outcomes $\mathcal{O}$ which we know in advance. The results of the measurement will depend on the state of the system. When we prepare a system in a state $v$, we might find that the outcome of the measurement is not always the same, and thus the best description we can give of the measurement outcomes is probabilistic. Thus for any state $v$, the measurement gives a probability distribution $p_v$ on $\mathcal{O}$. As in Chapter 1, assuming that $\mathcal{O}$ is finite, this is just a function $p_v : \mathcal{O} \to \mathbb{R}_{\geq 0}$ such that $\sum_{x \in \mathcal{O}} p_v(x) = 1$. Finally, as we saw in Chapter 1, measurement could affect the state of the system. To summarize, a **measurement process** on a Hilbert space $H$ is described by:

(1) a set of possible outcomes $\mathcal{O}$,

(2) a function $S(H) \to \mathrm{Prob}(\mathcal{O}) : v \mapsto p_v$ from states $S(H)$ to probability distributions $\mathrm{Prob}(\mathcal{O})$ over $\mathcal{O}$, and

(3) a way of saying what the new state of the system, given the starting state $v$ of the system and the outcome $x \in \mathcal{O}$ of the measurement.

Quantum mechanics is very specific about what measurement processes are allowed. Later we'll look at more general types of measurements, but for now, we'll look at one specific type of measurement allowed by quantum mechanics.

**Axiom 3** (Measurement in a basis)**.** *Let $H$ be the Hilbert space of a physical system, and let $\mathcal{B}$ be an orthonormal basis. There is a measurement associated to $\mathcal{B}$, in which*

- *the possible outcomes of the measurement are the elements of $\mathcal{B}$;*

- *(**Born rule**) the probability of getting outcome $x \in \mathcal{B}$ when the system is in state $v \in H$ is $|\langle x, v\rangle|^2$ ; and*

- *(**wave function collapse**) if the outcome of the measurement is $x$, then after measurement the system will be in state*

$$\frac{\langle x, v\rangle}{|\langle x, v\rangle|} x.$$

*This measurement is called **measurement with respect to $\mathcal{B}$**.*

Let's prove that the Born rule gives us a probability distribution on $\mathcal{B}$:

**Lemma 4.1.1.** *Let $v$ be a state in a Hilbert space $H$, and let $\mathcal{B}$ be an orthonormal basis. Then*

$$\sum_{x \in \mathcal{B}} |\langle x, v\rangle|^2 = 1.$$

*Proof.* Since $v$ is a unit vector and $\mathcal{B}$ is orthonormal,

$$\sum_{x\in\mathcal{B}} |\langle x, v\rangle|^2 = \|[v]_{\mathcal{B}}\|^2 = \|v\|^2 = 1.$$

□

We also need to check that the output of measurement is a unit vector. This follows because $\frac{\langle x,v\rangle}{|\langle x,v\rangle|}$ is a complex number of norm 1. Of course, this number is only well-defined when $|\langle x, v\rangle| \neq 0$, but if $|\langle x, v\rangle| = 0$, then the probability of measuring outcome $x$ is $|\langle x, v\rangle|^2 = 0$, so we don't worry about what the resulting state is in this case.

## 4.2 Quantum registers

The axioms we'll introduce in this course don't refer to any specific physical system, and how to apply the axioms to specific physical systems is beyond the scope of this course. However, to understand what the axioms mean, it's helpful to have a physical system in mind. Instead of using any specific physical system for this, we'll take inspiration from information science, and use an idealized physical system called a quantum register.

In information science, a "classical" (as opposed to "quantum") register is a physical system that can be used to store and manipulate classical information. A register holds an element of some predetermined set $\mathcal{X}$. The most common examples are **bit registers**, for which $\mathcal{X} = \{0, 1\}$, and **$n$-bit registers**, for which $\mathcal{X} = \{0, 1\}^n$. For an abstract register, $\mathcal{X}$ could be any finite set. With classical registers, we can perform two operations: read from the register, and write a string from $\mathcal{X}$ to the register. Note that with classical registers, we also make a distinction between physical system, and state: the physical system is described by the set of values $\mathcal{X}$ that the register can take, along with the allowed operations on the register, while the state of the register is the current value the register holds. at any given point in time. Classical registers are the basis of most abstract and practical models of computation. Most laptop and desktop computers have CPUs with 64-bit registers, while your phone might use a CPU with 32-bit or 64-bit registers.

A **quantum register** is a physical system for storing and manipulating quantum information. To see how this works, let's consider the analogue of bit registers. These are called **qubit registers**.

**Definition 4.2.1.** *A **qubit register** is the free Hilbert space $\mathbb{C}\{0, 1\}$, and an $n$-**qubit register** is the free Hilbert space $\mathbb{C}\{0, 1\}^n$.*

In general, the free vector space $\mathbb{C}\mathcal{X}$ can be regarded as a quantum version of a classical register which can hold values from the set $\mathcal{X}$.

Importantly, we can't read values freely from a quantum register, we can only measure the register. The basis

$$\{|x\rangle, x \in X\}$$

is called the **computational basis** of $\mathbb{C}\mathcal{X}$. Measuring the register $\mathbb{C}X$ in the computational basis gives an outcome from $X$, just like a classical register, and correspondingly we write the outcome as an element of $X$, dropping the Dirac notation.

Let's see what happens when we measure a qubit register in the computational basis $\mathcal{B} = \{|0\rangle, |1\rangle\}$. If the register is in state $|0\rangle$, then we get outcome 0 with probability $|\langle 0|0\rangle|^2 = 1$, and outcome 1 with probability $|\langle 1|0\rangle|^2 = 0$. So we just say that measuring $|0\rangle$ in the computational basis gives outcome 0, and leaves the system in state $|0\rangle$. Similarly, measuring $|1\rangle$ in the computational basis gives outcome 1, and leaves the system in state $|1\rangle$. In this sense, a quantum register behaves just like a classical register, and this is an important fact: a quantum register can hold classical information.

On the other hand, a quantum register can also be in states like

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ and } \frac{i}{\sqrt{50}}|0\rangle + \frac{7}{\sqrt{50}}|1\rangle.$$

States like this are said to be in a **superposition** of $|0\rangle$ and $|1\rangle$. If we measure $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ in the computational basis, we get outcome 0 with probability

$$|\langle 0|\psi\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2},$$

If we measure outcome 0, then the state of the system after measurement will be $|0\rangle$, and similarly if the outcome is 1, then the state will be $|1\rangle$. This aspect of measurement is called **collapse**. It guarantees that if we repeat a measurement in the same basis, we will get the same outcome. So if we measure $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and get outcome 0, then another measurement will also give outcome 0.

**Notation 4.2.2.** *To save time, we often write states like*

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \textit{ and } \frac{i}{\sqrt{50}}|0\rangle + \frac{7}{\sqrt{50}}|1\rangle.$$

*as*

$$|0\rangle + |1\rangle \textit{ and } i|0\rangle + 7|1\rangle.$$

*respectively. In general, when referring to a non-unit vector $v$ as a state, we mean the state $\frac{v}{\|v\|}$.*

A 3-qubit register can be in states like

$$|000\rangle\,, |010\rangle\,,\ \text{and}\ \frac{1}{\sqrt{3}}\,|100\rangle + \frac{1}{\sqrt{3}}\,|010\rangle + \frac{1}{\sqrt{3}}\,|001\rangle\,.$$

The last state could also be denoted by $|000\rangle + |010\rangle + |001\rangle$. If we measure this last state in the computational basis we get outcomes 100, 010, and 001 with probability 1/3 each, and every other string with probability 0. If we happened to get outcome 010, then we'd know that the state of the system at that point is $|010\rangle$.

Superposition can be a counterintuitive property. **Schrodinger's cat** is a thought experiment designed to illustrate the counterintuitive aspects of entanglement. In the thought experiment, we imagine a cat in a box. When we open the box, the cat is either dead or alive, so from a classical point of view, the state of the cat is either

$$|\text{Alive}\rangle\ \text{ or }\ |\text{Dead}\rangle\,.$$

But suppose we can put the system in the superposed state $|\text{Alive}\rangle + |\text{Dead}\rangle$? (Schrodinger proposed a specific mechanism, whereby the state of the cat would be coupled with the state of a radioactive atom. The rules of quantum mechanics would then describe the state of the cat using a state in superposition). Is the cat dead or alive? While this thought experiment is helpful in thinking about interpretations of quantum mechanics, as long as we measure in the computational basis, we haven't really added anything to classical probability theory at this point. The superposition $|0\rangle + |1\rangle$ is just a complicated way of referring to the uniform probability distribution on $\{0, 1\}$.

However, superposition starts to be interesting when we consider that we can measure in different bases. For qubit registers, an important orthonormal basis is the **plus-minus basis** (or **Hadamard basis**) $\{|+\rangle\,, |-\rangle\}$, where

$$|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\ \text{ and }\ |-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\,.$$

(Note that we've started using Dirac notation for arbitrary vectors.)

**Exercise 4.2.3.** *Show that if we start with a qubit register in state $|+\rangle$, then measurement in the computational basis and measurement in the Hadamard basis behave like the measurements $X$ and $Z$ in the measurement scenario from*

*Chapter 1. In particular, we measure in the Hadamard basis and then in the computational basis, we get outcome* $+$*, and then a 50/50 split between* 0 *and* 1*. If we measure in the computational basis first, and then in the Hadamard basis, we first get* 0 *or* 1 *with equal probability, and then we get* $+$ *or* $-$ *with equal probability.*

Thinking about free vector spaces as analogues of classical registers is very appealing, but we can really think of any Hilbert space as a quantum register, with the contents of the register given by a state (i.e. unit vector) in the Hilbert space. Consequently, we'll often use the terms "quantum register" and "finite-dimensional Hilbert space" interchangeably.

## 4.3 Distinguishing different states

When can we distinguish two different states? For classical registers, this is easy: we just read out the state of the register and compare. But for quantum registers, we can only make measurements. By measuring in the computational basis, we can distinguish between $|0\rangle$ and $|1\rangle$. But what about distinguishing between $|0\rangle$ and $\sqrt{1-\epsilon^2}\,|0\rangle + \epsilon\,|1\rangle$ as $\epsilon \to 0$? Should that be possible? To answer that question, let's formally define what it means to distinguish between two states:

**Definition 4.3.1.** *Let $H$ be a Hilbert space, and let $|\psi\rangle$, $|\phi\rangle$ be states in $H$. A measurement process on a Hilbert space $H$ with outcome set $\mathcal{O}$* ***perfectly distinguishes between*** $|\psi\rangle$ ***and*** $|\phi\rangle$ *if $\mathcal{O}$ is the disjoint union of two subsets $\mathcal{O}_1$ and $\mathcal{O}_2$, such that when the system is in state $|\psi\rangle$, then then the measurement process always returns an outcome in $\mathcal{O}_1$, and if the system is in state $|\phi\rangle$, the process always returns an outcome in $\mathcal{O}_2$.*

So what pairs of states can we distinguish with measurement in a basis? The answer turns out to be very intuitive, and is fun to prove on your own:

**Exercise 4.3.2.** *Let $|\psi\rangle$ and $|\phi\rangle$ be states in a Hilbert space $H$. Show that there is an orthonormal basis $\mathcal{B}$ such that measurement with respect to $\mathcal{B}$ distinguishes between $|\psi\rangle$ and $|\phi\rangle$ if and only if $\langle\psi|\phi\rangle = 0$.*

This means that we can perfectly distinguish between $|0\rangle$ and $|1\rangle$, or $|+\rangle$ and $|-\rangle$, but not between $|0\rangle$ and $|+\rangle$ or $|-\rangle$.

So far we've used the inner product that comes with a Hilbert space to define the measurement probabilities in measurement with a basis. Exercise 4.3.2 suggests it might also have something to do with distance between states.

Of course, we already have a notion of distance between two states $|\psi\rangle$ and $|\phi\rangle$: we can take the norm of the difference

$$\| \, |\psi\rangle - |\phi\rangle \, \|.$$

However, since we can't observe states directly, it's not clear how we'd calculate this distance if faced with two unknown states in the physical world. So instead, we can use the inner product to define a notion of distance between states:

**Definition 4.3.3.** *Let $|\psi\rangle$ and $|\phi\rangle$ be two states in a Hilbert space $H$. The* ***fidelity*** *between $|\psi\rangle$ and $|\phi\rangle$ is*

$$F(|\psi\rangle, |\phi\rangle) = |\, \langle\psi|\phi\rangle \,|^2.$$

If $|\phi\rangle$ is the state of the system $H$, then $F(|\psi\rangle, |\phi\rangle)$ is the probability of getting outcome $|\psi\rangle$ when measuring in any orthonormal basis $\mathcal{B}$ containing $|\psi\rangle$. (And since $F(|\psi\rangle, |\phi\rangle) = F(|\phi\rangle, |\psi\rangle)$, it's also the probability of getting outcome $|\phi\rangle$ when the system is in state $|\psi\rangle$.) In particular, $0 \leq F(|\psi\rangle, |\phi\rangle) \leq 1$. If the fidelity is high (close to 1), then $|\psi\rangle$ is a very likely outcome when doing such a measurement, so we think of the two states as being close together. If the fidelity is low (close to 0), then it's unlikely that we'd get $|\psi\rangle$, and we think of the two states as being far apart.

Looking at fidelity, it seems like there might be some hope for the norm distance, since we can relate it to fidelity with the following inequality:

**Lemma 4.3.4.**

$$\| \, |\psi\rangle - |\phi\rangle \, \| \geq \sqrt{2 - 2\sqrt{F(|\psi\rangle, |\phi\rangle)}}.$$

*Proof.*

$$\| \, |\psi\rangle - |\phi\rangle \, \|^2 = 2 - \langle\psi|\phi\rangle - \langle\psi|\phi\rangle = 2 - 2\,\mathrm{Re}\,\langle\psi|\phi\rangle \geq 2(1 - \sqrt{F(|\psi\rangle, |\phi\rangle)}),$$

where the last inequality comes from the fact that $\mathrm{Re}\,\langle\psi|\phi\rangle \leq |\,\langle\phi|\psi\rangle\,|$. □

This inequality implies states which are close in norm distance must have fidelity close to 1. However, there still seems to be some problems with states that are far apart. By the triangle inequality, the maximum distance between any two states is 2, and this maximum distance is attained by pairs $|\psi\rangle$, $-|\psi\rangle$. However, $F(|\psi\rangle, -|\psi\rangle) = 1$, so these states are supposed to be close together. Indeed, we'll see later in Chapter 6 that states which differ by scalar multiples are indistinguishable in quantum probability. So while the norm is not totally useless, it's not a great way to measure distance between states.

# Chapter 5

# Unitary evolution

## 5.1 Unitary evolution

Quantum mechanics contains rules for how the state of a system can change, or **evolve**, over time. In the last chapter, we saw how the state of a system can change as part of measurement with respect to a basis. In this chapter, we are going to look at the evolution rule for **closed quantum systems**. A closed physical system is one that doesn't interact with anything outside it. Our universe is a closed physical system, essentially by definition. The types of systems we study in a lab experiment are never closed, but if the lab conditions are arranged to minimize the effects of things outside the lab, then the lab is approximated by a closed system.

Suppose we allow a closed physical system with Hilbert space $H$ to evolve from time $t_1$ to time $t_2$. Since nothing outside the system affects the system, the state of the system at time $t_2$ should depend only on the state of the system at time $t_1$ (we could actually use this as a definition of a closed system if we wanted to). So there is a function $E : S(H) \to S(H)$, where $S(H)$ is the set of states in $H$, such that if the system is in state $|\psi\rangle$ at time $t_1$, then the system is in state $E(|\psi\rangle)$ at time $t_2$. The function $E$ is called the **time evolution operator**.

Note that measurement is not an example of evolution in a closed system. Although a measurement process tells us how the state changes, the state of the system after measurement is not determined by the state of the system before measurement; instead, it depends on the outcome of measurement. With a measurement, the measurement outcome we get is a type of interaction with another physical system, so when we measure we break the "closed" property of the system.

Quantum mechanics tells us what time evolution operators are possible.

**Axiom 4.** *Time evolution is linear: if $E : S(H) \to S(H)$ is a time evolution operator, then there is a linear transformation $T : H \to H$ such that $E = T|_{S(H)}$.*

Usually we just think of the time evolution operator $E$ as a linear function $H \to H$. The linearity of time evolution means that time evolution in quantum mechanics preserves superpositions. For instance, if $E$ is a time evolution operator on $H = \mathbb{C}\{0,1\}$, then

$$E(a\,|0\rangle + b\,|1\rangle) = aE(|0\rangle) + bE(|1\rangle).$$

Not every linear function $E : H \to H$ can be a time evolution operator: a time evolution operator has to satisfy $E(x) \in S(H)$ for all $x \in S(H)$.

**Definition 5.1.1.** *A linear map $T : H_1 \to H_2$ is an* ***isometry*** *if $\|T(x)\| = \|x\|$ for all $x \in H_1$. We also say that such a $T$ is a* ***linear isometry****.*

A time evolution operator is a linear isometry.

**Lemma 5.1.2.** *A linear function $T : H_1 \to H_2$ is an isometry if and only if $\|T(x)\| = 1$ for all $x \in H_1$ with $\|x\| = 1$.*

*Proof.* If $T$ is an isometry, then clearly $\|T(x)\| = \|x\| = 1$ for all $x \in H_1$ with $\|x\| = 1$.

Suppose conversely that $\|T(x)\| = 1$ for all $x \in H_1$ with $\|x\| = 1$, and let $x \in H_1$ be a general vector. If $x = 0$, then $\|T(x)\| = 0 = \|x\|$. If $x \neq 0$, then

$$\|T(x)\| = \|T\left(\frac{\|x\|x}{\|x\|}\right)\| = \|x\|\|T\left(\frac{x}{\|x\|}\right)\| = \|x\|\|\frac{x}{\|x\|}\| = \|x\|,$$

so $T$ is an isometry. □

We can go further using the **polarization identity**:

**Lemma 5.1.3.** *If $H$ is a Hilbert space, then*

$$2\,\mathrm{Re}\langle x, y\rangle = \|x+y\|^2 - \|x\|^2 - \|y\|^2.$$

*Proof.*

$$\begin{aligned} \|x+y\|^2 - \|x\|^2 - \|y\|^2 &= \langle x+y, x+y\rangle - \langle x, x\rangle - \langle y, y\rangle \\ &= \langle x, y\rangle + \langle y, x\rangle = \langle x, y\rangle + \overline{\langle x, y\rangle} = 2\,\mathrm{Re}\langle x, y\rangle. \end{aligned}$$

□

**Proposition 5.1.4.** *A linear function $T : H_1 \to H_2$ between Hilbert spaces $H_1, H_2$ is an isometry if and only if*

$$\langle T(x), T(y)\rangle = \langle x, y\rangle$$

*for all $x, y \in H_1$.*

*Proof.* If $\langle T(x), T(y)\rangle = \langle x, y\rangle$ for all $x, y \in H_1$, then $\|T(x)\| = \|x\|$ for all $x \in H$, so $T$ is an isometry.

If $T$ is an isometry, then

$$\begin{aligned}\operatorname{Re}\langle T(x), T(y)\rangle &= \frac{1}{2}\left[\|T(x)+T(y)\|^2 - \|T(x)\|^2 - \|T(y)\|^2\right]\\ &= \frac{1}{2}\left[\|x+y\|^2 - \|x\|^2 - \|y\|^2\right] = \operatorname{Re}\langle x, y\rangle\end{aligned}$$

for all $x, y \in H_1$. But this means that

$$\begin{aligned}\operatorname{Im}\langle T(x), T(y)\rangle &= -\operatorname{Re} i\langle T(x), T(y)\rangle = -\operatorname{Re}\langle T(x), T(iy)\rangle\\ &= -\operatorname{Re}\langle x, iy\rangle = -\operatorname{Re} i\langle x, y\rangle = \operatorname{Im}\langle x, y\rangle\end{aligned}$$

for all $x, y \in H_1$, so $\langle T(x), T(y)\rangle = \langle x, y\rangle$ for all $x, y \in H_1$. □

The condition in Proposition 5.1.4 previously came up in the definition of isomorphisms of Hilbert spaces. However, isomorphisms of Hilbert spaces were also required to be invertible.

**Exercise 5.1.5.** *Give an example of an isometry $H_1 \to H_2$ which is not invertible.*

However, invertibility holds automatically if $H_1 = H_2$.

**Corollary 5.1.6.** *$T : H \to H$ is an isometry if and only if $T$ is an isomorphism of Hilbert spaces.*

*Proof.* It's clear that isomorphism of Hilbert spaces are isometries. Suppose that $T : H \to H$ is an isometry, and let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be an orthonormal basis for $H$. By Proposition 5.1.4, $\langle Tv_i, Tv_j\rangle = \langle v_i, v_j\rangle = \delta_{ij}$. By Lemma 3.2.4, $\{T(v_1), \ldots, T(v_n)\}$ is an orthonormal basis of $H$. By Proposition 3.4.4, $T$ is an isomorphism of Hilbert spaces. □

So a time evolution operator on a Hilbert space $H$ is an isomorphism of $H$ with itself.

**Definition 5.1.7.** *Let $H$ be a Hilbert space. An isomorphism of Hilbert spaces $H \to H$ is also known as a* ***unitary operator on*** *$H$.*

Let's state the consequence of Corollary 5.1.6 in this language:

**Corollary 5.1.8.** *A time evolution operator on a closed quantum system is unitary. In particular, a time evolution operator on a closed quantum system is invertible.*

Often Corollary 5.1.8 is taken as the axiom for evolution of a closed system. But as we've shown, unitary of time evolution follows from linearity (when combined with Axiom 2). Can we deduce linearity from any weaker axioms? After all, why should a time evolution operator preserve superpositions (which is essentially what Axiom 4 says). There are a lot of different ways to answer this. Here's one:

**Exercise 5.1.9.** *Let $T : H \to H$ be a function (not necessarily linear), such that*

$$\langle Tx, Ty \rangle = \langle x, y \rangle$$

*for all $x, y \in H$. Show that $T$ is linear.*

So we would get an equivalent theory if we replaced Axiom 4 with the axiom that every time evolution operator has to come from a function $T : H \to H$ such that $\langle Tx, Ty \rangle = \langle x, y \rangle$, as every such function has to be linear.

## 5.2 Adjoints

By Corollary 5.1.8, any time evolution operator $T : H \to H$ is invertible. We also know that if $\mathcal{B}$ is an orthonormal basis for $H$, then $[T]_{\mathcal{B},\mathcal{B}}$ is a unitary matrix, so by Exercise 2.1.21, the matrix of $T^{-1}$ with respect to $\mathcal{B}$ is $[T^{-1}]_{\mathcal{B},\mathcal{B}} = [T]^{-1}_{\mathcal{B},\mathcal{B}} = [T]^{*}_{\mathcal{B},\mathcal{B}}$. While this gives us an expression for the inverse of $T$, we can also write down the inverse of $T$ without picking a basis using the notion of the adjoint of a linear map:

**Lemma 5.2.1.** *If $T : H_1 \to H_2$ is a map between Hilbert spaces, then there is a unique linear map $T^* : H_2 \to H_1$, called the* ***adjoint****, such that $\langle Tx, y \rangle = \langle x, T^*y \rangle$ for all $x \in H_1$, $y \in H_2$.*

*If $T^*$ is the adjoint of $T$, and $\mathcal{B}_i$ is an an orthonormal basis of $H_i$, then*

$$[T^*]_{\mathcal{B}_1,\mathcal{B}_2} = [T]^{*}_{\mathcal{B}_2,\mathcal{B}_1}.$$

*Proof.* Let $\mathcal{B}_i$ be a basis for $H_i$, $i = 1, 2$. Suppose $S : H_2 \to H_1$ is a linear map. If $x \in H_1$, $y \in H_2$, then

$$\langle Tx, y\rangle = [Tx]^*_{\mathcal{B}_2}[y]_{\mathcal{B}_2} = ([T]_{\mathcal{B}_2,\mathcal{B}_1}[x]_{\mathcal{B}_1})^*\,[y]_{\mathcal{B}_2} = [x]^*_{\mathcal{B}_1}[T]^*_{\mathcal{B}_2,\mathcal{B}_1}[y]_{\mathcal{B}_2},$$

while

$$\langle x, Sy\rangle = [x]^*_{\mathcal{B}_1}[S]_{\mathcal{B}_1,\mathcal{B}_2}[y]_{\mathcal{B}_2}.$$

Suppose $m = \dim H_1$, $n = \dim H_2$. From the above two equations, it follows that $\langle Tx, y\rangle = \langle x, Sy\rangle$ for all $x \in H_1$, $y \in H_2$ if and only if

$$u^*[T]^*_{\mathcal{B}_2,\mathcal{B}_1}v = u^*[S]_{\mathcal{B}_1,\mathcal{B}_2}v$$

for all $u \in \mathbb{C}^m$, $v \in \mathbb{C}^n$, and this happens if and only if $[T]^*_{\mathcal{B}_2,\mathcal{B}_1} = [S]_{\mathcal{B}_1,\mathcal{B}_2}$. Since there is a unique linear transform $S : H_2 \to H_1$ with $[S]_{\mathcal{B}_1,\mathcal{B}_2} = [T]^*_{\mathcal{B}_2,\mathcal{B}_1}$, this tells us both that $T^*$ exists, and is unique.

Furthermore, if $\mathcal{B}'_i$ is another orthonormal basis of $H_i$, then we must have $[T^*]_{\mathcal{B}'_1,\mathcal{B}'_2} = [T]^*_{\mathcal{B}'_2,\mathcal{B}'_1}$. □

**Lemma 5.2.2.** *1. $(T^*)^* = T$ for any linear transformation $T$.*

*2. $(T_1 + T_2)^* = T_1^* + T_2^*$ for all linear transformations $T_1, T_2 \in \mathrm{Lin}(H_1, H_2)$.*

*3. $(T_2T_1)^* = T_1^*T_2^*$ for all linear transformations $T_1 : \mathrm{Lin}(H_1, H_2)$ and $T_2 \in \mathrm{Lin}(H_2, H_3)$.*

*Proof.* Immediately follows from the corresponding facts for matrices and Lemma 5.2.1 □

Recall that in Dirac notation, $\langle w|$ is the element of $H^*$ defined by $|\psi\rangle \mapsto \langle w|\psi\rangle$. Suppose $|\phi\rangle = T\,|w\rangle$. Without Dirac notation, if we set $w = |w\rangle$ and $v = |\psi\rangle$, then

$$\langle Tw, v\rangle = \langle w, T^*v\rangle,$$

so we see that $\langle\phi|\psi\rangle = \langle w|T^*|\psi\rangle$ for all vectors $|\psi\rangle$. So if $|\phi\rangle = T\,|w\rangle$, then we get $\langle\phi| = \langle w|\,T^*$.

If $T \in \mathrm{Lin}(V, V)$ and $\mathcal{B}$ is a basis for $V$, we use the notation $[T]_{\mathcal{B}}$ for $[T]_{\mathcal{B},\mathcal{B}}$.

**Proposition 5.2.3.** *Let $U : H \to H$ be a linear map, and let $\mathcal{B}$ be an orthonormal bases for a (finite-dimensional) Hilbert space $H$. Then the following are equivalent:*

*(a) $U$ is unitary;*

*(b)* $[U]_{\mathcal{B},\mathcal{B}}$ *is a unitary matrix;*

*(c)* $U^*U = \mathbb{1}$*;*

*(d)* $UU^* = \mathbb{1}$*; and*

*(e)* $U(\mathcal{B})$ *is an orthonormal basis of* $H$*.*

In particular, if $T$ is a time evolution operator, then by parts (c) and (d), the inverse of $T$ is $T^*$.

*Proof.* We've already shown in Proposition 3.4.4 that (a), (b), and (e) are equivalent. We can prove the equivalence with (c) and (d) using matrices, but let's see how to do it without picking a basis. We have that $U$ is unitary if and only if

$$\langle Ux, Uy\rangle = \langle x, y\rangle$$

for all $x, y \in H$, and $\langle Ux, Uy\rangle = \langle x, U^*Uy\rangle$. So if $U^*U = \mathbb{1}$, then $\langle Ux, Uy\rangle = \langle x, y\rangle$ for all $x, y \in H$, and $U$ is unitary. Conversely, if $U$ is unitary, then $\langle x, U^*Uy\rangle = \langle x, y\rangle$ for all $x, y \in H$, and that means that

$$\langle x, y - U^*Uy\rangle = 0$$

for all $x, y \in H$. Plugging in $x = y - U^*Uy$, we see that $\|y - U^*Uy\| = 0$ for all $y \in H$, and hence $U^*Uy = y$ for all $y \in H$. In other words, $U^*U = \mathbb{1}$. So (c) and (a) are equivalent.

Finally, (c) is true if and only if $U$ is invertible with inverse $U^*$, and the same is true in part (d). □

Notice that this proof uses the fact that for a finite dimensional vector space $V$, if $S, T : V \to V$ are linear transformations such that $ST = \mathbb{1}$, then both maps are invertible, with $S = T^{-1}$. To see this, suppose $ST = \mathbb{1}$. If $Tx = 0$, then $0 = STx = x$, so $\ker T = 0$. By the rank-nullity theorem, $\dim \operatorname{Im} T = \dim V - \dim \ker T$, so $T$ is surjective as well, and hence invertible. Once we know that $T$ is invertible, we get that $T^{-1} = STT^{-1} = S$. This argument doesn't hold if $V$ is infinite-dimensional, so it's important in Proposition 5.2.3 that $H$ be finite-dimensional.

# Chapter 6

# The Bloch sphere

## 6.1 Equivalence relations

Equivalence relations came up previously in the context of isomorphism. It's now time to look at equivalence relations in more detail.

**Definition 6.1.1.** *A relation $\sim$ on a set $X$ is an* ***equivalence relation*** *if*

*(1) $x \sim x$ for all $x \in X$ ($\sim$ is* ***reflexive****),*

*(2) $x \sim y \implies y \sim x$ for all $x, y \in X$ ($\sim$ is* ***symmetric****), and*

*(3) $x \sim y$ and $y \sim z \implies x \sim z$ for all $x, y, z \in X$ ($\sim$ is* ***transitive****).*

*If $\sim$ is an equivalence relation and $x \in X$, the* ***equivalence class*** *of $x$ is $[x] := \{y \in X : x \sim y\}$.*

If $X$ is a set, a **partition of** $X$ is a collection $\mathcal{P}$ of non-empty subsets of $X$, such that $\bigcup_{U \in \mathcal{P}} = X$, and $U \cap V = \emptyset$ for all $U, V \in \mathcal{P}$. Informally, this means that a partition is a way of dividing $X$ into a collection of disjoint subsets. The significance of equivalence classes of an equivalence relation is explained by the following exercises:

**Exercise 6.1.2.** *Let $\sim$ be an equivalence relation on $X$, and suppose $x, y \in X$. Show that the following are equivalent:*

*1. $x \sim y$,*

*2. $[x] = [y]$, and*

*3. $[x] \cap [y] \neq \emptyset$.*

**Exercise 6.1.3.** *Prove the following:*

1. *If $\sim$ is an equivalence relation on $X$, then the set of equivalence classes $\{[x] : x \in X\}$ is a partition of $X$.*

2. *Suppose $\mathcal{P}$ is a partition of a set $X$, and let $\sim$ be the relation on $X$ defined by saying that $x \sim y$ if and only if there is a subset $U \in \mathcal{P}$ containing both $x$ and $y$. Then $\sim$ is an equivalence relation, and the equivalence classes of $\sim$ are the elements of $\mathcal{P}$.*

Although isomorphism of vector spaces (and of Hilbert spaces) satisfies the three properties in Definition 6.1.1, isomorphism is not actually an example of an equivalence relation, in the sense of Definition 6.1.1. That's because the class of vector spaces is not a set! There's too many vector spaces. We say that the class of vector spaces is a "proper class". In practice this is just a technicality (although it does mean we can't make any arguments which refer to a "set of all vector spaces"). Aside from isomorphism, normally when we work with equivalence relations we'll be working with equivalence relations on sets.

## 6.2 Global phases

If $|\psi\rangle$ is a unit vector in a Hilbert space, then $e^{i\theta} |\psi\rangle$ is also a unit vector for any $\theta \in \mathbb{R}$. We say that $|\psi\rangle$ and $e^{i\theta} |\psi\rangle$ **differ by a global phase**. By Exercise 4.3.2, we cannot perfectly distinguish $|\psi\rangle$ and $e^{i\theta} |\psi\rangle$. The situation turns out to be worse than that:

**Lemma 6.2.1.** *Let $|\psi\rangle$ be a state in $H$, and let $\theta \in \mathbb{R}$. When measuring with respect to an orthonormal basis $\mathcal{B}$, the probability of measuring any outcome $|w\rangle \in \mathcal{B}$ is the same for states $|\psi\rangle$ and $e^{i\theta} |\psi\rangle$.*

*Proof.*

$$| \langle w|\psi\rangle |^2 = | \langle w|e^{i\theta}\psi\rangle |^2$$

for any $w$. □

Given an $\mathbb{F}$-vector space $V$, let's introduce a relation $\sim$ on a $\mathbb{F}$-vector space $V$ by saying that $v \sim w$ if there is a scalar $a \in \mathbb{F} \setminus \{0\}$ such that $v = aw$. Note that if $v \sim 0$, then $v = 0$, and that if $v \sim w$ for $w \neq 0$, then there is a unique $a \in \mathbb{F} \setminus \{0\}$ such that $v = aw$. If, in addition, $v$ and $w$ are unit vectors, then $a$ must have norm 1, so $v$ and $w$ would differ by a global phase.

**Exercise 6.2.2.** *Show that the relation $\sim$ on $V$ is an equivalence relation, and that the equivalence classes of the relation are $\{0\}$ and the sets $L \setminus \{0\}$, where $L$ is a line through the origin in $V$.*[1]

**Definition 6.2.3.** *The set of equivalence classes of $\sim$ in a vector space $V$, excluding $\{0\}$, is called the **projective space of** $V$, and is denoted by $\mathbb{P}V$.*

It turns out $\mathbb{P}V$ is not just a set; it has a very nice geometric structure. In particular, it's both an *algebraic variety*, and a *manifold*. A course on algebraic geometry or manifolds will cover more about this.

By Lemma 6.2.1, if we measure different states in the same equivalence class $[v] \in \mathbb{P}V$, we get the same probability distribution on outcomes. What about the state of the system after measurement, or after a unitary operation? It turns out that both of these preserve $\sim$.

**Proposition 6.2.4.** *Let $v$ and $w$ be two states in a Hilbert space $H$ such that $v \sim w$, and suppose that one of the following two cases holds:*

*(a) $v'$ (resp. $w'$) is the state of the system after measuring $H$ in a basis $\mathcal{B}$ and getting outcome $u \in \mathcal{B}$, assuming the system starts in state $v$ (resp. $w$); or*

*(b) $v'$ (resp. $w'$) is the state of the system after applying time evolution operator $U$, assuming the system starts in state $v$ (resp. $w$).*

*Then $v' \sim w'$.*

*Proof.* Let $v = aw$ for $a \in \mathbb{C}$ with $|a| = 1$. If (a) holds, then

$$v' = \frac{\langle u, v\rangle}{|\langle u, v\rangle}u = \frac{\langle u, aw\rangle}{|\langle u, aw\rangle}u = \frac{a\langle u, w\rangle}{|\langle u, w\rangle}u = aw'.$$

If (b) holds, then $v' = Uv = U(aw) = aUw = aw'$. So in both cases, $v' \sim w'$. □

Applying Proposition 6.2.4 repeatedly, we see that two states which differ by a global phase will still differ by a global phase after any sequence of measurements or unitary time evolutions. Since we can never tell such states apart by measurement, we should regard them as the same state, as far as quantum probability is concerned. This leads to an alternative version of version of Axiom 2.

[1] A line through the origin in $V$ is a subspace of dimension 1.

**Axiom 2** (Alternative version)**.** *The state of a physical system with Hilbert space $H$ is an element of $\mathbb{P}H$.*

We can use either version of the axiom, as long as we declare which we are using. Of course, to properly use the alternative version, we need to think of our operations as functions $\mathbb{P}H \to \mathbb{P}H$, and then we find ourselves talking about transformations of algebraic varieties and manifolds. It's much simpler to stick with linear operations on Hilbert spaces, so by default, we will use the first version, although sometimes it is handy to declare that we are "ignoring a global phase" and implicitly work with the second version.

## 6.3 The Bloch sphere

Suppose we want to represent the space of quantum states visually. The smallest possible non-trivial Hilbert space is $\mathbb{C}^1$. The unit vectors in $\mathbb{C}^1$ are $\pm 1$, but since we have just learned that states don't really depend on phase, $\mathbb{C}^1$ essentially has only one state, and is hence a very uninteresting quantum register. So the smallest interesting system is the qubit register $\mathbb{C}\{0,1\}$. This space has complex dimension 2, and the states are the points

$$(a+bi)\,|0\rangle + (c+di)\,|1\rangle$$

where $a^2+b^2+c^2+d^2 = 1$. The set of points

$$\{(a,b,c,d) \in \mathbb{R}^4 : a^2+b^2+c^2+d^2 = 1\}$$

is called the 3-sphere, and is a 3-dimensional manifold. Unfortunately, 3-dimensional manifolds (aside from $\mathbb{R}^3$) are hard to draw. Fortunately, if we ignore global phases, we can cut down on the dimension of the state space.

**Lemma 6.3.1.** *Every equivalence class $p \in \mathbb{P}\mathbb{C}\{0,1\}$ contains a representative of the form*

$$|\psi(\theta,\phi)\rangle := \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle\,,$$

*where $0 \le \theta \le \pi$ and $0 \le \phi < 2\pi$. In addition:*

- $|\psi(0,\phi)\rangle = |\psi(0,0)\rangle = |0\rangle$ *for all* $0 \le \phi < 2\pi$*, and* $|0\rangle$ *is the unique representative of the form* $|\psi(\theta,\phi)\rangle$ *in the equivalence class* $[|0\rangle]$*.*

- *The elements* $|\psi(\pi,\phi)\rangle = e^{i\phi}\,|1\rangle$ *for* $0 \le \phi < 2\pi$ *belong to the same equivalence class, and these are the only elements of the form* $|\psi(\theta,\phi)\rangle$ *in the equivalence class* $[|1\rangle]$*.*

- *If* $p \neq [|0\rangle], [|1\rangle]$*, then there is a unique choice of* $0 < \theta < \pi$*,* $0 \leq \phi < 2\pi$ *such that* $|\psi(\theta, \phi)\rangle$ *belongs to* $p$*.*

*Proof.* If $|w\rangle = x\,|0\rangle + y\,|1\rangle$, then

$$\frac{|x|}{x}\,|w\rangle = |x|\,|0\rangle + \frac{|x|y}{x}\,|1\rangle = |x|\,|0\rangle + e^{i\phi}|y|\,|1\rangle$$

for some $0 \leq \phi < 2\pi$. Since $|x|^2 + |y|^2 = 1$, we can write $|x| = \cos(\theta/2)$, $|y| = \sin(\theta/2)$ for some $0 \leq \theta \leq \pi$. So $[|w\rangle]$ contains $|\psi(\theta, \phi)\rangle$.

If $\theta = 0$, then $p = [|0\rangle]$, while if $\theta = \pi$, then $p = [|1\rangle]$. So if $p \neq [|0\rangle], [|1\rangle]$ then we can assume that $0 < \theta < \pi$. If $|\psi(\theta', \phi')\rangle$ also belongs to $p$, then there is $s \in \mathbb{C}$, $|s| = 1$, such that

$$s\cos(\theta'/2) = \cos(\theta/2), se^{i\phi'}\sin(\theta'/2) = e^{i\phi}\sin(\theta/2).$$

When $0 < \theta < \pi$,

$$\cos(\theta'/2) = |s\cos(\theta'/2)| = |\cos(\theta/2)| = \cos(\theta/2)$$

and we must have $\theta' = \theta$. Since $\cos(\theta/2) \neq 0$, we also get $s = 1$ from the first equation. Since $\sin(\theta/2) \neq 0$, the second equation implies that $e^{i\phi'} = e^{i\phi}$, and since $0 \leq \phi, \phi' < 2\pi$, we get that $\phi = \phi'$. □

Points of the sphere can also be represented as pairs of angles $(\theta, \phi)$, where $0 \leq \theta \leq \pi$ measures the angle from the north pole $(1, 0, 0)$, and $0 \leq \phi < 2\pi$ measures the angle from the $xz$-plane. This representation is unique, except when $\theta = 0$ or $\theta = \pi$, in which case the pairs $(\theta, \phi)$ give either $(0, 0, 1)$ or $(0, 0, -1)$ respectively. So we can think of states in a qubit register, up to global phase, as points on a sphere. This representation is called the **Bloch sphere**.

**Exercise 6.3.2.** *Show that two states in* $\mathbb{C}\{0, 1\}$ *are orthogonal if and only if the corresponding points on the Bloch sphere are antipodal.*

In other words, we can perfectly distinguish two states via measurement in a basis if and only if they are as far apart as possible on the Bloch sphere. This indicates that distance on the Bloch sphere (or more generally on $\mathbb{P}H$) is a much better measure of distance between states than the norm distance.

# Chapter 7

# Concrete tensor products

## 7.1 Putting two quantum systems together

What happens when we consider a system consisting of two or more quantum registers? If we consider two classical registers capable of containing values from sets $X_1$ and $X_2$ respectively, then the joint system can be thought of as a register capable of containing values from $X_1 \times X_2$. In fact, we often think of an $n$-bit register as $n$ copies of a 1-bit register.

Let $H_1$ and $H_2$ be the Hilbert spaces for two quantum registers. According to Axiom 1 of QM, the joint system containing both registers should also be described by a Hilbert space. What Hilbert space should we use? A first guess might be the product Hilbert space $H_1 \times H_2$, which has dimension $\dim H_1 + \dim H_2$.[1] To see whether this is the right answer, let's consider the case an $m$-bit register and an $n$-bit register, so $H_1 = \mathbb{C}\{0,1\}^m$ and $H_2 = \mathbb{C}\{0,1\}^n$. If we measure the first register in the computational basis we get an $m$-bit string, while if we measure the second register in the computational basis, we get an $n$-bit string. If we measure the two together, we should get an $(m+n)$-bit string as output. Since quantum registers can hold classical information, any $(m+n)$-bit string should be possible as a measurement outcome, so the joint system should have a Hilbert space of dimension $2^{m+n} = \dim H_1 \cdot \dim H_2$, which can be much larger than $\dim H_1 + \dim H_2$. It turns out the correct answer is given by the tensor product of $H_1$ and $H_2$, which is denoted by $H_1 \otimes H_2$:

[1] The product Hilbert space is the same thing as the direct sum Hilbert space, denoted $H_1 \oplus H_2$. This is the Hilbert space with underlying vector space $H_1 \oplus H_2$, and inner product given by declaring that $\mathcal{B}_1 \cup \mathcal{B}_2$ is orthonormal for any orthonormal bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of $H_1$ and $H_2$ respectively.

**Axiom 5.** *Let $H_1$ and $H_2$ be the Hilbert spaces of two physical systems. Then the Hilbert space of the joint system is the tensor product $H_1 \otimes H_2$.*

The tensor product is notoriously difficult to define in full generality when compared to most other constructions in linear algebra. However, for vector spaces with a distinguished basis, like free vector spaces and $\mathbb{C}^n$, there are concrete ways to define the tensor product that are easier to understand. In this section we'll look at the concrete tensor products for these two spaces.

## 7.2 Free vector spaces

**Definition 7.2.1.** *Let $X_1$ and $X_2$ be sets. The* ***concrete tensor product*** *of $\mathbb{F}X_1$ and $\mathbb{F}X_2$ is*

$$\mathbb{F}X_1 \underline{\otimes} \mathbb{F}X_2 := \mathbb{F}X_1 \times X_2.$$

The free vector space $\mathbb{F}X_1 \times X_2$ has basis

$$\{|(x_1, x_2)\rangle : (x_1, x_2) \in X_1 \times X_2\}.$$

In the context of tensor products, this vector is often written as

$$|x_1, x_2\rangle \text{ or } |x_1\rangle |x_2\rangle \text{ or } |x_1\rangle \underline{\otimes} |x_2\rangle .$$

The tensor product of two vector spaces is usually denoted $V \otimes W$, for concrete tensor products, we use $\underline{\otimes}$ . This is to distinguish the concrete tensor product from the abstract tensor product defined in the next chapter. Once we're comfortable using both tensor products, we'll use $\otimes$ for both the abstract and concrete tensor products.

Recall that $\mathbb{C}X_i$ is the quantum analog of a register holding values in $X_i$. When we plug this definition into Axiom 5 above, it tells us that the joint system for two such quantum registers is the quantum analog of a register holding values in $X_1 \times X_2$, which matches our expectation about possible measurements outcomes for the joint system.

If $\mathbb{C}X_1$ and $\mathbb{C}X_2$ are separate registers, then we might expect to be able store a state in each register independently. Since this should be possible physically, we should expect there to be a function

$$\mathbb{C}X_1 \times \mathbb{C}X_2 \to \mathbb{C}X_1 \times X_2$$

which, given a pair of states $(|\psi_1\rangle , |\psi_2\rangle) \in \mathbb{C}X_1 \times \mathbb{C}X_2$, outputs a state $|\psi\rangle \in \mathbb{C}X_1 \times X_2$. And indeed, a nice function of this form exists:

**Definition 7.2.2.** *If*

$$v = \sum_{x \in X_1} a_x \left| x \right\rangle \in \mathbb{C}X_1 \text{ and } w = \sum_{y \in X_2} b_y \left| y \right\rangle \in \mathbb{C}X_2,$$

*then the* ***concrete tensor product*** *of $v$ and $w$ is*

$$v \underline{\otimes} w := \sum_{(x,y) \in X_1 \times X_2} a_x b_y \left| x, y \right\rangle .$$

*The function $\mathbb{C}X_1 \times \mathbb{C}X_2 \to \mathbb{C}X_1 \times X_2$ is called the* ***(concrete) tensor product map****.*

**Lemma 7.2.3.** *If $|\psi_i\rangle \in \mathbb{C}X_i$ is a unit vector for $i = 1, 2$, then $|\psi_1\rangle \underline{\otimes} |\psi_2\rangle$ is also a unit vector.*

*Proof.* Let

$$|\psi_1\rangle = \sum_{x \in X_1} a_x \left| x \right\rangle \in \mathbb{C}X_1 \text{ and } |\psi_2\rangle = \sum_{y \in X_2} b_y \left| y \right\rangle .$$

Then

$$\| |\psi_1\rangle \underline{\otimes} |\psi_2\rangle \|^2 = \sum_{x,y} |a_x b_y|^2 = \left( \sum_{x \in X_1} |a_x|^2 \right) \left( \sum_{y \in X_2} |b_y|^2 \right) = \| \, |\psi_1\rangle \, \|^2 \| \, |\psi_2\rangle \, \|^2 = 1.$$

□

The tensor product map $\underline{\otimes} : \mathbb{C}X_1 \times \mathbb{C}X_2 \to \mathbb{C}X_1 \times X_2$ is a function between two vector spaces. However, it's not a linear function. For instance, it's clear from the definition of $\underline{\otimes}$ that

$$v \underline{\otimes} 0 = 0 \underline{\otimes} w = 0$$

for any $v \in \mathbb{C}X_1$, $w \in \mathbb{C}X_2$. Now in $\mathbb{C}X_1 \times \mathbb{C}X_2$, $(v, w) = (v, 0) + (0, w)$, so in particular,

$$(\left| x \right\rangle, \left| y \right\rangle) = (\left| x \right\rangle, 0) + (0, \left| y \right\rangle)$$

for any $x \in X_1$, $y \in X_2$. But

$$\left| x \right\rangle \underline{\otimes} \left| y \right\rangle = \left| x, y \right\rangle \neq 0 = \left| x \right\rangle \underline{\otimes} 0 + 0 \underline{\otimes} \left| y \right\rangle ,$$

so $\underline{\otimes}$ is not linear.

Instead, $\underline{\otimes}$ is bilinear:

**Definition 7.2.4.** *Let $U$, $V$, and $W$ be vector spaces. A function $T : U \times V \to W$ is **bilinear** if*

$$T(\lambda u + w, v) = \lambda T(u, v) + T(w, v)$$

*and*

$$T(u, \lambda v + w') = \lambda T(u, v) + T(u, w')$$

*for all $\lambda \in \mathbb{C}$, $u, w \in U$, $v, w' \in V$.*

**Proposition 7.2.5.** *Let $X_1$, $X_2$ be sets. Then the tensor product map*

$$\underline{\otimes} : \mathbb{C}X_1 \times \mathbb{C}X_2 \to \mathbb{C}X_1 \times X_2$$

*is bilinear.*

*Proof.* Suppose $u, w \in \mathbb{C}X_1$, $v \in \mathbb{C}X_2$, and $\lambda \in \mathbb{C}$. Write

$$u = \sum_{x \in X_1} a_x \left| x \right\rangle, w = \sum_{x \in X_1} b_x \ \left| x \right\rangle, \text{ and } w = \sum_{y \in X_2} c_y \left| y \right\rangle.$$

Then

$$\begin{aligned}(\lambda u + w) \underline{\otimes} v &= \left( \sum_{x \in X_1} (\lambda a_x + b_x) \left| x \right\rangle \right) \underline{\otimes} \left( \sum_{y \in X_2} c_y \left| y \right\rangle \right) \\ &= \sum_{(x,y) \in X_1 \times X_2} (\lambda a_x + b_x) c_y \left| x, y \right\rangle \\ &= \lambda \sum_{(x,y) \in X_1 \times X_2} a_x c_y \left| x, y \right\rangle + \sum_{(x,y) \in X_1 \times X_2} b_x c_y \left| x, y \right\rangle \\ &= \lambda u \underline{\otimes} v + w \underline{\otimes} v.\end{aligned}$$

Similarly

$$u \underline{\otimes} (\lambda v + w') = \lambda u \underline{\otimes} v + u \underline{\otimes} w'$$

for all $u \in U$, $v, w' \in V$, $\lambda \in \mathbb{C}$. So $\underline{\otimes}$ is bilinear. □

Is every element of $\mathbb{C}X_1 \underline{\otimes} \mathbb{C}X_2$ of the form $v \underline{\otimes} w$? This is the same as asking if the function

$$\underline{\otimes} : \mathbb{C}X_1 \times \mathbb{C}X_2 \to \mathbb{C}X_1 \times X_2$$

is onto. If $\underline{\otimes}$ was linear, then this would be impossible in general, since $(\dim \mathbb{C}X_1)(\dim \mathbb{C}X_2)$ is in general much larger than $\dim \mathbb{C}X_1 + \dim \mathbb{C}X_2$. In fact, $\underline{\otimes}$ is a nice enough function that this dimension argument can be made to work (although since it requires some geometry, we won't go through the argument in this course). In fact, even when it's allowed by the dimensions, $\underline{\otimes}$ is not usually onto.

**Exercise 7.2.6.** *Let $X_1 = \{x_1, \ldots, x_m\}$, $X_2 = \{y_1, \ldots, y_n\}$, and let*

$$|\psi\rangle = \sum_{i,j} m_{ij} \, |x_i, y_j\rangle \in \mathbb{C}X_1 \underline{\otimes} \mathbb{C}X_2$$

*be a non-zero vector. Show that $|\psi\rangle = v \underline{\otimes} w$ for some $v \in \mathbb{C}X_1$, $w \in \mathbb{C}X_2$ if and only if the $m \times n$ matrix $M = (m_{ij})$ has rank $1$.*

**Definition 7.2.7.** *If $|\psi\rangle \in \mathbb{C}X_1 \underline{\otimes} \mathbb{C}X_2$ is not of the form $v \underline{\otimes} w$ for $v \in \mathbb{C}X_1$, $w \in \mathbb{C}X_2$, then we say that $|\psi\rangle$ is* ***entangled****.*

**Example 7.2.8.** *If $X_1 = X_2 = \{0, 1\}$, then $|00\rangle + |11\rangle$ is entangled, since the matrix $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has rank $2$.*

## 7.3 The Kronecker product

We can also define a concrete tensor product for vector spaces $\mathbb{C}^m$ and $\mathbb{C}^n$.

**Definition 7.3.1.** *If $m, n \geq 1$, then the* ***concrete tensor product*** *of $\mathbb{C}^m$ and $\mathbb{C}^n$ is $\mathbb{C}^m \underline{\otimes} \mathbb{C}^n := \mathbb{C}^{mn}$. If $u \in \mathbb{C}^m$ and $v \in \mathbb{C}^n$, then the* ***concrete tensor product****, or* ***Kronecker product****, of $u$ and $v$ is the vector*

$$u \underline{\otimes} v := \begin{pmatrix} u_1 v_1 \\ u_1 v_2 \\ \vdots \\ u_1 v_n \\ u_2 v_1 \\ \vdots \\ u_2 v_n \\ \vdots \\ u_m v_1 \\ \vdots \\ u_m v_n \end{pmatrix}$$

Often the Kronecker product is written in "block-vector" form as

$$u \underline{\otimes} v = \begin{pmatrix} u_1 v \\ u_2 v \\ \vdots \\ u_n v \end{pmatrix}.$$

We can think of the Kronecker product as replacing every entry of $u$ with that entry times $v$. With this definition, of $e_1, \ldots, e_m$ is the standard basis of $\mathbb{C}^m$, and $f_1, \ldots, f_n$ is the standard basis of $\mathbb{C}^n$, then $e_i \mathbin{\underline{\otimes}} f_j$ is the $((i-1)n+j)$th standard basis vector of $\mathbb{C}^{mn}$.

**Example 7.3.2.** *In the concrete tensor product $\mathbb{C}^2 \mathbin{\underline{\otimes}} \mathbb{C}^3 \cong \mathbb{C}^6$, the vector*

$$2e_1 \mathbin{\underline{\otimes}} f_1 + 7e_1 \mathbin{\underline{\otimes}} f_2 - e_1 \mathbin{\underline{\otimes}} f_3 - 4e_2 \mathbin{\underline{\otimes}} f_1 + 5e_2 \mathbin{\underline{\otimes}} f_2 - 8e_2 \mathbin{\underline{\otimes}} f_3$$

*is equal to*

$$\begin{pmatrix} 2 \\ 7 \\ -1 \\ -4 \\ 5 \\ -8 \end{pmatrix} \in \mathbb{C}^6.$$

The concrete tensor product of free vector spaces is connected to the Kronecker product as follows:

**Proposition 7.3.3.** *Let $X_1 = \{x_1, \ldots, x_m\}$, $X_2 = \{y_1, \ldots, y_n\}$ be ordered sets, and let $\beta_i$ be the computational basis of $\mathbb{C}X_i$, $i = 1, 2$, ordered using the order from $X_1$ and $X_2$. Let $\beta$ be the computational basis of $\mathbb{C}X_1 \times X_2$, with the lexicographic order*

$$\begin{gathered} \left|x_1, y_1\right\rangle, \left|x_1 y_2\right\rangle, \ldots, \left|x_1, y_n\right\rangle, \\ \left|x_2, y_1\right\rangle, \left|x_2, y_2\right\rangle, \ldots, \left|x_2, y_n\right\rangle, \\ \vdots \\ \left|x_m, y_1\right\rangle, \left|x_m, y_2\right\rangle, \ldots, \left|x_m, y_n\right\rangle. \end{gathered}$$

*Then*

$$[u \mathbin{\underline{\otimes}} v]_\beta = [u]_{\beta_1} \mathbin{\underline{\otimes}} [v]_{\beta_2}$$

*for all $u \in \mathbb{C}X_1$, $v \in \mathbb{C}X_2$, where the first concrete tensor product $\underline{\otimes}$ inside the brackets is the tensor product map for free vector spaces, and the second outside the brackets is the Kronecker product.*

*Proof.* If $u = \sum a_i \left|x_i\right\rangle$ and $v = \sum b_j \left|y_j\right\rangle$, then

$$u \mathbin{\underline{\otimes}} v = \sum_{i,j} a_i b_j \left|x_i, y_j\right\rangle.$$

So $[u \mathbin{\underline{\otimes}} v]_\beta$ is the vector with $((i-1)n+j)$th entry equal to $a_i b_j$, which is the Kronecker product of $[u]_{\beta_1}$ and $[v]_{\beta_2}$. □

It's not hard to see that the tensor product map

$$\mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}^{mn} : (u, v) \mapsto u \underline{\otimes} v$$

is bilinear. We can either prove this directly, or use Propositions 7.2.5 and 7.3.3.

# Chapter 8

# Abstract tensor products

The concrete tensor product works fine as a way to take tensor products of free vector spaces, but we still need to define the tensor product of vector spaces in general. Of course, if $V \cong V'$ and $W \cong W'$, then we expect that $V \otimes W \cong V' \otimes W'$ (and indeed, once we've defined the tensor product properly, we'll prove this). If $V$ is a finite-dimensional vector space with basis $b_1, \ldots, b_n$, then there is an isomorphism $\mathbb{C}\{1, \ldots, n\} \to V$ sending $|i\rangle \mapsto b_i$, and a similar argument works for infinite-dimensional vector spaces. Since every vector space is isomorphic to a free vector space, we could try to define the tensor product of $V$ and $W$ by picking isomorphisms $V \cong \mathbb{C}X$ and $W \cong \mathbb{C}Y$, and then setting $V \otimes W := \mathbb{C}X \underline{\otimes} \mathbb{C}Y$. This is actually not a bad idea, except that choosing an isomorphism $V \cong \mathbb{C}X$ amounts to choosing a basis for $V$. There are two reasons we'd like to avoid this:

(1) When we make new definitions based on $V \otimes W$, we'd like to know if the new definition depends on a choice of basis. If the definition of $V \otimes W$ itself depend on a choice of basis for $V$ and $W$, then this is something we'll have to check for each new definition we make.

(2) From the point of view of quantum mechanics, if $V$ and $W$ are Hilbert spaces corresponding to physical systems, then $V \otimes W$ is supposed to be the Hilbert space corresponding to the joint system of $V$ and $W$. Choosing an orthonormal basis for $V$ or $W$ is like choosing a specific measurement process to apply to the system. We should be able to talk about the joint system of two subsystems without having to make such a choice.

For these reasons, we'd like to find a "natural" definition of $V \otimes W$, meaning a definition that does not depend on a choice of basis. For this, we'll need to know some facts about quotient spaces.

## 8.1 Quotient spaces

**Lemma 8.1.1.** *Let $U \subseteq V$ be a subspace of a vector space $V$. Define a relation $\sim$ on $V$ by setting $u \sim v$ if and only if $u - v \in U$. Then $\sim$ is an equivalence relation.*

*Proof.* Since $v - v = 0 \in U$, $v \sim v$ for all $v \in V$. Also if $u - v \in U$, then $v - u = -(u - v) \in U$ so $u \sim v$ implies that $v \sim u$. Finally if $u \sim v$ and $v \sim w$ then $u - v, v - w \in U$, so $(u - v) + (v - w) = u - w \in U$, and hence $u \sim w$. □

**Definition 8.1.2.** *Let $U \subset V$ be a subspace of a vector space $V$, and let $\sim$ be the relation on $V$ from Lemma 8.1.1. Then the **quotient space of** $V$ **by** $U$ is the set of equivalence classes of $\sim$. The quotient space is denoted by $V/U$.*

**Proposition 8.1.3.** *The quotient space $V/U$ is a vector space with operations*

$$[u] + [v] = [u + v]$$

*and*

$$\lambda \cdot [u] = [\lambda u]$$

*for all $\lambda \in \mathbb{F}$, $u, v \in V$. The zero element of this space is $[0]$, the equivalence class of the zero element of $V$.*

*Furthermore, the map*

$$q : V \to V/U : v \mapsto [v]$$

*is linear and surjective, with $\ker q = U$.*

The map $q$ is called the **quotient map**.

*Proof.* We need to show that the operations are well-defined. Suppose that $[u] = [u']$ and $[v] = [v']$. Then $u \sim u'$ and $v \sim v'$, so $u - u', v - v' \in U$, and hence $u + v - (u' + v') = u - u' + v - v' \in U$. Hence $[u + v] = [u' + v']$. If $\lambda \in \mathbb{F}$, then $\lambda u - \lambda u' = \lambda(u - u') \in U$, so $[\lambda u] = [\lambda u']$. So both operations are well-defined functions.

We also have to check that these operations satisfy all the axioms of a vector space. We leave this as an exercise. However, to see how this works, notice that $[0]$ satisfies the axioms required by the zero element, since $[v]+[0] = [v + 0] = [v]$, $0 \cdot [v] = [0 \cdot v] = [0]$, and so on. Since a vector space has a unique zero element, $[0]$ must be the zero element.

The operations on $V/U$ are defined precisely so that $q$ is linear. Indeed, if $\lambda \in \mathbb{F}$ and $u, v \in V$, then

$$q(\lambda u + v) = [\lambda u + v] = \lambda[u] + [v] = \lambda q(u) + q(v).$$

The map $q$ is also clearly surjective. We have $u \in \ker q$ if and only if $[u] = 0_{V/U} = 0$, and this happens if and only if $u - 0 = u \in U$. So $\ker q = U$. □

If $T : V/U \to W$ is linear, then $T \circ q : V \to W$ is also linear. We'd like to know what linear functions $\tilde{T} : V \to W$ can be written in this form. One thing we see immediately is that since $\ker q = U$, if $\tilde{T} = T \circ q$, then $U \subseteq \ker \tilde{T}$. It turns out that this condition is enough to guarantee that the linear function $T$ exists:

**Proposition 8.1.4** (Universal property of quotient spaces)**.** *Let $\tilde{T} : V \to W$ be linear, let $U$ be a subspace of $V$, and let $q : V \to V/U$ be the quotient map. Then there is a linear function $T : V/U \to W$ such that $\tilde{T} = T \circ q$ if and only if $U \subseteq \ker \tilde{T}$.*

*Proof.* If $\tilde{T} = T \circ q$ and $u \in U$, then $\tilde{T}(u) = T(q(u)) = T(0) = 0$. So $U \subseteq \ker \tilde{T}$.

On the other hand, suppose $U \subseteq \ker \tilde{T}$, and define $T : V/U \to W$ by $T[v] = \tilde{T}(v)$. To see that $T$ is well-defined, suppose that $[v] = [v']$ for some $v, v' \in V$. Then $v - v' \in U$, so $\tilde{T}(v - v') = 0$, and hence $\tilde{T}(v) = \tilde{T}(v')$. So $T$ is well-defined.

If $\lambda \in \mathbb{F}$, $u, v \in V$, then

$$T(\lambda[u] + [v]) = T([\lambda u + v]) = \tilde{T}(\lambda u + v) = \lambda \tilde{T}(u) + \tilde{T}(v) = \lambda T([u]) + T([v]),$$

so $T$ is linear. □

Proposition 8.1.4 is called the universal property for quotient spaces because it shows that every linear transformation $T : V \to W$ with $U \subset \ker T$ factors through the quotient map $q : V \to V/U$. In this sense, the quotient map is "universal" for the property of containing $U$ in the kernel.

## 8.2 Defining the tensor product

We can now define the tensor product of two vector spaces as a quotient space:

**Definition 8.2.1.** *Let $V$ and $W$ be vector spaces. If $v \in V$, $w \in W$, we let $v \boxtimes w$ denote the element $|v, w\rangle \in \mathbb{F}V \times W$. Let $Q$ be the subspace of $\mathbb{F}V \times W$ spanned by*

$$(\lambda u + v) \boxtimes w - \lambda(u \boxtimes w) - v \boxtimes w$$

*and*

$$v \boxtimes (\lambda u' + w) - \lambda(v \boxtimes u') - v \boxtimes w$$

*for all $\lambda \in \mathbb{F}$, $u, v \in V$, $u', w \in W$. The* ***tensor product*** *of $V$ and $W$ is the quotient space*

$$V \otimes W := \mathbb{F}V \times W/Q.$$

*If $v \in V$, $w \in W$, then the* ***tensor product of*** *$v$* ***and*** *$w$ is*

$$v \otimes w := [v \boxtimes w],$$

*the equivalence class of $v \boxtimes w$ in $(\mathbb{F}V \times W)/Q$.*

Notice that this definition uses the free vector space $\mathbb{F}V \times W$. Unless both $V$ and $W$ are trivial vector spaces, this free vector space is very big: it not only contains the vectors $|v, w\rangle$ for all $v \in V$ and $w \in V$, but these vectors are all orthogonal to each other. This can be a bit counterintuitive: for instance, if $v \in V$ is non-trivial, then $|v, 0\rangle$ and $|\lambda v, 0\rangle$ are orthogonal for all $\lambda \in \mathbb{F}$ with $\lambda \neq 1$, even though $v$ and $\lambda v$ are linearly dependent in $V$.

The notation $v \boxtimes w$ for $|v, w\rangle$ is not very consequential, and we only use it in this section. However, it is helpful in suggesting the intent of the definition.

**Lemma 8.2.2.** *Let $V$ and $W$ be vector spaces. The tensor product map*

$$V \times W \to V \otimes W : (v, w) \mapsto v \otimes w$$

*is bilinear.*

*Proof.* If $\lambda \in \mathbb{F}$, $u, v \in V$, $w \in W$, then

$$(\lambda u + v) \otimes w = [(\lambda u + v) \boxtimes w].$$

Let $Q$ be the subspace of $\mathbb{F}V \times W$ from Definition 8.2.1. Since

$$(\lambda u + v) \boxtimes w - (\lambda(u \boxtimes w) + v \boxtimes w) \in Q,$$

the definition of the equivalence relation for $\mathbb{F}V \times W/Q$ implies that

$$[(\lambda u + v) \boxtimes w] = [(\lambda(u \boxtimes w) + v \boxtimes w)] = \lambda[u \boxtimes w] + [v \boxtimes w] = \lambda u \otimes w + v \otimes w.$$

Similarly, if $\lambda \in \mathbb{F}$, $v \in V$, and $u, w \in W$, then

$$v \otimes (\lambda u + w) = \lambda v \otimes u + v \otimes w.$$

So the tensor product map is bilinear. □

Note that if we have a bilinear map, we can compose the inputs or the outputs with a linear map to get another bilinear map:

**Exercise 8.2.3.** *Let $A : U' \to U$, $B : V' \to V$, and $C : W \to W'$ be linear. Show that if $T : U \times V \to W$ is bilinear, then the function*

$$U' \times V' \to W' : (u, v) \mapsto C(T(A(u), B(v)))$$

*is bilinear.*

We'll use Exercise 8.2.3 in the next section. But for now, note that in the special case when $A$ and $B$ are the identity maps $U \to U$ and $V \to V$ respectively, Exercise 8.2.3 implies that if we compose a linear map with a bilinear map, we get another bilinear map. So if $C : U \otimes V \to W$ is linear, then the composition

$$U \times V \to U \otimes V \to W : (u, v) \mapsto C(u \otimes v)$$

of $C$ with the tensor product map is bilinear. So composing with the tensor product map gives a function

$$\mathrm{Lin}(U \otimes V, W) \to \{\text{bilinear maps } U \times V \to W\}$$

The next proposition tells us that this function is a bijection, so that every bilinear map $U \times V \to W$ can be identified with a unique linear map $U \otimes V \to W$:

**Proposition 8.2.4** (Universal property of tensor products)**.** *If $T : U \times V \to W$ is bilinear, then there is a unique linear map $T' : U \otimes V \to W$ such that $T(u, v) = T'(u \otimes v)$ for all $u \in U$, $v \in V$.*

Once again, this proposition is called a "universal property" because it implies that every bilinear map factors through the tensor product map.

Before proving the proposition, we need one lemma:

**Lemma 8.2.5.** *If $U, V$ are vector spaces, then the elements $\{u \otimes v : u \in U, v \in V\}$ span $U \otimes V$.*

*Proof.* The elements $u \boxtimes v$, $u \in U$, $v \in V$, form a basis for $\mathbb{F}V \times W$. The quotient map $q$ is surjective by Proposition 8.1.3, so

$$q(\{u \boxtimes v : u \in U, v \in V\}) = \{u \otimes v : u \in U, v \in V\}$$

is a spanning set of $U \otimes V$. □

*Proof of Proposition 8.2.4.* Given $T$, define

$$\tilde{T} : \mathbb{F}U \times V \to W$$

by setting $\tilde{T}(u \boxtimes v) = T(u, v)$ and extending linearly. Then by the bilinearity of $T$,

$$\tilde{T}((\lambda u + v) \boxtimes w - \lambda(u \boxtimes w) - v \boxtimes w) = T(\lambda u + v, w) - \lambda T(u, w) - T(v, w) = 0$$

for all $\lambda \in \mathbb{F}$, $u, v \in U$, and $w \in V$. Similarly

$$\tilde{T}(v \boxtimes (\lambda u + w) - \lambda(v \boxtimes u) - v \boxtimes w) = 0$$

for all $\lambda \in \mathbb{F}$, $v \in U$, and $u, w \in W$. So $Q \subseteq \ker \tilde{T}$. By Proposition 8.1.4, there is a linear map $T' : \mathbb{F}U \times V/Q \to W$ such that $\tilde{T} = T' \circ q$, where $q : \mathbb{F}U \times V \to \mathbb{F}U \times V/Q$ is the quotient map. This means that

$$T'(v \otimes w) = T'([v \boxtimes w]) = \tilde{T}(v \boxtimes w) = T(v, w)$$

as required.

If $T''(u \otimes v) = T(u, v)$, then by Lemma 8.2.5, $T''$ and $T'$ agree on a spanning set for $U \otimes V$, so $T' = T''$. □

Using the universal property, we can prove that the abstract tensor product and the concrete tensor product are isomorphic, in the following sense:

**Proposition 8.2.6.** *Let $X_1, X_2$ be finite sets. Then there is an isomorphism*

$$T : \mathbb{F}X_1 \otimes \mathbb{F}X_2 \to \mathbb{F}X_1 \underline{\otimes} \mathbb{F}X_2$$

*such that*

$$T(u \otimes v) = u \underline{\otimes} v$$

*for all $u \in \mathbb{F}X_1$, $v \in \mathbb{F}X_2$.*

*Proof.* Recall that the tensor product map

$$\mathbb{F}X_1 \times \mathbb{F}X_2 \to \mathbb{F}X_1 \underline{\otimes} \mathbb{F}X_2 : (u, v) \mapsto u \underline{\otimes} v$$

is bilinear. By the universal property of tensor products, there is a linear map

$$T : \mathbb{F}X_1 \otimes \mathbb{F}X_2 \to \mathbb{F}X_1 \underline{\otimes} \mathbb{F}X_2$$

such that $T(u \otimes v) = u \underline{\otimes} v$ for all $u \in \mathbb{F}X_1$, $v \in \mathbb{F}X_2$.

To show that $T$ is an isomorphism, we can construct an inverse to $T$. Define

$$S : \mathbb{F}X_1 \times X_2 \to \mathbb{F}X_1 \otimes \mathbb{F}X_2$$

by setting

$$S(|x, y\rangle) = |x\rangle \otimes |y\rangle$$

for all $x \in X_1$, $y \in X_2$, and extending linearly. Since

$$T \circ S(|x, y\rangle) = T(|x\rangle \otimes |y\rangle) = |x, y\rangle \,,$$

and the elements $|x, y\rangle$, $x \in X_1, y \in X_2$ form a basis for $\mathbb{F}X_1 \times X_2$, $T \circ S = \mathbb{1}$ on $\mathbb{F}X_1 \times X_2$.

For the other direction, suppose

$$u = \sum_{x \in X_1} a_x \, |x\rangle \in \mathbb{F}X_1 \text{ and } v = \sum_{y \in X_2} b_y \, |y\rangle \in \mathbb{F}X_2.$$

Since $\otimes$ is bilinear,

$$u \otimes v = \sum_{x,y} a_x b_y \, |x\rangle \otimes |y\rangle \,.$$

So

$$S \circ T(u \otimes v) = S(u \underline{\otimes} v) = S(\sum_{x,y} a_x b_y \, |x, y\rangle) = \sum_{x,y} a_x b_y \, |x\rangle \otimes |y\rangle = u \otimes v.$$

Thus $S \circ T$ agrees with the identity on $\mathbb{F}X_1 \otimes \mathbb{F}X_2$ on a spanning set, so $S \circ T = \mathbb{1}$. Thus $S$ and $T$ are inverses, so $T$ is an isomorphism. □

Since there's an isomorphism $\mathbb{F}X_1 \underline{\otimes} \mathbb{F}X_2 \cong \mathbb{F}X_1 \otimes \mathbb{F}X_2$ sending $|x, y\rangle \mapsto |x\rangle \otimes |y\rangle$, we identify these concrete and abstract tensor products from now on. In particular, we can write $|x, y\rangle$ as $|x\rangle \otimes |y\rangle$. It's also common to drop the tensor product symbol and write $|x\rangle \, |y\rangle$ when using Dirac notation.

## 8.3 Tensor products of linear maps

So far we've defined the tensor product of spaces $V \otimes W$, and the tensor product of vectors $v \otimes w$. We can also take the tensor product of linear maps.

**Proposition 8.3.1.** *Let $A : U' \to U$ and $B : V' \to V$ be linear maps. Then there is a unique linear map*

$$C : U' \otimes V' \to U \otimes V$$

*such that $C(u \otimes v) = A(u) \otimes B(v)$ for all $u \in U'$, $v \in V'$.*

*Proof.* Let $T : U \times V \to U \otimes V$ be the tensor product map $T(x, y) = x \otimes y$. Then $T$ is bilinear. By Exercise 8.2.3,

$$S : U' \times V' \to U \otimes V : (u, v) \mapsto T(A(u), B(v))$$

is bilinear. By the universal property of tensor products, there is a linear map

$$C : U' \otimes V' \to U \otimes V$$

such that

$$C(u \otimes v) = S(u, v) = T(A(u), B(v)) = A(u) \otimes B(v)$$

for all $u \in U'$, $v \in V'$.

If $C'(u \otimes v) = A(u) \otimes B(v)$ for all $u \in U'$, $v \in V'$, then by Lemma 8.2.5, $C'$ and $C$ agree on a spanning set of $U' \otimes V'$, so $C = C'$. □

**Definition 8.3.2.** *The linear map $C$ from Proposition 8.3.1 is called the* ***tensor product*** *of $A$ and $B$, and is denoted by $A \otimes B$.*

Although we've used an abstract theorem, the universal property of tensor products, so show that $A \otimes B$ exists, in practice it is simple to compute $A \otimes B$ using the fact that $(A \otimes B)(v \otimes w) = A(v) \otimes B(w)$.

**Example 8.3.3.** *Define $T : \mathbb{C}\{0, 1, 2\} \to \mathbb{C}\{0, 1, 2\}$ by $S\,|i\rangle = |i + 1 \mod 3\rangle$, and $S : \mathbb{C}\{0, 1\} \to \mathbb{C}\{0, 1\}$ by $T\,|0\rangle = |0\rangle$ and $T\,|1\rangle = 0$. Then*

$$S \otimes T(3\,|0, 1\rangle - 3\,|1, 1\rangle + 7\,|0, 2\rangle) = 3S\,|0\rangle \otimes T\,|1\rangle - 3S\,|1\rangle \otimes T\,|1\rangle + 7S\,|0\rangle \otimes T\,|2\rangle = 3\,|0, 2\rangle + 7\,|0, 0\rangle\,.$$

**Proposition 8.3.4.** *(1) If $S_0 : U_0 \to U_1$, $S_1 : U_1 \to U_2$, $T_0 : V_0 \to V_1$, and $T_1 : V_1 \to V_2$ are linear maps, then*

$$(S_1 \otimes T_1)(S_0 \otimes T_0) = S_1 S_0 \otimes T_1 T_0.$$

*(2) If $\mathbb{1}_U$ and $\mathbb{1}_V$ denote the identity maps $U \to U$ and $V \to V$ for vector spaces $U$ and $V$ respectively, then $\mathbb{1}_U \otimes \mathbb{1}_V = \mathbb{1}_{U \otimes V}$, the identity map $U \otimes V \to U \otimes V$.*

*Proof.* For (1), if $u \in U_0$, $v \in V_0$, then

$$(S_1 \otimes T_1)(S_0 \otimes T_0)(u \otimes v) = (S_1 \otimes T_1)(S_0(u) \otimes T_0(v)) = S_1 S_0(u) \otimes T_1 T_0(v).$$

Since $S_1 S_0 \otimes T_1 T_0$ is the unique linear map $U_0 \otimes V_0 \to U_2 \to V_2$ with $(S_1 S_0 \otimes T_1 T_0)(u \otimes v) = S_1 S_0(u) \otimes T_1 T_0(v)$ for all $u \in U_0$, $v \in V_0$, we must have $(S_1 \otimes T_1)(S_0 \otimes T_0) = S_1 S_0 \otimes T_1 T_0$.

Part (2) is similar. If $u \in U$, $v \in V$, then

$$\mathbb{1}_{U \otimes V}(u \otimes v) = u \otimes v = \mathbb{1}_U(u) \otimes \mathbb{1}_V(v).$$

So $\mathbb{1}_{U \otimes V} = \mathbb{1}_U \otimes \mathbb{1}_V$. □

**Corollary 8.3.5.** *If $S : U' \to U$ and $T : V' \to V$ are isomorphisms, then $S \otimes T : U' \otimes V' \to U \otimes V$ is an isomorphism with inverse $S^{-1} \otimes T^{-1}$.*

*Proof.* By parts (1) and (2) of Proposition 8.3.4,

$$(S \otimes T)(S^{-1} \otimes T^{-1}) = SS^{-1} \otimes TT^{-1} = \mathbb{1}_U \otimes \mathbb{1}_V = \mathbb{1}_{U \otimes V}.$$

Similarly, $(S^{-1} \otimes T^{-1})(S \otimes T) = \mathbb{1}_{U' \otimes V'}$. So $S \otimes T$ is an isomorphism with inverse $S^{-1} \otimes T^{-1}$. □

In the previous section we showed that $\mathbb{F}X_1 \otimes \mathbb{F}X_2 \cong \mathbb{F}X_1 \underline{\otimes} \mathbb{F}X_2$. Since $\{|x, y\rangle : x \in X_1, y \in X_2\}$ is a basis for $\mathbb{F}X_1 \underline{\otimes} \mathbb{F}X_2$, it follows that $\{|x\rangle \otimes |y\rangle : x \in X_1, y \in X_2\}$ is a basis for $\mathbb{F}X_1 \otimes \mathbb{F}X_2$. In particular, the tensor product of two finite-dimensional free vector spaces is also finite-dimensional. With Corollary 8.3.5, we can easily extend this to the tensor product $U \otimes V$ of two arbitrary finite-dimensional vector spaces. The following theorem is the most important theorem about the structure of tensor product spaces:

**Theorem 8.3.6.** *let $U$ and $V$ be vector spaces with bases $\alpha = \{a_1, \ldots, a_m\}$ and $\beta = \{b_1, \ldots, b_n\}$ respectively. Then*

$$\gamma = \{a_i \otimes b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

*is a basis for $U \otimes V$. In particular, $\dim U \otimes V = (\dim U)(\dim V)$.*

*Furthermore, if we order $\gamma$ lexicographically as*

$$\gamma = \{a_1 \otimes b_1, a_1 \otimes b_2, \ldots, a_1 \otimes b_n, a_2 \otimes b_1, \ldots, a_2 \otimes b_n, \ldots, a_m \otimes b_1, \ldots, a_m \otimes b_n\}$$

*then*

$$[u \otimes v]_\gamma = [u]_\alpha \underline{\otimes} [v]_\beta$$

*for all $u \in U$, $v \in V$, where $\underline{\otimes}$ is the Kronecker product.*

*Proof.* Define isomorphisms $S : \mathbb{F}\{1, \ldots, m\} \to U$ and $T : \mathbb{F}\{1, \ldots, n\} \to V$ by $S\,|i\rangle = a_i$ and $T\,|j\rangle = b_j$, respectively. Then

$$S \otimes T : \mathbb{F}\{1, \ldots, m\} \otimes \mathbb{F}\{1, \ldots, n\} \to U \otimes V$$

is an isomorphism. Composing with the isomorphism

$$\mathbb{F}\{1, \ldots, m\} \underline{\otimes} \mathbb{F}\{1, \ldots, n\} \to \mathbb{F}\{1, \ldots, m\} \otimes \mathbb{F}\{1, \ldots, n\}$$

from Proposition 8.2.6, we get an isomorphism

$$I : \mathbb{F}\{1, \ldots, m\} \underline{\otimes} \mathbb{F}\{1, \ldots, n\} \to U \otimes V$$

sending $|i,j\rangle \mapsto S|i\rangle \otimes T|j\rangle = a_i \otimes b_j$. Since $\{|i,j\rangle : 1 \le i \le m, 1 \le j \le n\}$ is a basis for $\mathbb{F}\{1,\ldots,m\} \underline{\otimes} \mathbb{F}\{1,\ldots,n\}$, and $\gamma$ is the image of this basis through $I$, $\gamma$ must be a basis for $U \otimes V$.

If $u = \sum u_i a_i \in U$ and $v = \sum v_j b_j \in V$, then by bilinearity of the tensor product map, $u \otimes v = \sum u_i v_j a_i \otimes b_j$. So with the lexicographic order,

$$[u \otimes v]_\gamma = \begin{pmatrix} u_1 v \\ u_2 v \\ \vdots \\ u_m v \end{pmatrix} = [u]_\alpha \underline{\otimes} [v]_\beta.$$

□

**Example 8.3.7.** *Let $\alpha = \{e_1,\ldots,e_m\}$ be the standard basis for $\mathbb{C}^m$, and let $\beta = \{f_1,\ldots,f_n\}$ be the standard basis for $\mathbb{C}^n$. Let*

$$\gamma = \{e_i \otimes f_j : 1 \le i \le m, 1 \le j \le n\},$$

*ordered in lexicographic order. Since $\gamma$ is a basis for $\mathbb{C}^m \otimes \mathbb{C}^n$, we get an isomorphism*

$$C : \mathbb{C}^m \otimes \mathbb{C}^n \to \mathbb{C}^{mn} : w \mapsto [w]_\gamma$$

*of $\mathbb{C}^m \otimes \mathbb{C}^n$ with $\mathbb{C}^{mn}$. This isomorphism identifies $u \otimes v$ with $[u]_\alpha \underline{\otimes} [v]_\beta$, and in particular, identifies $e_i \underline{\otimes} f_j$ with $g_{(i-1)n+j}$, where $g_k$ is the $k$th standard basis vector of $\mathbb{C}^{mn}$. For this reason, $\mathbb{C}^m \otimes \mathbb{C}^n$ is often identified with $\mathbb{C}^{mn}$, and $e_i \otimes f_j$ is identified with $g_{(i-1)n+j}$.*

Given $S : U_1 \to V_1$ and $T : U_2 \to V_2$, we might like to know the matrix of $S \otimes T$ in some basis. If we choose bases for $U_1 \otimes U_2$ and $V_1 \otimes V_2$ appropriately, then there is a nice formula for this matrix.

**Definition 8.3.8.** *If $A$ is an $m_1 \times n_1$ matrix, and $B$ is an $m_2 \times n_2$ matrix, then the **Kronecker product** $A \underline{\otimes} B$ is the $m_1 m_2 \times n_1 n_2$ matrix with block form*

$$\begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1n_1}B \\ A_{21}B & A_{22}B & \cdots & A_{2n_1}B \\ & \vdots & & \\ A_{m_1 1}B & A_{m_1 2}B & \cdots & A_{m_1 n_1}B \end{pmatrix}$$

In other words, the Kronecker product replaces the $ij$th entry of $A$ with the block matrix $A_{ij}B$.

**Proposition 8.3.9.** *Let $T_i : U_i \to V_i$ be a linear map, $i = 1, 2$. Let $\alpha_i = \{a_{i1}, \dots, a_{in_i}\}$ be a basis for $U_i$, $i = 1, 2$, and let $\beta_i = \{b_{i1}, \dots, b_{im_i}\}$ be a basis for $V_i$, $i = 1, 2$. Let $\alpha$ and $\beta$ be the bases*

$$\alpha = \{a_{1j_1} \otimes a_{2j_2} : 1 \leq j_1 \leq n_1, 1 \leq j_2 \leq n_2\}$$

*and*

$$\beta = \{b_{1i_1} \otimes b_{2i_2} : 1 \leq i_1 \leq m_1, 1 \leq i_2 \leq m_2\}$$

*of $U_1 \otimes U_2$ and $V_1 \otimes V_2$ respectively. Order $\alpha$ and $\beta$ lexicographically. Then*

$$[T_1 \otimes T_2]_{\beta,\alpha} = [T_1]_{\beta_1,\alpha_1} \underline{\otimes} [T_2]_{\beta_2,\alpha_2}.$$

*Proof.* Let $A = [T_1]_{\beta_1,\alpha_1}$, $B = [T_2]_{\beta_2,\alpha_2}$, and $C = [T_1 \otimes T_2]_{\beta,\alpha}$. Note that $A$ is an $m_1 \times n_1$ matrix, $B$ is an $m_2 \times n_2$ matrix, and $C$ is an $m_1 m_2 \times n_1 n_2$ matrix. Suppose we are given $1 \leq i \leq m_1 m_2$ and $1 \leq j \leq n_1 n_2$. Then $i$ can be written uniquely as $(i_1 - 1)m_2 + i_2$ for some $1 \leq i_1 \leq m_1$ and $1 \leq i_2 \leq m_2$, and $j$ can be written uniquely as $(j_1 - 1)n_2 + j_2$ for some $1 \leq j_1 \leq n_1$, and $1 \leq j_2 \leq n_2$. The $ij$th entry of $A \underline{\otimes} B$ is $A_{i_1 j_1} B_{i_2 j_2}$. So we want to show that $C_{ij} = A_{i_1 j_1} B_{i_2 j_2}$.

For this, note that the $i$th element of $\beta$ is $b_{1i_1} \otimes b_{2i_2}$ and the $j$th element of $\alpha$ is $a_{1j_1} \otimes a_{2j_2}$. Now if $e_j$ is the $j$th standard basis vector in $\mathbb{F}^{n_1 n_2}$, then

$$\begin{aligned} Ce_j &= [T_1 \otimes T_2]_{\beta,\alpha}[a_{1j_1} \otimes a_{2j_2}]_\alpha = [(T_1 \otimes T_2)(a_{1j_1} \otimes a_{2j_2})]_\beta \\ &= [T_1(a_{1j_1}) \otimes T_2(a_{2j_2})]_\beta = [T_1(a_{1j_1})]_{\beta_1} \underline{\otimes} [T_2(a_{2j_2})]_{\beta_2} \\ &= [T_1]_{\beta_1,\alpha_1}[a_{1j_1}]_{\alpha_1} \underline{\otimes} [T_2]_{\beta_2,\alpha_2}[a_{1j_2}]_{\alpha_2} = Ae_{j_1} \otimes Be_{j_2}. \end{aligned}$$

From the definition of the Kronecker product of vectors, we see that if $u \in \mathbb{F}^{m_1}$, $v \in \mathbb{F}^{m_2}$, then the $i$th entry of $u \underline{\otimes} v$ is $u_{i_1} v_{i_2}$. The $i_1$th entry of $Ae_{j_1}$ is $A_{i_1 j_1}$, and the $i_2$th entry of $Be_{j_2}$ is $B_{i_2 j_2}$, so we see that $C_{ij} = A_{i_1 j_1} B_{i_2 j_2}$ as required. □

**Corollary 8.3.10.** *If $A$ is an $m_1 \times n_1$ matrix, $B$ is an $m_2 \times n_2$ matrix, $u \in \mathbb{F}^{n_1}$, and $v \in \mathbb{F}^{n_2}$, then*

$$(A \underline{\otimes} B)(u \underline{\otimes} v) = Au \underline{\otimes} Bv.$$

It's not too hard to prove Corollary 8.3.10 directly, but it's more convenient to use Proposition 8.3.9.

*Proof.* Let $U_i = \mathbb{F}^{n_i}$, $V_i = \mathbb{F}^{m_i}$, $i = 1, 2$. Let $\alpha_i$ and $\beta_i$ be the standard bases of $\mathbb{F}^{n_i}$ and $\mathbb{F}^{m_i}$ respectively, $i = 1, 2$. Define linear transformations

$$T_1 : \mathbb{F}^{n_1} \to \mathbb{F}^{m_1} : u \mapsto Au$$

and

$$T_2 : \mathbb{F}^{n_2} \to \mathbb{F}^{m_2} : v \mapsto Bv.$$

Let $\alpha$ and $\beta$ be the bases of $U_1 \otimes U_2$ and $V_1 \otimes V_2$ from the previous proposition. If $u \in \mathbb{F}^{n_1}$, $v \in \mathbb{F}^{n_2}$, then

$$\begin{aligned}
(A \underline{\otimes} B)(u \underline{\otimes} v) &= ([T_1]_{\beta_1,\alpha_1} \underline{\otimes} [T_2]_{\beta_2,\alpha_2})([u]_{\alpha_1} \underline{\otimes} [v]_{\alpha_2}) \\
&= [T_1 \otimes T_2]_{\beta,\alpha}[u \otimes v]_{\alpha} \\
&= [(T_1 \otimes T_2)(u \otimes v)]_{\beta} = [T_1(u) \otimes T_2(v)]_{\beta} = [Au \otimes Bv]_{\beta} \\
&= [Au]_{\beta_1} \underline{\otimes} [Bv]_{\beta_2} = Au \underline{\otimes} Bv.
\end{aligned}$$

□

**Exercise 8.3.11.** *Use Propositions 8.3.4 and 8.3.9 and Exercise 2.1.21 to show that if $A_i$ is an $m_i \times n_i$ matrix and $B_i$ is an $n_i \times k_i$ matrix, $i = 1, 2$, then*

$$(A_1 \underline{\otimes} A_2)(B_1 \underline{\otimes} B_2) = A_1B_1 \underline{\otimes} A_2B_2.$$

# Chapter 9

# Natural properties of tensor products

The abstract tensor product gives us a way to define the tensor product without picking a basis. In this section we go through some of the important properties of the abstract tensor product. The properties that we look at in this chapter are all properties that we can define without picking a basis for our spaces. Properties like this are sometimes called natural properties. We explain a little more about this term as we go.

## 9.1 Basic properties

To start, observe that for any finite-dimensional $\mathbb{F}$-vector space $V$, $\dim V \otimes \mathbb{F} = (\dim V)(\dim \mathbb{F}) = \dim V$, since $\dim \mathbb{F} = 1$ (it's helpful to remember that $\mathbb{F}$ is the special case of $\mathbb{F}^n$ with $n = 1$). Since $V \otimes \mathbb{F}$ and $V$ have the same dimension, they must be isomorphic. Our first property is that there is a nice choice of isomorphism between these two spaces.

**Proposition 9.1.1.** *Let $V$ be a vector space. Then there is a unique isomorphism*

$$\phi : V \otimes \mathbb{F} \to V$$

*such that $\phi(v \otimes \lambda) = \lambda v$ for all $\lambda \in \mathbb{F}$ and $v \in V$.*

*Proof.* It's easy to check that the map

$$T : V \times \mathbb{F} \to V : (v, \lambda) \mapsto \lambda v$$

is bilinear. Thus by the universal property of tensor products, there is a linear map $\phi : V \otimes \mathbb{F} \to V$ such that $\phi(v \otimes \lambda) = \lambda v$. If $\{v_i\}$ is a basis for $V$, then

$\{v_i \otimes 1\}$ is a basis for $V \otimes \mathbb{F}$, and $\phi(v_i \otimes 1) = v_i$, so $\phi$ sends a basis for $V \otimes \mathbb{F}$ to a basis for $V$, and hence is an isomorphism. (We could also argue that $\phi$ is an isomorphism using a dimension argument, but this argument works even for infinite-dimensional spaces.)

If $\phi' : V \otimes \mathbb{F} \to V$ is another isomorphism with $\phi(v \otimes \lambda) = \lambda v$ for all $\lambda \in \mathbb{F}$, $v \in V$, then $\phi'$ and $\phi$ agree on a spanning set of $V \otimes \mathbb{F}$, and hence $\phi = \phi'$. □

Suppose $V$ and $W$ are two spaces with $\dim V = \dim W$, so that $V \cong W$. To get an isomorphism between $V$ and $W$, we can pick bases $\{v_i\}$ and $\{w_i\}$ for $V$ and $W$ respectively, and then take the linear map sending $v_i \mapsto w_i$. This gives us many choices of isomorphism. The isomorphism $\phi$ between $V \otimes \mathbb{F}$ and $V$ is nice because we can identify $\phi$ without picking a basis for $V$—indeed, the proposition tells us that $\phi$ is the unique isomorphism with $\phi(v \otimes \lambda) = \lambda v$. Because we can specify $\phi$ without picking a basis for $V$, we say that $V \otimes \mathbb{F}$ and $V$ are *naturally isomorphic.* This term has a formal definition in category theory, which is actually a bit more involved than just being able to specify $\phi$ without picking a basis. Although the category theoretic definition is beyond the scope of this course, natural isomorphisms are an important concept in higher mathematics, so it's nice to get some intuition for this concept now. With that in mind, let's prove that the isomorphisms $V \otimes \mathbb{F} \to V$ are naturally isomorphic (even though we don't have the definition of this term):

**Corollary 9.1.2.** *For any vector space $V$, let $\phi_V : V \otimes \mathbb{F} \to V$ be the isomorphism from Proposition 9.1.1. If $T : V \to W$ is a linear map, then the diagram*

$$\begin{tikzcd}
V \otimes \mathbb{F} \arrow[r, "\phi_V"] \arrow[d, "T \otimes \mathbb{1}"'] & V \arrow[d, "T"] \\
W \otimes \mathbb{F} \arrow[r, "\phi_W"'] & W
\end{tikzcd}$$

*commutes, meaning that $\phi_W \circ (T \otimes \mathbb{1}) = T \circ \phi_V$.*

*Proof.* If $v \otimes \lambda \in V \otimes \mathbb{F}$, then

$$T(\phi_V(v \otimes \lambda)) = T(\lambda v) = \lambda T(v),$$

while

$$\phi_W((T \otimes \mathbb{1})(v \otimes \lambda)) = \phi_W(Tv \otimes \lambda) = \lambda T(v).$$

So $\phi_W \circ (T \otimes \mathbb{1}) = T \circ \phi_V$ on $V \otimes \mathbb{F}$. □

So the idea is that we can change $V$ to $W$ by an arbitrary linear map, but it doesn't matter if we apply $\phi_V$ and then apply $T$, or apply $T \otimes \mathbb{1}$ and then apply $\phi_W$. Hence we say that $\phi_V$ is *natural*—it does the same thing no matter how we change the space.

All the properties we look at in this section are natural in this sense. For instance, we can compare $V \otimes W$ and $W \otimes V$. Again, these two spaces both have dimension $(\dim V)(\dim W)$, so we know they are isomorphic. However, we can again specify a swap isomorphism without choosing a basis:

**Proposition 9.1.3.** *Let $V$ and $W$ be vector spaces. Then there is a unique isomorphism*

$$\phi : V \otimes W \to W \otimes V$$

*such that $\phi(v \otimes w) = w \otimes v$ for all $v \in V$, $w \in W$.*

This proof is a good exercise to try yourself:

**Exercise 9.1.4.** *Prove Proposition 9.1.3.*

Once again, if we let $\phi_{V,W}$ be the isomorphism from Proposition 9.1.3, and let $S : V \to V'$ and $T : W \to W'$ be linear maps, then we find that the diagram

$$\begin{tikzcd}
V \otimes W \arrow[r, "\phi_{V,W}"] \arrow[d, "S \otimes T"'] & W \otimes V \arrow[d, "T \otimes S"] \\
V' \otimes W' \arrow[r, "\phi_{V',W'}"'] & W' \otimes V'
\end{tikzcd}$$

commutes, so $\phi_{V,W}$ is a natural isomorphism. However, to avoid going off track we'll leave proving this as an exercise as well, and focus on the basis independence aspect of natural isomorphisms in the rest of this section.

One of the most important instances of this phenomenon occurs when we take tensor products of three or more vector spaces:

**Proposition 9.1.5.** *Let $U$, $V$, and $W$ be vector spaces. Then there is a unique isomorphism*

$$\phi : U \otimes (V \otimes W) \to (U \otimes V) \otimes W$$

*such that $\phi(u \otimes (v \otimes w)) = (u \otimes v) \otimes w$ for all $u \in U$, $v \in V$, $w \in W$.*

*Proof.* Pick bases $\{u_i : i \in I\}$, $\{v_j : j \in J\}$, and $\{w_k : k \in K\}$ for $U$, $V$, and $W$. Then

$$\{v_j \otimes w_k : (j,k) \in J \times K\}$$

is a basis for $V \otimes W$, so

$$\{u_i \otimes (v_j \otimes w_k) : (i,j,k) \in I \times J \times K\}$$

is a basis for $U \otimes (V \otimes W)$. Similarly

$$\{(u_i \otimes v_j) \otimes w_k : (i,j,k) \in I \times J \times K\}$$

is a basis for $(U \otimes V) \otimes W$. So we can define an isomorphism

$$\phi : U \otimes (V \otimes W) \to (U \otimes V) \otimes W$$

sending $u_i \otimes (v_j \otimes w_k) \mapsto (u_i \otimes v_j) \otimes w_k$ for all $i \in I$, $j \in J$, $k \in K$.

Suppose $u \in U$, $v \in V$, $w \in W$. Then $u = \sum a_i u_i$, $v = \sum b_j v_j$, and $w = \sum c_k w_k$, so

$$\phi(u \otimes (v \otimes w)) = \phi(\sum_{i,j,k} a_i b_j c_k u_i \otimes (v_j \otimes w_k)) = \sum_{i,j,k} a_i b_j c_k (u_i \otimes v_j) \otimes w_k = (u \otimes v) \otimes w.$$

If $\phi'$ is another isomorphism with $\phi'(u \otimes (v \otimes w)) = (u \otimes v) \otimes w$ for all $u \in U$, $v \in V$, $w \in W$, then $\phi$ and $\phi'$ agree on a spanning set for $U \otimes (V \otimes W)$, so $\phi = \phi'$. □

Notice that to prove Proposition 9.1.5, we pick a basis for $U$, $V$, and $W$. This doesn't mean that the isomorphism we construct isn't natural; the important point is that $\phi$ is uniquely identified without having to pick a basis (in particular, we'll get the same isomorphism no what basis we pick in the proof). In many cases, even if we can construct $\phi$ without picking a basis, it's faster just to define the isomorphism on a basis, and then show that the map we construct satisfies the required property.

Suppose that we have four spaces, $U_1$, $U_2$, $U_3$, and $U_4$. Then Proposition 9.1.5 shows that there are unique isomorphisms

$$((U_1 \otimes U_2) \otimes U_3) \otimes U_4 \cong (U_1 \otimes U_2) \otimes (U_3 \otimes U_4) \cong U_1 \otimes (U_2 \otimes (U_3 \otimes U_4))$$

identifying

$$((u_1 \otimes u_2) \otimes u_3) \otimes u_4 \cong (u_1 \otimes u_2) \otimes (u_3 \otimes u_4) \cong u_1 \otimes (u_2 \otimes (u_3 \otimes u_4)),$$

and we can identify every other tensor product of $U_1$, $U_2$, $U_3$, and $U_4$ in this order in the same way. In general, all the possible ways of tensoring $U_1, \ldots, U_k$ together (in the specified order) are naturally isomorphic. As a result, we think of these spaces as being equal, and write them without the braces as

$$U_1 \otimes U_2 \otimes \cdots \otimes U_k.$$

Similarly, the tensor product of vectors $u_1, \ldots, u_k$, where $u_i \in U_i$, is written without the brackets as $u_1 \otimes \cdots \otimes u_k$.

## 9.2 The space of linear transformations

One of the most useful properties of tensor products is that we can express the space of linear transformations from $V$ to $W$ as a tensor product.

**Proposition 9.2.1.** *Let $V, W$ be finite-dimensional vector spaces. Then there is a unique isomorphism*

$$\phi : W \otimes V^* \to \mathrm{Lin}(V, W)$$

*such that $\phi(w \otimes f)(v) = f(v)w$ for all $f \in V^*$, $v \in V$, $w \in W$.*

*Furthermore, if $\alpha$ is a basis for $V$ and $\beta$ is a basis for $W$, then*

$$[\phi(w \otimes f)]_{\beta,\alpha} = [w]_\beta [f]_{\{1\},\alpha}$$

*for all $w \in W$, $f \in V^*$.*

By default, we assume that $V$ and $W$ are finite-dimensional in this text. However, we include it as a hypothesis here to emphasis that Proposition 9.2.1, and many of the other propositions in this section, do not necessarily hold in infinite-dimensional spaces.

*Proof.* First suppose $f \in V^*$, $w \in W$. Let

$$T_{f,w} : V \to W : v \mapsto f(v)w.$$

If $u, v \in V$, $\lambda \in \mathbb{F}$, then

$$T_{f,w}(\lambda u + v) = f(\lambda u + v)w = \lambda f(u)w + f(v)w, = \lambda T_{f,w}(u) + T_{f,w}(v).$$

So $T_{f,w}$ is linear. Furthermore, if $\lambda \in \mathbb{F}$, $f, g \in V^*$, $w \in W$, then

$$T_{\lambda f+g,w}(v) = (\lambda f + g)(v)(w) = \lambda f(v)w + g(v)(w) = \lambda T_{f,w}(v) + \lambda T_{g,w}(v)$$

for all $v \in V$. So $T_{\lambda f+g,w} = \lambda T_{f,w} + T_{g,w}$. Similarly,

$$T_{f,\lambda u+w} = \lambda T_{f,u} + T_{f,w}$$

for all $f \in V^*$, $u, w \in W$, $\lambda \in \mathbb{F}$. So the function

$$W \times V^* \to \mathrm{Lin}(V, W) : (w, f) \mapsto T_{f,w}$$

is bilinear. By the universal property of tensor products, there is a linear map

$$\phi : W \otimes V^* \to \mathrm{Lin}(V, W)$$

such that $\phi(w \otimes f) = T_{f,w}$ for all $f \in V^*$, $w \in W$.

To see that $\phi$ is an isomorphism, observe that

$$\dim W \otimes V^* = (\dim W)(\dim V^*) = (\dim W)(\dim V) = \dim \mathrm{Lin}(V, W).$$

So it suffices to show that $\phi$ is injective. Suppose $\alpha = \{a_1, \dots, a_n\}$ is a basis for $V$ and $\beta = \{b_1, \dots, b_m\}$ is a basis for $W$. Let $\{a^1, \dots, a^n\}$ be the dual basis for $V^*$. Then

$$\{b_j \otimes a^i : 1 \le j \le m, 1 \le i \le n\}$$

is a basis for $W \otimes V^*$. Suppose $T \in W \otimes V^*$ is an element with $\phi(T) = 0$. Let $T = \sum_{i,j} c_{i,j} b_j \otimes a^i$. Then

$$0 = \phi(T)(a_k) = \sum_{i,j} c_{i,j} \phi(b_j \otimes a^i)(a_k) = \sum_{i,j} c_{i,j} a^i(a_k) b_j = \sum_j c_{k,j} b_j.$$

Because the elements of $\beta$ are linearly independent, we must have $c_{k,j} = 0$ for all $j$. But then $c_{k,j} = 0$ for all $k$ and $j$, so $T = 0$. We conclude that $\phi$ is injective.

If $w \in W$, $f \in V^*$, then

$$[w]_\beta [f]_{\{1\},\alpha} [v]_\alpha = f(v)[w]_\beta = [\phi(w \otimes f)(v)]_\beta = [\phi(w \otimes f)]_{\beta,\alpha} [v]_\alpha$$

for all $v \in V$, so

$$[\phi(w \otimes f)]_{\beta,\alpha} = [w]_\beta [f]_{\{1\},\alpha}.$$

Finally, if $\phi' : W \otimes V^* \to \mathrm{Lin}(V, W)$ is another function with the same property, then $\phi(w \otimes f)(v) = \phi'(w \otimes f)(v)$ for all $v \in V$, $w \in W$, and $f \in V^*$. Hence $\phi(w \otimes f) = \phi'(w \otimes f)$ for all $w \in W$ and $f \in V^*$, and thus $\phi = \phi'$ as they agree on a spanning set. □

**Example 9.2.2.** *Recall that if $|\psi\rangle \in H = \mathbb{F}\{0,1\}$, then $\langle\psi| \in H^*$ is the function sending $|\phi\rangle \mapsto \langle\psi|\phi\rangle$. If $|\phi\rangle \in H'$, then Proposition 9.2.1 tells us that $|\phi\rangle \otimes \langle\psi|$ denotes an element of $\mathrm{Lin}(H, H')$. Usually we drop the tensor product and just write $|\phi\rangle\langle\psi|$ for this element.*

*For instance, let $H = H' = \mathbb{F}\{0,1\}$. Then $|0\rangle\langle 1|$ sends*

$$|0\rangle \mapsto \langle 1|0\rangle\,|0\rangle = 0 \text{ and } |1\rangle \mapsto \langle 1|1\rangle\,|0\rangle = |0\rangle .$$

*Similarly $|1\rangle\langle 0|$ sends*

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

*and $|1\rangle\langle 0| + |0\rangle\langle 1|$ sends*

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

If $T \in \mathrm{Lin}(V, W)$ and $S \in \mathrm{Lin}(U, V)$ for vector spaces $U, V, W$, then we can compose $T$ and $S$ to get $T \circ S \in \mathrm{Lin}(U, W)$. What if we represent $T$ and $S$ as elements of $W \otimes V^*$ and $V \otimes U^*$? Can we compute this composition in terms of these representations? It turns out there is a natural way to do this:

**Exercise 9.2.3.** *Let $\phi_{U,V} : \mathrm{Lin}(U, V) \to V \otimes U^*$, $\phi_{V,W} : \mathrm{Lin}(V, W) \to W \otimes V^*$, and $\phi_{U,W} : \mathrm{Lin}(U, W) \to W \otimes U^*$ be the natural isomorphisms from Proposition 9.2.1.*

*(a) Show that $\phi_{U,W}(T \circ S) = (T \otimes \mathbb{1})\phi_{U,V}(S)$.*

*(b) Suppose $U$, $V$, and $W$ are Hilbert spaces, and that*

$$\phi_{U,V}(S) = \sum_{i=1}^{m} |v_i\rangle \otimes \langle u_i| , \quad \phi_{V,W}(T) = \sum_{i=1}^{n} |w_j\rangle \otimes \langle x_j|$$

*for some vectors $|u_i\rangle \in U$, $|v_i\rangle , |x_j\rangle \in V$, and $|w_j\rangle \in W$. Show that*

$$\phi_{U,W}(T \circ S) = \sum_{i,j} \langle x_j|v_i\rangle\,|w_j\rangle \otimes \langle u_i| .$$

**Example 9.2.4.** *Let $H = \mathbb{C}\{0,1\}$, and suppose $T : H \to H$ is the linear operator sending $|0\rangle \mapsto |+\rangle$ and $|1\rangle \mapsto |-\rangle$. Let $S : H \to H$ be the linear operator sending $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$. In $H \otimes H^*$, $T$ corresponds to $|+\rangle\langle 0| + |-\rangle\langle 1|$ and $S$ corresponds to $|1\rangle\langle 0| + |0\rangle\langle 1|$. To compute $T \circ S$ in $H \otimes H^*$, we can either take*

$$(T \otimes \mathbb{1})(|1\rangle\langle 0| + |0\rangle\langle 1|) = |-\rangle\,|0\rangle + |+\rangle\,|1\rangle ,$$

*or*

$$\langle 0|1\rangle\,|+\rangle\langle 0| + \langle 0|0\rangle\,|+\rangle\langle 1| + \langle 1|1\rangle\,|-\rangle\langle 0| + \langle 1|0\rangle\,|-\rangle\langle 1| = |-\rangle\langle 0| + |+\rangle\langle 1| .$$

*We get the same thing in either case.*

## 9.3 Dual spaces

**Proposition 9.3.1.** *Let $V$, $W$ be finite-dimensional vector spaces. Then there is a unique isomorphism*

$$\phi : V^* \otimes W^* \to (V \otimes W)^*$$

*such that $\phi(f \otimes g)(v \otimes w) = f(v)g(w)$ for all $f \in V^*$, $g \in W^*$, $v \in V$, $w \in W$.*

*Proof.* Suppose $f \in V^*$, $g \in W^*$. Then the map

$$V \times W \to \mathbb{F} : (v, w) \mapsto f(v)g(w)$$

is bilinear. So by the universal property of tensor products, there is a unique linear function $T_{f,g} : V \otimes W \to \mathbb{F}$ such that $T_{f,g}(v \otimes w) = f(v)g(w)$. It's not hard to check that the map

$$V^* \times W^* \to (V \otimes W)^* : (f, g) \mapsto T_{f,g}$$

is bilinear. So we get a linear map

$$\phi : V^* \otimes W^* \to (V \otimes W)^*$$

such that $\phi(f \otimes g) = T_{f,g}$, or in other words such that

$$\phi(f \otimes g)(v \otimes w) = f(v)g(w).$$

Let $\{e_i\}$ be a basis for $V$ and $\{f_j\}$ be a basis for $W$. Let $\{e^i\}$ and $\{f^j\}$ be the corresponding dual bases. Then

$$\phi(e^i \otimes f^j)(e_k \otimes f_l) = e^i(e_k)f^j(f_l) = \delta_{ik}\delta_{jl} = \delta_{(i,j),(k,l)}.$$

So $\phi$ sends the basis $\{e^i \otimes f^j\}$ for $V^* \otimes W^*$ to the dual basis for the basis $\{e_i \otimes f_j\}$ of $V \otimes W$. Thus $\phi$ is an isomorphism. □

**Example 9.3.2.** *Recall that if $|\psi\rangle \in H = \mathbb{C}\{0, 1\}$, then $\langle\psi| \in H^*$ is the function sending $|\phi\rangle \mapsto \langle\psi|\phi\rangle$. If $\langle\psi_1| , \langle\psi_2| \in H^*$, then $\langle\psi_1| \otimes \langle\psi_2|$ represents the element of $H_1 \otimes H_2$ which sends $|\phi_1\rangle \otimes |\phi_2\rangle$ to $\langle\psi_1|\phi_1\rangle \langle\psi_2|\phi_2\rangle$.*

*Usually we just drop the brackets and write*

$$\langle\psi_1| \langle\psi_2| |\phi_1\rangle |\phi_2\rangle = \langle\psi_1|\phi_1\rangle \langle\psi_2|\phi_2\rangle .$$

By the universal property of tensor products, for every bilinear map $T : U \times V \to W$ there is a corresponding unique linear map $\tilde{T} : U \otimes V \to W$. In fact, this is another example of a natural isomorphism:

**Exercise 9.3.3.** *Let* $\mathrm{Bilin}(U, V; W)$ *be the set of bilinear maps* $U \times V \to W$*.*

*(a) Show that* $\mathrm{Bilin}(U, V; W)$ *is a subspace of* $\mathrm{Fun}(U \times V, W)$*, and hence a vector space in its own right.*

*(b) Show that the function* $\mathrm{Bilin}(U, V; W) \to \mathrm{Lin}(U \otimes V; W)$ *sending a bilinear function* $T$ *to the unique linear fuction* $\tilde{T}$ *with* $T(u, v) = \tilde{T}(u \otimes v)$ *for all* $u \in U$*,* $v \in V$ *is an isomorphism.*

Taking $W = \mathbb{F}$, Exercise 9.3.3 shows that $(U \otimes V)^*$ is isomorphic to the space of bilinear maps $U \times V \to \mathbb{F}$. By Proposition 9.3.1, $U^* \otimes V^* \cong (U \otimes V)^* \cong \mathrm{Bilin}(U, V; \mathbb{F})$. Furthermore, this isomorphism is natural, and in particular doesn't require choosing a basis for $U^*$ and $V^*$ at all. This gives us another way we could have defined tensor products, although it seemingly only applies to dual spaces: given $U^*$ and $V^*$, we could have defined $U^* \otimes V^*$ in a basis independent manner by setting $U^* \otimes V^* := \mathrm{Bilin}(U, V; \mathbb{F})$.

Could this work as a definition of general tensor products $U \otimes V$, and not just the tensor product $U^* \otimes V^*$ of dual spaces? We know that $V \cong V^*$ for any space $V$, but unfortunately the only way of getting such an isomorphism in general is by picking a basis — there is no natural isomorphism $V \to V^*$. However, it turns out there is a natural isomorphism $V \to (V^*)^*$, where the latter space is the double dual of $V$.

**Definition 9.3.4.** *Let* $V$ *be an* $\mathbb{F}$*-vector space, and suppose* $v \in V$*. The* ***evaluation function*** $\mathrm{ev}_v : V^* \to \mathbb{F}$ *sends* $f \in V^*$ *to* $\mathrm{ev}_v(f) := f(v)$*.*

**Exercise 9.3.5.** *Let* $V$ *be a vector space.*

*(a) Show that* $\mathrm{ev}_v : V^* \to \mathbb{F}$ *is linear, and hence an element of* $(V^*)^*$ *for all* $v \in V$*.*

*(b) Show that* $\mathrm{ev} : V \to (V^*)^* : v \mapsto \mathrm{ev}_v$ *is linear.*

*(c) Show that (assuming* $V$ *is finite-dimensional)* $\mathrm{ev}$ *is an isomorphism.*

Notice that we defined ev without picking a basis for $V$, and this is indeed a natural isomorphism. We need one more isomorphism: by Exercise 2.1.24, if $T : V \to W$ is an isomorphism, then $W^* \to V^* : f \mapsto f \circ T$ is an isomorphism, and (since this doesn't require picking a basis at all) if there is a natural isomorphism $V \to W$, then there is a natural isomorphism $W^* \to V^*$. Combining Exercises 2.1.24, 9.3.3, and 9.3.5, we see that there is a natural isomorphism

$$U \otimes V \cong ((U \otimes V)^*)^* \cong \mathrm{Bilin}(U, V; \mathbb{F})^*.$$

Thus the dual space $\mathrm{Bilin}(U, V; \mathbb{F})^*$ of $\mathrm{Bilin}(U, V; \mathbb{F})$ gives us a relatively concrete way of thinking of the tensor product $U \otimes V$, without having to pick bases for $U$ and $V$. This is often used as an alternative definition of $U \otimes V$.

## 9.4 Contractions and trace

A natural operation which unifies a number of constructions in tensors is **contraction**:

**Proposition 9.4.1.** *Let $V$ be an $\mathbb{F}$ vector space. Then there is a unique homomorphism*

$$C : V^* \otimes V \to \mathbb{F}$$

*such that $f \otimes v \mapsto f(v)$.*

*Proof.* The dual pairing $V^* \times V \to \mathbb{F} : (f, v) \mapsto f(v)$ is bilinear, so by the universal property of tensor products, there is a unique linear map $C : V^* \otimes V \to \mathbb{F}$ such that $C(f \otimes v) = f(v)$. □

Contraction can be used to define the linear transformation $V \to W$ corresponding to an element $W \otimes V^*$. Indeed, if $t \in W \otimes V^*$, then the linear transformation $V \to W$ corresponding to $t$ in Proposition 9.2.1 is

$$V \to W : v \mapsto \alpha(\mathbb{1} \otimes C)(t \otimes v),$$

where $\alpha : W \otimes \mathbb{F} \to W$ is the isomorphism from Proposition 9.1.1. In fact, we can go a step further:

**Exercise 9.4.2.** *Let $V, W$ be vector spaces.*

*(a) Show that*

$$m : \mathrm{Lin}(V, W) \times V \to W : (T, v) \mapsto T(v)$$

*is bilinear, and hence there is a linear map*

$$m' : \mathrm{Lin}(V, W) \otimes V \to W$$

*such that $m'(T \otimes v) = T(v)$.*

*(b) Let $\phi_{V,W} : \mathrm{Lin}(V, W) \to W \otimes V^*$ be the isomorphism from Proposition 9.2.1, and let $\alpha : W \otimes \mathbb{F} \to W$ be the isomorphism from Proposition 9.1.1. Show that $m' = \alpha \circ (\mathbb{1} \otimes C) \circ (\phi_{V,W} \otimes \mathbb{1})$, where $C : V^* \otimes V \to \mathbb{F}$ is contraction.*

For the same reason, contraction is closely related to the formula from Exercise 9.2.3 for composition of linear transformation in terms of tensors. In fact, we can repeat Exercise 9.4.2 for multiplication of linear transformations.

**Exercise 9.4.3.** *Let $U, V, W$ be vector spaces, and let $\phi_{U,V} : \mathrm{Lin}(U, V) \to V \otimes U^*$, $\phi_{V,W} : \mathrm{Lin}(V, W) \to W \otimes V^*$, and $\phi_{U,W} : \mathrm{Lin}(U, W) \to W \otimes U^*$ be the natural isomorphisms from Proposition 9.2.1. Let $\alpha : W \otimes \mathbb{F} \to W$ be the isomorphism from Proposition 9.1.1.*

*(a) Show that the function*

$$m : \mathrm{Lin}(V, W) \times \mathrm{Lin}(U, V) \to \mathrm{Lin}(U, W) : (T, S) \mapsto T \circ S$$

*is bilinear, and hence there is a linear map*

$$m' : \mathrm{Lin}(V, W) \otimes \mathrm{Lin}(U, V) \to \mathrm{Lin}(U, W)$$

*such that $m'(T \otimes S) = T \circ S$.*

*(b) Show that*

$$\phi_{U,W} \circ m' = (\alpha \otimes \mathbb{1})(\mathbb{1} \otimes C \otimes \mathbb{1})(\phi_{V,W} \otimes \phi_{U,V}).$$

In other words, part (b) of Exercise 9.4.3 states that if $T \in \mathrm{Lin}(V, W)$, $S \in \mathrm{Lin}(U, V)$, then

$$\phi_{U,W}(T \circ S) = (\alpha \otimes \mathbb{1})(\mathbb{1} \otimes C \otimes \mathbb{1})\phi_{V,W}(T) \otimes \phi_{U,V}(S).$$

We can also use contraction and the dual pairing between $(V \otimes W)^* \otimes (V \otimes W)$. Now that we've had two exercises to show the pattern, it's worth trying to formulate this connection yourself:

**Exercise 9.4.4.** *Following the pattern in Exercises 9.4.2 and 9.4.3, show that there is a way to express the dual pairing $(V \otimes W)^* \otimes (V \otimes W) \to \mathbb{F}$ using contraction and other natural maps.*

Although these are all important uses of contraction, we'll be interested in contraction for a different reason: its connection with trace.

**Definition 9.4.5.** *The **trace** of an $n \times n$ matrix $M$ is*

$$\mathrm{tr}(M) = \sum_{i=1}^{n} M_{ii}.$$

*The **trace** of a linear transformation $T : V \to V$ is*

$$\mathrm{tr}\, T = \mathrm{tr}[T]_{\mathcal{B},\mathcal{B}},$$

*where $\mathcal{B}$ is a basis of $V$.*

Suppose $\mathcal{B} = \{v_1, \dots, v_n\}$, and let $\mathcal{B}' = \{v^1, \dots, v^n\}$ be the dual basis to $\mathcal{B}$. Because

$$([T]_{\mathcal{B},\mathcal{B}})_{ii} = v^i(T(v_i)),$$

we can also write the trace of $T$ without using the matrix of $T$ as

$$\operatorname{tr} T = \sum_{i=1}^{n} v^i(T(v_i)).$$

However, this still requires picking a basis $\mathcal{B}$ for $V$. To show that the trace of a linear transformation is well-defined, we need to show that this formula doesn't depend on the choice of basis for $V$:

**Exercise 9.4.6.** *Using the change of basis formula for $[T]_{\mathcal{B},\mathcal{B}}$, as well as the fact that the trace of matrices satisfies $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, show that $\operatorname{tr} T$ does not depend on the choice of basis $\mathcal{B}$.*

Although this is a valid strategy for showing that the trace of a linear transformation is well-defined, it doesn't explain *why* the formula for the trace is independent of the choice of basis. So we might ask, is there a natural (aka. basis independent) formula for the trace? It turns out that we can get such a formula by combining contraction with the swap isomorphism:

**Proposition 9.4.7.** *Let $V$ be a vector space, let $C : V^* \otimes V \to \mathbb{F}$ be contraction, let $S : V \otimes V^* \to V^* \otimes V$ be the swap isomorphism from Proposition 9.1.3, and let $\phi : \operatorname{Lin}(V, V) \to V \otimes V^*$ be the isomorphism from Proposition 9.2.1. Then*

$$\operatorname{tr}(T) = C \circ S \circ \phi(T).$$

*Proof.* Suppose $\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis for $V$, and let $\mathcal{B} = \{v^1, \dots, v^n\}$ be the dual basis of $V^*$. Then $\{v_j \otimes v^\ell : 1 \le j, \ell \le n\}$ is a basis for $V \otimes V^*$. Suppose

$$\phi(T) = \sum_{1 \le j,\ell \le n} a_{j\ell} v_j \otimes v^\ell.$$

Then

$$T(v_i) = \sum_{1 \le j,\ell \le n} a_{j\ell} v^\ell(v_i) v_j = \sum_{j=1}^{n} a_{ji} v_j,$$

so

$$v^i(T(v_i)) = a_{ii}, \text{ and } \operatorname{tr}(T) = \sum_{i=1}^{n} a_{ii}.$$

But

$$C(S(\phi(T))) = C\left(\sum_{1\leq j,\ell\leq n} a_{j\ell} v^{\ell} \otimes v_j\right) = \sum_{1\leq j,\ell\leq n} a_{j\ell} v^{\ell}(v_j) = \sum_{j=1}^{n} a_{jj} = \operatorname{tr}(T).$$

□

Breaking it down a bit more, the proof of Proposition 9.4.7 shows that

$$C \circ S \circ \phi(T) = \sum_{i=1}^{n} v^i(T(v_i))$$

for any basis $\mathcal{B} = \{v_1, \ldots, v_n\}$. Since the left hand side of this equation does not depend on the choice of basis $\mathcal{B}$, this gives another way to prove Exercise 9.4.6. In fact, if we wanted to we could use $C \circ S \circ \phi(T)$ as the definition of $\operatorname{tr}(T)$, and then we wouldn't have to mention bases at all.

The basis independent formula for trace is also very useful for calculations:

**Example 9.4.8.** *Suppose $H$ is a Hilbert space, and $T : H \to H$ is a linear transformation corresponding to the tensor $\sum_i |\psi_i\rangle \langle\phi_i| \in H \otimes H^*$. Then*

$$\operatorname{tr} T = CS \sum_i |\psi_i\rangle \langle\phi_i| = \sum_i C \langle\phi_i| \otimes |\psi_i\rangle = \sum_i \langle\phi_i|\psi_i\rangle .$$

It's interesting to try to derive the properties of trace from this basis independent definition. For instance, $C \circ S \circ \phi$ is a composition of linear maps, and hence $\operatorname{tr} : \operatorname{Lin}(V, V) \to \mathbb{F}$ is linear as well. Of course, this is easy to see from the definition of trace in Definition 9.4.5 as well.

The other main property of trace is that $\operatorname{tr}(AB) = \operatorname{tr}(BA)$. As mentioned in Exercise 9.4.6, this holds for the trace of matrices, and consequently this also holds for linear transformations.

**Proposition 9.4.9.** *Let $V, W$ be vector spaces, let $S \in \operatorname{Lin}(V, W)$, and let $T \in \operatorname{Lin}(W, V)$. Then*

$$\operatorname{tr}_W(ST) = \operatorname{tr}_V(TS),$$

*where $\operatorname{tr}_W$ is the trace on $\operatorname{Lin}(W, W)$ and $\operatorname{tr}_V$ is the trace on $\operatorname{Lin}(V, V)$.*

Although Proposition 9.4.9 follows immediately from the corresponding fact for the trace of matrices, we can also give a basis independent proof:

*Proof.* Let

$$m_1 : \mathrm{Lin}(V, W) \otimes \mathrm{Lin}(W, V) \to \mathrm{Lin}(W, W) : S \otimes T \mapsto S \circ T$$

and

$$m_2 : \mathrm{Lin}(W, V) \otimes \mathrm{Lin}(V, W) \to \mathrm{Lin}(V, V) : T \otimes S \mapsto T \circ S$$

be multiplication maps as in Exercise 9.4.3, part (a). For any pair of spaces $U, U'$, let $\phi_{U,U'} : \mathrm{Lin}(U, U') \to U' \otimes U^*$ be the isomorphism from Proposition 9.2.1, let $\mathrm{SWAP}_{U,U'} : U \otimes U' \to U' \otimes U$ be the swap isomorphism from Proposition 9.1.3, and let $\alpha_U : U \otimes \mathbb{F} \to U$ be the isomorphism from Proposition 9.1.1.

$$\mathrm{tr}_W \circ m_1(S \otimes T) = \mathrm{tr}_V \circ m_2(T \otimes S),$$

or in other words that

$$\mathrm{tr}_W \circ m_1 = \mathrm{tr}_V \circ m_2 \circ \mathrm{SWAP}_{\mathrm{Lin}(V,W),\mathrm{Lin}(W,V)} \tag{9.4.1}$$

as linear transformations $\mathrm{Lin}(V, W) \otimes \mathrm{Lin}(W, V) \to \mathbb{F}$.

By Proposition 9.4.7 and Exercise 9.4.3, part (b),

$$\mathrm{tr}_W \circ m_1 = C_W \circ \mathrm{SWAP}_{W,W^*} \circ \phi_{W,W} \circ m_1 = C_W \circ \mathrm{SWAP}_{W,W^*} \circ (\alpha_W \otimes \mathbb{1}) \circ (\mathbb{1} \otimes C_V \otimes \mathbb{1}) \circ (\phi_{V,W} \otimes \phi_{W,V}),$$

and similarly

$$\mathrm{tr}_V \circ m_2 = C_V \circ \mathrm{SWAP}_{V,V^*} \circ \phi_{V,V} \circ m_2 = C_V \circ \mathrm{SWAP}_{V,V^*} \circ (\alpha_V \otimes \mathbb{1}) \circ (\mathbb{1} \otimes C_W \otimes \mathbb{1}) \circ (\phi_{W,V} \otimes \phi_{V,W}).$$

Now if $S \in \mathrm{Lin}(V, W)$, $T \in \mathrm{Lin}(W, V)$, then

$$\begin{aligned}(\phi_{W,V} \otimes \phi_{V,W}) \circ \mathrm{SWAP}_{\mathrm{Lin}(V,W),\mathrm{Lin}(W,V)}(S \otimes T) &= \phi_{W,V}(T) \otimes \phi_{V,W}(S)\\ &= \mathrm{SWAP}_{W \otimes V^*, V \otimes W^*}\, \phi_{V,W}(S) \otimes \phi_{W,V}(T),\end{aligned}$$

so

$$\begin{aligned}\mathrm{tr}_V \circ m_2 \circ \mathrm{SWAP}_{\mathrm{Lin}(V,W),\mathrm{Lin}(W,V)} &= C_V \circ \mathrm{SWAP}_{V,V^*} \circ \phi_{V,V} \circ m_2 \circ \mathrm{SWAP}_{\mathrm{Lin}(V,W),\mathrm{Lin}(W,V)}\\ &= C_V \circ \mathrm{SWAP}_{V,V^*} \circ (\alpha_V \otimes \mathbb{1}) \circ (\mathbb{1} \otimes C_W \otimes \mathbb{1})\\ &\qquad \circ \mathrm{SWAP}_{W \otimes V^*, V \otimes W^*} \circ (\phi_{V,W} \otimes \phi_{W,V}).\end{aligned}$$

Multiplying on the right by $\phi_{V,W}^{-1} \otimes \phi_{W,V}^{-1}$, we see that Equation 9.4.1 holds if and only if

$$C_W \circ \mathrm{SWAP}_{W,W^*} \circ (\alpha_W \otimes \mathbb{1}) \circ (\mathbb{1} \otimes C_V \otimes \mathbb{1})$$

is equal to

$$C_V \circ \mathrm{SWAP}_{V,V^*} \circ (\alpha_V \otimes \mathbb{1}) \circ (\mathbb{1} \otimes C_W \otimes \mathbb{1}) \circ \mathrm{SWAP}_{W \otimes V^*, V \otimes W^*}$$

as linear transformations $W \otimes V^* \otimes V \otimes W^* \to \mathbb{F}$. It is enough to show that these two linear transformations are equal on a spanning set. So let $w \in W$, $f \in V^*$, $v \in V$, and $g \in W^*$. Then

$$\begin{aligned} C_W \circ \mathrm{SWAP}_{W,W^*} \circ &(\alpha_W \otimes \mathbb{1}) \circ (\mathbb{1} \otimes C_V \otimes \mathbb{1})(w \otimes f \otimes v \otimes g) \\ &= C_W \circ \mathrm{SWAP}_{W,W^*} \circ (\alpha_W \otimes \mathbb{1})(w \otimes f(v) \otimes g) \\ &= C_W \circ \mathrm{SWAP}_{W,W^*}(f(v)w \otimes g) \\ &= f(v)C_W(g \otimes w) = f(v)g(w), \end{aligned}$$

while

$$\begin{aligned} C_V \circ \mathrm{SWAP}_{V,V^*} \circ &(\alpha_V \otimes \mathbb{1}) \circ (\mathbb{1} \otimes C_W \otimes \mathbb{1}) \circ \mathrm{SWAP}_{W \otimes V^*, V \otimes W^*}(w \otimes f \otimes v \otimes g) \\ &= C_V \circ \mathrm{SWAP}_{V,V^*} \circ (\alpha_V \otimes \mathbb{1}) \circ (\mathbb{1} \otimes C_W \otimes \mathbb{1})(v \otimes g \otimes w \otimes f) \\ &= C_V \circ \mathrm{SWAP}_{V,V^*} \circ (\alpha_V \otimes \mathbb{1})(v \otimes g(w) \otimes f) \\ &= C_V \circ \mathrm{SWAP}_{V,V^*}(g(w)v \otimes f) \\ &= g(w)C_V(f \otimes v) = g(w)f(v). \end{aligned}$$

So the two linear transformations are equal as desired. □

## 9.5 Combining natural isomorphisms

As can be seen from the preceeding sections, it can be very interesting to combine natural isomorphisms. For another example of this, consider the tensor product

$$\mathrm{Lin}(U_1, V_1) \otimes \mathrm{Lin}(U_2, V_2).$$

By Proposition 9.2.1, this space is isomorphic to

$$(V_1 \otimes U_1^*) \otimes (V_2 \otimes U_2^*).$$

By Proposition 9.1.5, we can drop the brackets in this expression. By Propositions 9.1.3 and 9.3.1, there are isomorphisms

$$V_1 \otimes U_1^* \otimes V_2 \otimes U_2^* \cong V_1 \otimes V_2 \otimes U_1^* \otimes U_2^* \cong (V_1 \otimes V_2) \otimes (U_1 \otimes U_2)^*.$$

But Proposition 9.2.1 tells us that this space is isomorphic to

$$\mathrm{Lin}(U_1 \otimes U_2, V_1 \otimes V_2).$$

So we can think of elements of $\mathrm{Lin}(U_1, V_1) \otimes \mathrm{Lin}(U_2, V_2)$ as elements of $\mathrm{Lin}(U_1 \otimes U_2, V_1 \otimes V_2)$.

**Example 9.5.1.** *While this identification of*

$$\mathrm{Lin}(U_1, V_1) \otimes \mathrm{Lin}(U_2, V_2) \cong \mathrm{Lin}(U_1 \otimes U_2, V_1 \otimes V_2)$$

*is the composition of a lot of intermediate isomorphisms, it's easy to calculate it on specific linear maps. For instance, suppose $U_1 = U_2 = V_1 = V_2 = \mathbb{C}\{0, 1\}$, and let $S = |0\rangle\langle 0|$ and $T = |1\rangle\langle 1|$. Then the isomorphism sends*

$$S \otimes T \mapsto |0\rangle \otimes \langle 0| \otimes |1\rangle \otimes \langle 1| \mapsto |0\rangle \otimes |1\rangle \otimes \langle 0| \otimes \langle 1| .$$

*Using the concrete tensor product, we can identify $|0\rangle \otimes |1\rangle$ as $|01\rangle$, and $\langle 0| \otimes \langle 1|$ with $\langle 01|$. So we get the linear map $|01\rangle\langle 01|$, which represents the linear map $\mathbb{C}\{0, 1\}^2 \to \mathbb{C}\{0, 1\}^2$ which sends $|01\rangle \mapsto |01\rangle$, and every other computational basis state to* 0*.*

Let $\psi : \mathrm{Lin}(U_1, V_1) \otimes \mathrm{Lin}(U_2, V_2) \to \mathrm{Lin}(U_1 \otimes U_2, V_1 \otimes V_2)$ denote this composed natural isomorphism. We now have to different ways we might define the tensor product of linear maps $T_1 \in \mathrm{Lin}(U_1, V_1)$ and $T_2 \in \mathrm{Lin}(U_2, V_2)$. We can take the unique linear map $T_1 \otimes T_2 : U_1 \otimes U_2 \to V_1 \otimes V_2$ sending $u_1 \otimes u_2 \mapsto T_1(u_1) \otimes T_2(u_2)$, as defined in the previous chapter. Or we can take $\psi(T_1 \otimes' T_2)$, where $T_1 \otimes' T_2$ now refers to the tensor product of $T_1$ and $T_2$ in $\mathrm{Lin}(U_1, V_1) \otimes \mathrm{Lin}(U_2, V_2)$.

**Exercise 9.5.2.** *Show that $T_1 \otimes T_2 = \psi(T_1 \otimes' T_2)$.*

Another interesting case to consider is the dual $(V \otimes V^*)^*$ of $V \otimes V^*$. By Proposition 9.3.1, there is a natural isomorphism

$$(V \otimes V^*)^* \cong V^* \otimes (V^*)^*.$$

By Exercise 9.3.5, there is a natural isomorphism $\alpha : (V^*)^* \to V$, and hence a natural isomorphism

$$\mathbb{1}_{V^*} \otimes \alpha : V^* \otimes (V^*)^* \to V^* \otimes V.$$

By Proposition 9.1.3, there is a natural isomorphism $V^* \otimes V \to V \otimes V^*$. Finally, by Proposition 9.2.1 there is a natural isomorphism $\mathrm{Lin}(V, V) \cong V \otimes V^*$. Putting all these natural isomorphisms together, we get

$$\mathrm{Lin}(V, V)^* \cong (V \otimes V^*)^* \cong V^* \otimes (V^*)^* \cong V^* \otimes V \cong V \otimes V^* \cong \mathrm{Lin}(V, V).$$

In other words, while $V$ is not naturally isomorphic to $V^*$, $\mathrm{Lin}(V, V)$ is naturally isomorphic to $\mathrm{Lin}(V, V)^*$. One interesting aspect of this is that $\mathrm{Lin}(V, V)$

contains a non-zero "distinguished element", namely the identity map $\mathbb{1}_V$. Note that the identity map is, in a sense, natural as well, since we can write it down without picking a basis for $V$ or making any other choices. Since $\mathrm{Lin}(V, V)$ and $\mathrm{Lin}(V, V)^*$ are naturally isomorphic, there should be a corresponding "distinguished element" of $\mathrm{Lin}(V, V)^*$, and indeed, we just showed that $\mathrm{Lin}(V, V)^*$ contains the trace.

**Exercise 9.5.3.** *Show that the natural isomorphism* $\mathrm{Lin}(V, V) \to \mathrm{Lin}(V, V)^*$ *described above sends* $\mathbb{1}_V$ *to* $\mathrm{tr}$*.*

# Chapter 10

# Tensor product of Hilbert spaces

In this chapter, we finally return the reason we started looking at tensor products, namely Axiom #3, which states that if $H_1$ and $H_2$ are the Hilbert spaces of physical systems, then the Hilbert space of the joint system is the tensor product $H_1 \otimes H_2$. If $H_1 = \mathbb{C}X_1$ and $H_2 = \mathbb{C}X_2$, then $H_1 \underline{\otimes} H_2 = \mathbb{C}X_1 \times X_2$ is a Hilbert space with orthonormal basis $\{|x_1, x_2\rangle : x_1 \in X_1, x_2 \in X_2\}$. However, we haven't explained how to make the abstract tensor product $H_1 \otimes H_2$ into a Hilbert space. Of course, we can define an inner product on any space simply by picking a basis and declaring it to be orthonormal. However, since $H_1 \otimes H_2$ is the joint system of two subsystems, we should expect $H_1 \otimes H_2$ to have a natural inner product, i.e. we should be able to uniquely define the inner product without picking a basis. This is indeed the case:

**Proposition 10.0.1.** *Let $H_1$, $H_2$ be (finite-dimensional) Hilbert spaces. Then there is a unique positive form $\langle , \rangle$ on $H_1 \otimes H_2$ such that*

$$\langle u_1 \otimes v_1, u_2 \otimes v_2 \rangle = \langle u_1, u_2 \rangle_{H_1} \cdot \langle v_1, v_2 \rangle_{H_2}$$

*for all $u_1, u_2 \in H_1$, $v_1, v_2 \in H_2$.*

If we believe the proposition that $\langle , \rangle$ exists, and $\{a_1, \dots, a_m\}$ and $\{b_1, \dots, b_n\}$ are orthonormal bases of $H_1$ and $H_2$ respectively, then

$$\langle a_{i_1} \otimes b_{j_1}, a_{i_2} \otimes b_{j_2} \rangle = \langle a_{i_1}, a_{i_2} \rangle \cdot \langle b_{j_1}, b_{j_2} \rangle = \delta_{i_1, i_2} \cdot \delta_{j_1, j_2} = \delta_{(i_1, i_2), (j_1, j_2)}.$$

So

$$\{a_i \otimes b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

is an orthonormal basis of $H_1 \otimes H_2$. We will use this idea in the proof.

*Proof of Proposition 10.0.1.* Pick an orthonormal basis $\{a_1, \ldots, a_m\}$ of $H_1$ and an orthonormal basis of $b_1, \ldots, b_n$ of $H_2$. The set

$$\{a_i \otimes b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

is a basis for $H_1 \otimes H_2$, so there is an inner product $\langle , \rangle$ for which this basis is orthonormal.

Suppose $u_i \in H_1$, $i = 1, 2$, $v_i \in H_2$, $i = 1, 2$. For each $i = 1, 2$, write

$$u_i = \sum_{j=1}^{m} c_{ij} a_j \text{ and } v_i = \sum_{k=1}^{n} d_{ik} b_k.$$

Then

$$u_i \otimes v_i = \sum_{\substack{1 \leq j \leq m \\ 1 \leq k \leq n}} c_{ij} d_{ik}\ a_j \otimes b_k.$$

So

$$\begin{aligned}
\langle u_1 \otimes v_1, u_2 \otimes v_2 \rangle &= \sum_{\substack{1 \leq j_1, j_2 \leq m \\ 1 \leq k_1, k_2 \leq n}} \overline{c_{1j_1} d_{1k_1}} c_{2j_2} d_{2k_2} \langle a_{j_1} \otimes b_{k_1}, a_{j_2} \otimes b_{k_2} \rangle \\
&= \sum_{\substack{1 \leq j_1, j_2 \leq m \\ 1 \leq k_1, k_2 \leq n}} \overline{c_{1j_1} d_{1k_1}} c_{2j_2} d_{2k_2} \delta_{j_1, j_2} \delta_{k_1, k_2} \\
&= \sum_{\substack{1 \leq j \leq m \\ 1 \leq k \leq n}} (\overline{c_{1j}} c_{2j})(\overline{d_{1k}} d_{2k}) \\
&= \left( \sum_{1 \leq j \leq m} \overline{c_{1j}} c_{2j} \right) \left( \sum_{1 \leq k \leq n} \overline{d_{1k}} d_{2k} \right) \\
&= \langle u_1, u_2 \rangle_{H_1} \cdot \langle v_1, v_2 \rangle_{H_2}.
\end{aligned}$$

□

If $U$, $V$, and $W$ are Hilbert spaces, then we can use Proposition 10.0.1 to define a Hilbert space structure on $U \otimes (V \otimes W)$ and $(U \otimes V) \otimes W$. In $U \otimes (V \otimes W)$,

$$\langle u_1 \otimes (v_1 \otimes w_1), u_2 \otimes (v_2 \otimes w_2) \rangle = \langle u_1, u_2 \rangle \cdot \langle v_1 \otimes w_1, v_2 \otimes w_2 \rangle = \langle u_1, u_2 \rangle \cdot \langle v_1, v_2 \rangle \cdot \langle w_1, w_2 \rangle.$$

Similarly,

$$\langle (u_1 \otimes v_1) \otimes w_1, (u_2 \otimes v_2) \otimes w_2 \rangle = \langle u_1, u_2 \rangle \cdot \langle v_1, v_2 \rangle \cdot \langle w_1, w_2 \rangle$$

in $(U \otimes V) \otimes W$, so the natural map

$$U \otimes (V \otimes W) \to (U \otimes V) \otimes W : u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$$

sends an orthonormal basis to an orthonormal basis, and hence is an isomorphism of Hilbert spaces, not just of vector spaces. In this way, we can also talk about tensor products $H_1 \otimes \cdots \otimes H_k$ for Hilbert spaces $H_1, \ldots, H_k$ without specifying a bracketing.

Recall that if $H$ is a Hilbert space, then $H$ is antilinearly isomorphic to $H^*$, via the map that sends $|\psi\rangle \mapsto \langle\psi|$. For a tensor product of Hilbert spaces $H_1 \otimes H_2$, this map sends

$$|\psi_1\rangle\,|\psi_2\rangle \mapsto \langle\psi_1|\,\langle\psi_2|\,,$$

where we think of $\langle\psi_1|\,\langle\psi_2|$ as an element of $(H_1 \otimes H_2)^*$. To see this, observe that

$$\langle\psi_1|\,\langle\psi_2|\,|\phi_1\rangle\,|\phi_2\rangle = \langle\psi_1|\phi_1\rangle\,\langle\psi_2|\phi_2\rangle$$

is the inner product of $|\psi_1\rangle\,|\psi_2\rangle$ and $|\phi_1\rangle\,|\phi_2\rangle$. Since the product vectors span $H_1 \otimes H_2$, it follows that $\langle\psi_1|\,\langle\psi_2|$ applied to any vector $|\phi\rangle \in H_1 \otimes H_2$ will be the inner product of $|\psi_1\rangle\,|\psi_2\rangle$ with $|\phi\rangle$.

**Exercise 10.0.2.** *Let $S : V_1 \to V_2$ and $T : W_1 \to W_2$ be linear operators between Hilbert spaces. Using the definition of adjoint operators, show that*

$$(S \otimes T)^* = S^* \otimes T^*$$

*as operators $V_2 \otimes W_2 \to V_1 \otimes W_1$.*

**Exercise 10.0.3.** *Let $U : H_1 \to H_1$ and $V : H_2 \to H_2$ be unitary linear transformations. Use the previous exercise to show that $U \otimes V : H_1 \otimes H_2 \to H_1 \otimes H_2$ is unitary.*

We previously showed in Section 3.5 that if $H$ is a Hilbert space, then $H^*$ is also a Hilbert space. Since we could define the inner product on $H^*$ without picking a basis for $H$, this inner product structure on $H^*$ is natural. Thus if $V$ and $W$ are Hilbert spaces, then the spaces we looked at in the previous chapter like $W \otimes V^*$ and $V^* \otimes W^*$ are also Hilbert spaces in a natural way.

**Exercise 10.0.4.** *Suppose $V$ and $W$ are Hilbert spaces. By combining Proposition 10.0.1 and Exercise 3.5.8, we can define natural Hilbert space structures on $V^* \otimes W^*$ and $(V \otimes W)^*$. Show that the natural map*

$$V^* \otimes W^* \to (V \otimes W)^*$$

*from Proposition 9.3.1 is an isomorphism of Hilbert spaces.*

## 10.1 The Frobenius inner product

If $V$ and $W$ are Hilbert spaces, we can use the natural Hilbert space structure on $W \otimes V^*$ to define an inner product on $\mathrm{Lin}(V, W)$, since $\mathrm{Lin}(V, W)$ and $W \otimes V^*$ are isomorphic. This inner product is called the **Frobenius inner product**, and will be denoted by $\langle , \rangle_F$. The corresponding norm on $\mathrm{Lin}(V, W)$ is called the **Frobenius norm**, and will be denoted by $\| \cdot \|_F$. Outside of this book, these are also sometimes known as the **Hilbert-Schmidt inner product and norm**. To better understand the Frobenius inner product, we first need to work out what taking adjoints does in $W \otimes V^*$.

**Lemma 10.1.1.** *Let $V$ and $W$ be Hilbert spaces, and suppose $|v\rangle \in V$, $|w\rangle \in W$. If $T = |w\rangle \langle v| \in \mathrm{Lin}(V, W)$, then $T^* = |v\rangle \langle w| \in \mathrm{Lin}(W, V)$.*

*Proof.* Suppose $|x\rangle \in V$ and $|y\rangle \in W$. Then

$$\langle T |x\rangle , |y\rangle\rangle = \langle \langle v|x\rangle |w\rangle , |y\rangle\rangle = \overline{\langle v|x\rangle} \langle w|y\rangle = \langle |x\rangle , |v\rangle \langle w| \cdot |y\rangle\rangle,$$

so $|v\rangle \langle w|$ satisfies the defining condition for the adjoint. □

Suppose $|v\rangle , |x\rangle \in V$ and $|w\rangle , |y\rangle \in W$. Then the Frobenius inner product of $|w\rangle \langle v|$ and $|y\rangle \langle x|$ in $\mathrm{Lin}(V, W)$ is, by definition,

$$\langle |w\rangle \langle v| , |y\rangle \langle x|\rangle_F = \langle |w\rangle , |y\rangle\rangle \langle \langle v| , \langle x|\rangle = \langle w|y\rangle \langle x|v\rangle .$$

It is often convenient to rewrite this formula in the following way, now stated for general linear transformations:

**Proposition 10.1.2.** *Let $V$ and $W$ be Hilbert spaces, and let $S, T \in \mathrm{Lin}(V, W)$. Then the Frobenius inner product of $S$ and $T$ is*

$$\langle S, T\rangle_F = \mathrm{tr}(S^* T).$$

*Proof.* First suppose that $S = |w\rangle \langle v|$ and $T = |y\rangle \langle x|$ for $|v\rangle , |x\rangle \in V$ and $|w\rangle , |y\rangle \in W$. Then

$$\langle S, T\rangle_F = \langle w|y\rangle \langle x|v\rangle = \langle w|y\rangle \mathrm{tr}(|v\rangle \langle x|) = \mathrm{tr}\left(|v\rangle \langle w| \cdot |y\rangle \langle x|\right) = \mathrm{tr}\left((|w\rangle \langle v|)^* \cdot |y\rangle \langle x|\right)$$

by Lemma 10.1.1. In general, if

$$S = \sum_i |w_i\rangle \langle v_i| \text{ and } T = \sum_j |y_j\rangle \langle x_j| ,$$

then

$$\begin{aligned}\langle S,T\rangle_F &= \sum_{i,j}\langle |w_i\rangle\langle v_i|\,, |y_j\rangle\langle x_j|\rangle_F = \sum_{i,j}\operatorname{tr}((|w_i\rangle\langle v_i|)^*\cdot|y_j\rangle\langle x_j|)\\ &= \operatorname{tr}\left(\left[\sum_i |w_i\rangle\langle v_i|\right]^*\left[\sum_j |y_j\rangle\langle x_j|\right]\right) = \operatorname{tr}(S^*T).\end{aligned}$$

□

**Exercise 10.1.3.** *Let $V$ and $W$ be Hilbert spaces.*

*(a) Show that if $S \in \operatorname{Lin}(V,V)$, then $\overline{\operatorname{tr}(S)} = \operatorname{tr}(S^*)$. (Hint: there are several ways to prove this. One way is to use the trace of matrices. Another way is to set $T = \mathbb{1}$ in Proposition 10.1.2).*

*(b) Prove directly (using part (a) and properties of trace and adjoint) that $\langle S,T\rangle := \operatorname{tr}(S^*T)$ defines an inner product on $\operatorname{Lin}(V,W)$.*

**Exercise 10.1.4.** *Let $V$ and $W$ be Hilbert spaces, with orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$. Let $S,T \in \operatorname{Lin}(V,W)$, and let $A = [S]_{\mathcal{B}',\mathcal{B}}$ and $B = [T]_{\mathcal{B}',\mathcal{B}}$. Show that*

$$\langle S,T\rangle_F = \sum_{i,j}\overline{A_{ij}}B_{ij}.$$

## 10.2 The no-cloning theorem

We finish this chapter with an important application of what we've learned so far: the no-cloning theorem. Unitarity of the evolution operator tells us a lot about how quantum states behave. One of the key features of classical information is that we can copy it. For instance, on a classical computer, there is an operation which takes a register with value $a$ and an uninitialized register, changes the value of the uninitialized register to $a$, and leaves the original register unchanged. Now that we know how to take a tensor product of Hilbert spaces, we can show that copying isn't possible with quantum systems. Suppose we have a quantum register $H$. Two identical registers would be given by $H \otimes H$. Suppose the state of an uninitialized register is $|0\rangle$. A copying operation would be a unitary map $U : H \otimes H \to H \otimes H$ such that

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

for all states $|\psi\rangle$ and $|0\rangle$. It's clear this isn't possible, even if $\dim H = 1$, since if this equation held, we'd have

$$e^{i\theta}|\psi\rangle|\psi\rangle = e^{i\theta}U|\psi\rangle|0\rangle = Ue^{i\theta}|\psi\rangle|0\rangle = e^{2i\theta}|\psi\rangle|\psi\rangle$$

for all $\theta \in \mathbb{R}$, a contradiction. However, from what we learned previously, we should ignore phases when working with quantum states, so a copying operation only has to satisfy

$$U\left|\psi\right\rangle\left|0\right\rangle = c\left|\psi\right\rangle\left|\psi\right\rangle$$

for all states $\left|\psi\right\rangle$, where the constant $c \in \mathbb{C}^x$ can depend on $\left|\psi\right\rangle$.

**Theorem 10.2.1** (No-cloning theorem)**.** *Let $H$ be a Hilbert space with $\dim H \geq 2$, and let $\left|0\right\rangle \in H$ be a state. Then there is no unitary operator $U$ such that*

$$U\left|\psi\right\rangle\left|0\right\rangle = c\left|\psi\right\rangle\left|\psi\right\rangle$$

*for all states $\left|\psi\right\rangle$.*

*Proof.* Suppose $U$ is such a unitary, and let $\left|\phi_1\right\rangle$ and $\left|\phi_2\right\rangle$ be two states such that $0 < \left\langle\phi_1|\phi_2\right\rangle < 1$. For each $i = 1, 2$, there is a constant $c_i$ such that

$$U\left|\phi_i\right\rangle\left|0\right\rangle = c_i\left|\phi_i\right\rangle\left|\phi_i\right\rangle.$$

Note that $|c_1| = |c_2| = 1$. Since $U$ is a unitary,

$$\overline{c_1}c_2 = \left\langle\phi_1|\phi_2\right\rangle\left\langle\phi_1|\phi_2\right\rangle = \left\langle\phi_1\right|\left\langle 0\right| U^*U\left|\phi_2\right\rangle\left|0\right\rangle = \left\langle\phi_1|\phi_2\right\rangle.$$

Taking absolute values on both sides, we get that

$$\left\langle\phi_1|\phi_2\right\rangle^2 = \left\langle\phi_1|\phi_2\right\rangle,$$

a contradiction. □

# Chapter 11

# Projective measurements

Suppose we have two systems with Hilbert spaces $H_A$ and $H_B$. Suppose $\mathcal{B} = \{|u_1\rangle, \ldots, |u_m\rangle\}$ is a basis for $H_A$, and $\mathcal{C} = \{|v_1\rangle, \ldots, |v_n\rangle\}$ is a basis for $H_B$. If we measure $|\psi\rangle \in H_A \otimes H_B$ in basis

$$\mathcal{D} = \{|u_i\rangle |v_j\rangle : 1 \leq i \leq m, 1 \leq j \leq n\}$$

for $H_A \otimes H_B$, we get outcome $|u_i\rangle |v_j\rangle$ with probability

$$|\langle u_i| \langle v_j| |\psi\rangle|^2,$$

and the state after measurement will be

$$\frac{\langle u_i| \langle v_j| |\psi\rangle}{|\langle u_i| \langle v_j| |\psi\rangle|} |u_i\rangle |v_j\rangle .$$

While it certainly makes sense to measure both systems like this, we should also be able to measure $H_A$ by itself, and leave $H_B$ unchanged. For instance, $H_A$ and $H_B$ could be separate laboratories, and we should be able to do an experiment in $H_A$ without doing one at the same time in $H_B$.

What should a measurement like this look like? If $|\psi\rangle = |\phi_A\rangle |\phi_B\rangle$, and we measure in basis $\mathcal{B}$, then focusing in on register $H_A$, we'd expect to get outcome $|u_i\rangle$ with probability $|\langle u_i|\phi_A\rangle|^2$, and the state of $H_A$ after measurement should be

$$\frac{\langle u_i|\phi_A\rangle}{|\langle u_i|\phi_A\rangle|} |u_i\rangle .$$

Since $H_B$ is unchanged, the state of $H$ after the measurement should be

$$\frac{\langle u_i|\phi_A\rangle}{|\langle u_i|\phi_A\rangle|} |u_i\rangle |\phi_B\rangle .$$

This analysis works for product states, but doesn't tell us what happens if $|\psi\rangle$ is entangled. To answer this question, we might try to model this measurement process as measurement in a basis. Unfortunately, if $\dim H_B \geq 2$, then this measurement process can't be described by measurement with respect to a basis, even on product states. Indeed, suppose we claim that this measurement is described by measurement in a basis $\mathcal{B}'$ for $H_A \otimes H_B$ (not necessarily a product basis). Then no matter what the input state $|\psi\rangle$ or outcome of the measurement is, the state after measurement must be a scalar multiple of one of the states in $\mathcal{B}'$.

**Exercise 11.0.1.** *Suppose* $\dim H_B \geq 2$*. Given* $|\psi\rangle \in H_A \otimes H_B$*, let* $[|\psi\rangle]$ *denote the equivalence class of* $|\psi\rangle$ *with respect to global phase.*

*(a) Show that for any fixed non-zero* $|u\rangle \in H_A$*, the set*

$$\{[|u\rangle |\phi\rangle] : |\phi\rangle \in H_B\} \subseteq H_A \otimes H_B$$

*contains infinitely many elements.*

*(b) Conclude that, even if we restrict the input to product states, it's impossible for measurement with respect to a basis to give all the possible output states for the measurement process described above.*

We need a more general theory of measurement which includes measurement in a basis, but also allows us to model situations where we want to measure part of a system, but leave another part of the system unchanged. Ideally the theory should apply to situations that don't have anything to do with tensor product. After all, even if our motivation comes from measuring $H_A$ as part of a larger system $H = H_A \otimes H_B$, we should be able to forget about the fact that $H$ splits into subsystems and just think about what we're doing as measurement on $H$. We can get such a theory by thinking of splitting systems up into subspaces via direct sums.

## 11.1 Direct sums and projections

Recall the following theorem of linear algebra:

**Theorem 11.1.1.** *Let* $V$ *be a finite-dimensional vector space, and let* $V_1, \ldots, V_k$ *be a collection of subspaces. Then the following are equivalent:*

*(1)*

$$V_i \cap \operatorname{span} \bigcup_{j \neq i} V_j = 0$$

*for all* $1 \leq i \leq k$ *and* $\operatorname{span} V_1 \cup \cdots \cup V_k = V$.

(2)

$$V_i \cap \operatorname{span} \bigcup_{j \neq i} V_j = 0$$

*for all* $1 \leq i \neq j \leq k$ *and* $\sum_{i=1}^{k} \dim V_i = \dim V$.

(3) *There is a basis* $\mathcal{B}_i$ *of* $V_i$, $i = 1, \ldots, k$, *such that* $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$ *for all* $1 \leq i \neq j \leq k$, *and* $\cup \mathcal{B}_i$ *is a basis of* $V$.

(4) *If* $\mathcal{B}_i$ *is a basis for* $V_i$, $i = 1, \ldots, k$, *then* $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$ *for all* $1 \leq i \neq j \leq k$, *and* $\cup \mathcal{B}_i$ *is a basis of* $V$.

(5) *Every element of* $V$ *can be written uniquely as* $v = v_1 + \ldots + v_k$, *where* $v_i \in V_i$ *for all* $1 \leq i \leq V_i$.

The point of requiring $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$ in parts (3) and (4) is so the union $\bigcup \mathcal{B}_i$ will be disjoint. The difference between parts (3) and (4) is that (4) is a statement about all choices of basis $\mathcal{B}_i$ for $V_i$. Uniqueness in part (5) means that if $v_1 + \ldots + v_k = v'_1 + \ldots + v'_k$, where $v_i, v'_i \in V_i$ for all $1 \leq i \leq k$, then $v_i = v'_i$ for all $1 \leq i \leq k$.

*Proof of Theorem 11.1.1.* Suppose (1) holds. Then every element $v \in V$ can be written as $v = v_1 + \ldots + v_n$ for $v_i \in V_i$, and if $v$ is also equal to $v'_1 + \ldots + v'_n$ for $v'_i \in V_i$, then

$$v_i - v'_i = \sum_{j \neq i} v'_j - v_j \in V_i \cap \operatorname{span}_{j \neq i} V_j = 0,$$

so $v_i - v'_i = 0$, and hence $v_i = v'_i$. So (1) implies (5).

Now suppose that (5) holds, and that

$$\mathcal{B}_i = \{v_{i1}, \ldots, v_{in_i}\}$$

is a basis for $V_i$, $1 \leq i \leq k$. Let $\mathcal{B} = \bigcup \mathcal{B}_i$. If $v \in V$, then $v = v_1 + \ldots + v_n$ for $v_i \in V$. Because $\mathcal{B}_i$ spans $V_i$, $v_i = \sum_{j=1}^{n_i} a_{ij} v_{ij}$. So

$$v = \sum_{i=1}^{k} \sum_{j=1}^{n_i} a_{ij} v_{ij},$$

and hence $\mathcal{B}$ spans $V$. For linear independence, suppose

$$\sum_{i=1}^{k}\sum_{j=1}^{n_i} a_{ij}v_{ij} = 0$$

for some $a_{ij}$, $1 \leq i \leq k$, $1 \leq j \leq n_i$. Let $v_i = \sum_{j=1}^{n_i} a_{ij}v_{ij}$. Since 0 can be written as $0 = 0 + \ldots + 0$, where each $0 \in V_i$, and this decomposition is unique, we conclude that $v_i = 0$. Since $\mathcal{B}_i$ is linearly independent, $a_{ij} = 0$ for all $i, j$. This doesn't just show that $\mathcal{B}$ is linearly independent, it shows that $v_{ij}$ is linearly independent from $\bigcup_{\ell \neq i} \mathcal{B}_\ell$ for all $1 \leq i \leq k$, $1 \leq j \leq n_i$. In particular, $\mathcal{B}_i \cap \mathcal{B}_\ell = \emptyset$ if $\ell \neq i$. So (5) implies (4).

(3) follows immediately from (4). Suppose (3) holds for some choice of bases $\mathcal{B}_i = \{v_{i1}, \ldots, v_{in_i}\}$ for $V_i$. Since $\mathcal{B} = \bigcup \mathcal{B}_i$ is a basis for $V$, and $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$ if $i \neq j$, we conclude that

$$\dim V = |\mathcal{B}| = \sum_i |\mathcal{B}_i| = \sum_i \dim V_i.$$

If

$$v \in V_i \cap \operatorname{span} \bigcup_{\ell \neq i} V_\ell$$

for some $1 \leq i \leq k$, then we can write

$$v = \sum_{j=1}^{n_i} a_j v_{ij}, \text{ and also } v = \sum_{\ell \neq i} \sum_{j=1}^{n_\ell} b_{\ell j} v_{\ell j}.$$

But since $\mathcal{B} = \bigcup \mathcal{B}_i$ is linearly independent and $\mathcal{B}_i \cap \mathcal{B}_\ell = \emptyset$ for $\ell \neq i$, we must have $v = 0$. So (3) implies (2).

Finally, suppose (2) holds, and let $W = \operatorname{span} \bigcup V_i$. Then (1) holds for $W$ and $V_1, \ldots, V_k$, so (2) holds for $W$ and $V_1, \ldots, V_k$ by what we've already shown, and hence

$$\dim W = \sum_i \dim V_i = \dim V.$$

We conclude that $W = V$, so given what we've already shown, (2) implies (1). □

**Definition 11.1.2.** *If any of the conditions in Theorem 11.1.1 hold, then we say that $V$ is the* ***direct sum of*** *$V_1, \ldots, V_k$, and write $V = V_1 \oplus \cdots \oplus V_k$.*

The canonical example of a direct sum decomposition comes from products:

**Example 11.1.3.** *Let $W_1, \ldots, W_k$ be a collection of finite-dimensional vector spaces, and let $V = W_1 \times \cdots \times W_k$ be the product vector space, with operations*

$$c\cdot(v_1, \ldots, v_k) = (cv_1, \ldots, cv_n) \text{ and } (v_1, \ldots, v_k)+(w_1, \ldots, w_k) = (v_1+w_1, \ldots, v_k+w_k).$$

*Let $V_i \subseteq W$ be the subset of tuples $(v_1, \ldots, v_k)$ where $v_j = 0$ for all $j \neq i$. Then $V = V_1 \oplus \ldots \oplus V_k$, as can easily be seen from Theorem 11.1.1, part (5). In this case, we also say that $V = W_1 \oplus \ldots \oplus W_k$.*

If $V = V_1 \oplus \cdots \oplus V_k$, then we refer to the unique way of writing $v \in V$ as $v = \sum_{i=1}^k v_i$ with $v_i \in V_i$ for $1 \leq i \leq k$ as the **direct sum decomposition of** $v$. In Example 11.1.3, we can break every element $v = (v_1, \ldots, v_k)$ into its components $v_i$. Direct sum decompositions allow us to work with $V = V_1 \oplus \cdots \oplus V_k$ in the same way. If $v, w \in V$ have direct sum decompositions

$$v = \sum_{i=1}^k v_i, \quad w = \sum_{i=1}^k w_i,$$

then for any $c \in \mathbb{F}$,

$$cv + w = \sum_{i=1}^k (cv_i + w_i) \tag{11.1.1}$$

where $cv_i + w_i \in V_i$, so Equation (11.1.1) gives the direct sum decomposition of $cv + w$.

**Definition 11.1.4.** *A **projection** on a vector space $V$ is a linear operator $P : V \to V$ such that $P^2 = P$. Two projections $P$ and $P'$ on $V$ are said to be **orthogonal** if $PP' = P'P = 0$.*

*A **complete family of orthogonal projections** is a collection of projections $\{P_1, \ldots, P_k\}$ such that*

*(a) $P_i$ is a projection for all $1 \leq i \leq k$,*

*(b) $P_iP_j = 0$ for all $1 \leq i \neq j \leq k$, and*

*(c) $\sum_{i=1}^k P_i = \mathbb{1}$.*

**Lemma 11.1.5.** *Let $V = V_1 \oplus \cdots \oplus V_k$. Then for every $1 \leq i \leq k$, there is a linear map $P_i : V \to V$ which sends $v \mapsto v_i$, where $v = \sum_j v_j$ is the direct sum decomposition of $v$. Furthermore, $\{P_1, \ldots, P_k\}$ is a complete family of orthogonal projections.*

*Proof.* $P_i$ is a well-defined function by uniqueness of the direct sum decomposition. Linearity of $P_i$ follows from Equation (11.1.1).

If $v \in V_i$, then the direct sum decomposition of $v$ is $v = \sum_{j=1}^{k} v_j$, where $v_i = v$ and $v_j = 0$ if $j \neq i$. Hence if $v \in V_i$, then $P_i v = v$, while $P_j v = 0$. For any $v \in V$, $P_i v \in V_i$, and hence $P_i^2 v = P_i(P_i v) = P_i v$, so $P_i^2 = P_i$. Similarly, $P_j P_i v = 0$ if $i \neq j$, so $P_j P_i = 0$.

Finally, if $v \in V$ has direct sum decomposition $v = \sum_{i=1}^{k} v_i$, then

$$\sum_{i=1}^{k} P_i v = v_1 + \ldots + v_k = v,$$

so $\sum_{i=1}^{k} P_i = \mathbb{1}$. □

One small part of this proof comes up enough that it's worth recording in its own lemma:

**Lemma 11.1.6.** *If $P$ is a projection, and $v \in \operatorname{Im} P$, then $Pv = v$.*

*Proof.* If $v \in \operatorname{Im} P$, then $v = Px$, so $Pv = P^2 x = Px = v$. □

The projection $P_i$ in Lemma 11.1.5 is called the **projection onto the $i$th factor** (or the **projection onto $V_i$**). To make it clear what direct sum decomposition we are talking about, we can also call this map the **projection onto $V_i$ with respect to the direct sum** $V = V_1 \oplus \cdots \oplus V_k$.

It can be helpful to see how $P_i$ acts on a basis. Suppose $V = V_1 \oplus \cdots \oplus V_k$, and that $\mathcal{B}_i$ is a basis for $V_i$. By definition, $\mathcal{B} = \bigcup \mathcal{B}_i$ is a basis for $V$. Any element $v \in V$ can be written uniquely as

$$v = \sum_{v \in \mathcal{B}} c_v v$$

for some constants $c_v \in \mathbb{F}$. The direct sum decomposition of $v$ is

$$v = \sum_{j=1}^{k} \sum_{v \in \mathcal{B}_i} c_v v,$$

so

$$P_i v = \sum_{v \in \mathcal{B}_i} c_v v.$$

In particular, if $v \in \mathcal{B}$, then $P_i v = v$ if $v \in \mathcal{B}_i$, and $P_i v = 0$ if $v \notin \mathcal{B}_i$. The matrix $[P_i]_{\mathcal{B}}$ is the diagonal matrix with 1's in the diagonal entries corresponding to the basis elements of $\mathcal{B}_i$, and 0's elsewhere.

**Theorem 11.1.7.** *Let $V$ be a vector space, and let $k \geq 1$. Then there is a bijection $\Phi$ between the set*

$$\{(V_1, \ldots, V_k) \ : \ V_1, \ldots, V_k \text{ are subspaces of } V \text{ such that } V = V_1 \oplus \cdots \oplus V_k\}$$

*and the set*

$$\{(P_1, \ldots, P_k) \ : \{P_1, \ldots, P_k\} \text{ is a complete family of orthogonal projections}\}.$$

*This bijection sends $(V_1, \ldots, V_k) \mapsto (P_1, \ldots, P_k)$, where $P_i$ is the projection onto the ith factor in the direct sum decomposition $V = V_1 \oplus \cdots \oplus V_k$. The inverse $\Phi^{-1}$ sends $(P_1, \ldots, P_k) \mapsto (\operatorname{Im} P_1, \ldots, \operatorname{Im} P_k)$.*

*Proof.* We've already seen in Lemma 11.1.5 that if $V = V_1 \oplus \cdots \oplus V_k$, then we get a $k$-tuple of projections $(P_1, \ldots, P_k)$ such that $P_i P_j = 0$ for $i \neq j$ and $\sum_{j=1}^k P_j = \mathbb{1}$.

Suppose we are given a $k$-tuple $(P_1, \ldots, P_k)$ with $P_i P_j = 0$ if $i \neq j$, and $\sum_j P_j = \mathbb{1}$. Let $V_i = \operatorname{Im} P_i$. If $v \in V$, then

$$v = \mathbb{1}v = \sum_{i=1}^k P_i v,$$

where $P_i v \in V_i$. If $v = \sum_{i=1}^k v_i'$ with $v_i' \in V_i$ for all $1 \leq i \leq k$, then

$$P_i v = \sum_{j=1}^k P_i v_j' = v_i' + \sum_{j \neq i} P_i P_j v_j' = v_i',$$

so every $v \in V$ can be written uniquely as $v = v_1 + \ldots + v_k$ with $v_i \in V_i$ for $1 \leq i \leq k$. We conclude that $V = V_1 \oplus \ldots \oplus V_k$, so we get a map from $k$-tuples of projections meeting the required conditions, to $k$-tuples $(V_1, \ldots, V_k)$ of subspaces meeting the required conditions.

We leave it as an exercise to show that these maps are inverses. □

The case that $k = 2$ in Theorem 11.1.7 is especially interesting, due to the following lemma:

**Lemma 11.1.8.** *Let $P : V \to V$ be a projection. Then $\mathbb{1} - P$ is a projection, and $P(\mathbb{1} - P) = (\mathbb{1} - P)P = 0$. Also, $\operatorname{Im}(\mathbb{1} - P) = \ker P$.*

*Proof.*

$$(\mathbb{1} - P)^2 = \mathbb{1} - 2P + P^2 = \mathbb{1} - 2P + P = \mathbb{1} - P,$$

and

$$P(\mathbb{1} - P) = (\mathbb{1} - P)P = P - P^2 = P - P = 0.$$

Finally, if $v \in \operatorname{Im}(\mathbb{1} - P)$, then $v = (\mathbb{1} - P)x$ for some $x \in V$, so $Pv = P(\mathbb{1} - P)x = 0$. Hence $\operatorname{Im}(\mathbb{1} - P) \subseteq \ker P$. Conversely, if $v \in \ker P$, then $(\mathbb{1} - P)v = v$, so $v \in \operatorname{Im} P$. □

**Corollary 11.1.9.**

*(a) If $P : V \to V$ is a projection, then there is a direct sum decomposition $V = \operatorname{Im} P \oplus \ker P$.*

*(b) If $V = V_1 \oplus V_2$, then there is a unique projection $P$ such that* $\operatorname{Im} P = V_1$ *and* $\ker P = V_2$.

*Proof.* Let $\Phi$ be the bijection from Theorem 11.1.7 with $k = 2$. For part (a), $\{P, \mathbb{1} - P\}$ is a complete family of orthogonal projections by Lemma 11.1.8. Then

$$\Phi^{-1}(P, \mathbb{1} - P) = (\operatorname{Im} P_1, \operatorname{Im} \mathbb{1} - P) = (\operatorname{Im} P, \ker P),$$

so $V = \operatorname{Im} P \oplus \ker P$.

For part (b), if $(P_1, P_2) = \Phi(V_1, V_2)$, then $\operatorname{Im} P_1 = V_1$, and $P_2 = \mathbb{1} - P_1$, so $\ker P_1 = \operatorname{Im} \mathbb{1} - P_1 = \operatorname{Im} P_2 = V_2$. If $P$ is another projection with $\operatorname{Im} P = V_1$ and $\ker P = V_2$, then $\Phi^{-1}(P, \mathbb{1} - P) = (V_1, V_2)$. Since $\Phi$ is a bijection,

$$(P_1, P_2) = \Phi(V_1, V_2) = (P, \mathbb{1} - P),$$

so $P_1 = P$. □

Given $W \subset V$, the basis extension theorem implies that there is a subspace $W' \subset V$ such that $V = W \oplus W'$, and hence there is a projection $P$ with $\operatorname{Im} P = W$. However, while we can always find a projection mapping onto a subspace $W$, there can be infinitely many choices of for $\ker P$, so there is no natural definition of "the" projection onto $W$.

**Example 11.1.10.** *Let $W = \operatorname{span}\{e_1\} \subseteq \mathbb{C}^2$. Then $\mathbb{C}^2 = W \oplus \operatorname{span}\{e_2\}$, and hence there is a unique projection $P$ with* $\operatorname{Im} P = W$ *and* $\ker P = \operatorname{span}\{e_2\}$. *The matrix of this projection is* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

*We also have $\mathbb{C}^2 = W \oplus \operatorname{span}\{e_1 + e_2\}$, so there is a projection $P'$ with* $\operatorname{Im} P = W$ *and* $\ker P = \operatorname{span}\{e_1 + e_2\}$.

**Exercise 11.1.11.** *Find the matrix of $P'$ in Example 11.1.10.*

## 11.2 Orthogonal direct sums and self-adjoint projections

We can extend the concept of a direct sum decomposition to Hilbert spaces. The idea is that if $H = H_1 \oplus \cdots \oplus H_k$ is a direct sum decomposition of $H$ as a Hilbert space, then we should be able to calculate the inner product $\langle v, w\rangle$ as

$$\langle v, w\rangle = \sum_{i=1}^{k} \langle P_i v, P_i w\rangle,$$

where $P_i$ is the projection onto $H_i$. In particular, if $v \in H_i$ and $w \in H_j$ for $i \neq j$, then $P_i w = 0$ and $P_j v = 0$, so we should have $\langle v, w\rangle = 0$.

**Definition 11.2.1.** *Two subspace $V$ and $W$ of a Hilbert space $H$ are said to be **orthogonal**, written $V \perp W$, if $\langle v, w\rangle = 0$ for all $v \in V$, $w \in W$.*

**Theorem 11.2.2.** *Let $H$ be a Hilbert space, and let $H_1, \ldots, H_k$ be a collection of Hilbert spaces. Then the following are equivalent:*

*(1) $H = H_1 \oplus \cdots \oplus H_k$ as vector spaces, and $H_i \perp H_j$ for all $1 \leq i \neq j \leq k$.*

*(2) $H = H_1 \oplus \cdots \oplus H_k$ as vector spaces, and if $v, w \in H$ have direct sum decompositions $v = v_1 + \ldots v_k$, $w = w_1 + \ldots + w_k$, then*

$$\langle v, w\rangle = \sum_{i=1}^{k} \langle v_i, w_i\rangle.$$

*(3) $H_i \perp H_j$ for $1 \leq i \neq j \leq k$, and $\operatorname{span} H_1 \cup \ldots \cup H_k = H$.*

*(4) $H_i \perp H_j$ for $1 \leq i \neq j \leq k$, and $\sum_{i=1}^{k} \dim H_i = \dim H$.*

*(5) There is a basis $\mathcal{B}_i$ of $H_i$, $i = 1, \ldots, k$, such that $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$ for all $1 \leq i \neq j \leq k$, and $\bigcup \mathcal{B}_i$ is an orthonormal basis of $H$.*

*(6) If $\mathcal{B}_i$ is an orthonormal basis of $H_i$, $1 \leq i \leq k$, such that $\mathcal{B}_i \cap \mathcal{B}_j \neq \emptyset$ for all $1 \leq i \neq j \leq k$, then $\cup \mathcal{B}_i$ is an orthonormal basis of $H$.*

*Proof.* We leave this proof as an exercise. (1) $\implies$ (2) and (3) $\implies$ (1) are particularly worth working out. □

**Definition 11.2.3.** *If any of the conditions of Theorem 11.2.2 hold, we say that $H$ is the* ***Hilbert space direct sum of*** $H_1, \ldots, H_k$ *(or the* ***direct sum of*** $H_1, \ldots, H_k$ ***as a Hilbert space****). We write*

$$H = H_1 \oplus \cdots \oplus H_k.$$

Note that the notation for a direct sum of Hilbert spaces is the same as the notation for the direct sum of vector spaces. With direct sums, the convention is that a direct sum refers to a direct sum of vector spaces unless we explicitly mention that the direct sum is a direct sum of Hilbert spaces.

**Proposition 11.2.4.** *If $H = H_1 \oplus \cdots \oplus H_k$ is a Hilbert space direct sum, and $\mathcal{B}_i$ is an orthonormal basis for $H_i$, then the linear operator*

$$P_i := \sum_{|x\rangle \in \mathcal{B}_i} |x\rangle \langle x|$$

*is the projection onto the $i$th factor.*

*Proof.* The set $\mathcal{B} = \bigcup \mathcal{B}_i$ is a basis of $H$. If $v \in H$, then

$$v = \sum_{|x\rangle \in \mathcal{B}} \langle x|v\rangle |x\rangle = \sum_{j=1}^{k} \left[ \sum_{|x\rangle \in \mathcal{B}_j} \langle x|v\rangle |x\rangle \right]. \tag{11.2.1}$$

Since

$$\sum_{|x\rangle \in \mathcal{B}_j} \langle x|v\rangle |x\rangle \in H_i,$$

Equation (11.2.1) must be the direct sum decomposition of $v$. So the projection onto the $i$th factor sends

$$v \mapsto \sum_{|x\rangle \in \mathcal{B}_j} \langle x|v\rangle |x\rangle = P_j v.$$

□

One interesting consequence of this proposition is that the projections

$$P_i = \sum_{|x\rangle \in \mathcal{B}_i} |x\rangle \langle x| \tag{11.2.2}$$

that occur in the proposition depend only on the direct sum decomposition, not on the choice of basis $\mathcal{B}_i$ for $H_i$. Another thing to note is that, although the projection onto the $i$th factor is supposed to depend on the full direct sum decomposition, the formula for $P_i$ only refers to a basis for $H_i$, so it doesn't seem to depend on the choice of $H_j$, $j \neq i$. In fact, we can show that if $W$ is a subspace of a Hilbert space, then it does make sense to talk about "the projection onto $W$". That's because there is a natural way to choose a complementary subspace to $W$: we can take the **orthogonal complement**

$$W^{\perp} := \{v \in H : \langle w, v\rangle = 0 \text{ for all } w \in W\}.$$

**Lemma 11.2.5.** *If $W$ is a subspace of a Hilbert space $H$, then $H = W \oplus W^{\perp}$ as Hilbert spaces.*

*Proof.* Choose an orthonormal basis $\mathcal{B} = \{x_1, \ldots, x_k\}$ for $W$, and then extend it to an orthonormal basis $\{x_1, \ldots, x_n\}$ for $H$. The vectors $\{x_{k+1}, \ldots, x_n\}$ are orthogonal to the vectors in $\mathcal{B}$, and hence belong to $W^{\perp}$. Hence $\operatorname{span} W \cup W^{\perp} = \operatorname{span} \mathcal{B} = H$. We know that $W \perp W^{\perp}$ by definition, so $H = W \oplus W^{\perp}$. □

**Definition 11.2.6.** *Let $W$ be a subspace of a Hilbert space $H$, so that $H = W \oplus W^{\perp}$. The projection onto $W$ with respect to this direct sum is called the* ***orthogonal projection onto*** *$W$.*

By Corollary 11.1.9, the orthogonal projection onto $W$ with respect to the direct sum $H = W \oplus W^{\perp}$ is the unique projection $P$ with $\operatorname{Im} P = W$ and $\ker P = W^{\perp}$. This is another way to state the definition of orthogonal projection.

Proposition 11.2.4 implies:

**Corollary 11.2.7.** *If $\mathcal{B}$ is an orthonormal basis for a subspace $W$ of $H$, then*

$$P = \sum_{|x\rangle \in \mathcal{B}} |x\rangle \langle x|$$

*is the orthogonal projection onto $W$.*

*As a result, if $H = H_1 \oplus \cdots \oplus H_k$ is a Hilbert space direct sum, then the projection $P_i$ onto the $i$th factor with respect to this direct sum is equal to the orthogonal projection onto $H_i$.*

*Proof.* The formula is immediate. Since the formula for $P_i$ in Proposition 11.2.4 agrees with the formula for the orthogonal projection onto $H_i$, the second part of the corollary follows immediately. □

While Corollary 11.2.7 implies that operators of the form in Equation (11.2.7) are projections, it's also interesting to note that we can prove this directly. This method of proof can also be used to show that such projections are self-adjoint.

**Definition 11.2.8.** *A linear transformation $T : H \to H$ is* ***self-adjoint*** *if $T^* = T$.*

**Lemma 11.2.9.** *Let $\mathcal{B}$ be an orthonormal set of a Hilbert space $H$, and let*

$$P = \sum_{|x\rangle \in \mathcal{B}} |x\rangle \langle x| .$$

*Then*

$$P^2 = P = P^*$$

*Proof.*

$$\begin{aligned} P^2 &= \sum_{|x\rangle, |y\rangle \in \mathcal{B}} |x\rangle \langle x| |y\rangle \langle y| \\ &= \sum_{|x\rangle, |y\rangle \in \mathcal{B}} |x\rangle \langle x|y\rangle \langle y| \\ &= \sum_{|x\rangle} |x\rangle \langle x| = P, \end{aligned}$$

since $\mathcal{B}$ is orthonormal.

To see that $P$ is self-adjoint, note that for any two vectors $|v\rangle , |w\rangle \in H$,

$$\langle |v\rangle , P |w\rangle \rangle = \sum_{|x\rangle \in \mathcal{B}} \langle v|x\rangle \langle x|w\rangle = \langle P |v\rangle , |w\rangle \rangle,$$

so $P$ is self-adjoint. □

**Proposition 11.2.10.** *A projection $P : H \to H$ is the orthogonal projection onto $W = \operatorname{Im} P$ if and only if $P^* = P$.*

*Proof.* If $P$ is the orthogonal projection onto $W = \operatorname{Im} P$, then $P$ is self-adjoint by Corollary 11.2.7 and Lemma 11.2.9.

Conversely, suppose $P$ is a self-adjoint projection. Then $v \in \ker P$ if and only if

$$\langle x, Pv\rangle = 0$$

for all $x \in H$. But since $P$ is self-adjoint,

$$\langle x, Pv\rangle = \langle Px, v\rangle,$$

so $Pv = 0$ if and only if $\langle w, v\rangle = 0$ for all $w \in \operatorname{Im} P$. In other words, $\ker P = (\operatorname{Im} P)^{\perp}$. Thus $P$ is the orthogonal projection onto $W$. □

This leads to our version of Theorem 11.1.7 for Hilbert space direct sums:

**Theorem 11.2.11.** *Let $H$ be a Hilbert space and $k \geq 1$. The bijection from Theorem 11.1.7 restricts to a bijection from*

$$\{(H_1, \ldots, H_k) : H_1, \ldots, H_k \text{ subspaces of } H \text{ such that } H = H_1 \oplus \cdots \oplus H_k \text{ as a Hilbert space}\}$$

*to*

$$\left\{(P_1, \ldots, P_k) : P_1, \ldots, P_k \text{ are self-adjoint projections on } H \text{ such that} \sum_{j=1}^{k} P_j = \mathbb{1}\right\}.$$

Note that we've changed both sets from Theorem 11.1.7. In the first set, we've restricted from vector space direct sums to Hilbert space direct sums. In the second set, we've added the restriction that the projections be self-adjoint, but removed the restriction that $P_i P_j = 0$ for $i \neq j$.

**Definition 11.2.12.** *A **complete family of self-adjoint projections** on a Hilbert space $H$ is a family $\{P_1, \ldots, P_k\}$ of self-adjoint projections on $H$ such that*

$$P_1 + \ldots + P_k = \mathbb{1}.$$

We'll make frequent use of the following basic fact about complete families of self-adjoint projections:

**Lemma 11.2.13.** *If $P$ is a self-adjoint projection on a Hilbert space $H$, then*

$$\langle\psi|P|\psi\rangle = \|P\,|\psi\rangle\,\|^2.$$

*Consequently, if $\{P_1, \ldots, P_k\}$ is a complete family of self-adjoint projections on $H$, then*

$$\sum_{i=1}^{k} \|P_i\,|x\rangle\,\|^2 = \langle x|x\rangle$$

*for all $|x\rangle \in H$.*

*Proof.* If $P$ is a self-adjoint projection, then

$$\langle\psi|P|\psi\rangle = \langle|\psi\rangle\,, P\,|\psi\rangle\rangle = \langle|\psi\rangle\,, P^2\,|\psi\rangle\rangle = \langle P\,|\psi\rangle\,, P\,|\psi\rangle\rangle = \|P\,|\psi\rangle\,\|^2.$$

For the second part,

$$\sum_{i=1}^{k} \|P_i\,|x\rangle\,\|^2 = \sum_{i=1}^{k} \langle x|P_i|x\rangle = \langle x|\sum_{i=1}^{k} P_i|x\rangle = \langle x|x\rangle\,.$$

□

Although it seems like complete families of self-adjoint projections and complete families of orthogonal projections are incomparable, it turns out that, somewhat surprisingly, self-adjointness is strong enough to replace the orthogonality condition: a complete family of self-adjoint projections is a complete family of orthogonal projections.

**Lemma 11.2.14.** *If $P_1, \ldots, P_k$ are self-adjoint projections on a Hilbert space $H$ such that*

$$\sum_{i=1}^{k} P_i = \mathbb{1},$$

*then $P_i P_j = 0$ for all $1 \leq i \neq j \leq k$.*

*Proof.* Without loss of generality, we just need to show that $P_j P_1 = 0$ for all $j \neq 1$. Let $W = \operatorname{Im} P_1$. By Proposition 11.2.10, $P_1$ is the orthogonal projection onto $W$, so if $\mathcal{B}$ is an orthonormal basis for $W$, then

$$P_1 = \sum_{|x\rangle \in \mathcal{B}} |x\rangle \langle x| . \tag{11.2.3}$$

Now

$$P_1 \left( \sum_{j=1}^{k} P_j \right) P_1 = P_1 \cdot \mathbb{1} \cdot P_1 = P_1.$$

But

$$P_1 \left( \sum_{j=1}^{k} P_j \right) P_1 = P_1 \left( P_1 + \sum_{j=2}^{k} P_j \right) P_1 = P_1 + \sum_{j=2}^{k} P_1 P_j P_1.$$

Combining the last two equations, we see that

$$\sum_{j=2}^{k} P_1 P_j P_1 = 0.$$

So using Equation (11.2.3), we see that

$$\sum_{j=2}^{k} P_1 P_j P_1 = \sum_{j=2}^{k} \sum_{|x\rangle, |y\rangle \in \mathcal{B}} \langle x | P_j | y \rangle \, |x\rangle \langle y| .$$

But the set $\{|x\rangle \langle y| : |x\rangle , |y\rangle \in \mathcal{B}\}$ is a linearly independent set in $H \otimes H^* \cong \operatorname{Lin}(H, H)$, so the only way for this sum to be zero is if

$$\sum_{j=2}^{k} \langle x | P_j | y \rangle = 0$$

for all $|x\rangle, |y\rangle \in \mathcal{B}$. When $|y\rangle = |x\rangle$, we see that

$$0 = \sum_{j=2}^{k} \langle x|P_j|x\rangle = \sum_{j=2}^{k} \| P_j |x\rangle \|^2$$

for all $|x\rangle \in \mathcal{B}$. Since the summands in this sum are non-negative, this can only happen if $P_j |x\rangle = 0$ for all $2 \leq j \leq k$ and $|x\rangle \in \mathcal{B}$. Thus

$$P_j P_1 = P_j \sum_{|x\rangle \in \mathcal{B}} |x\rangle \langle x| = 0$$

for all $1 \leq j \leq k$. □

*Proof of Theorem 11.2.11.* Suppose we start with a Hilbert space direct sum $H = H_1 \oplus \cdots \oplus H_k$, and let $(P_1, \ldots, P_k)$ be the $k$-tuple of projections we get from the bijection in Theorem 11.1.7. This means that $P_i$ is the projection onto the $i$th factor with respect to this direct sum. By Corollary 11.2.7, $P_i$ is the orthogonal projection onto $H_i$, and hence $P_i$ is self-adjoint by Proposition 11.2.10. We already know from Theorem 11.1.7 that $\sum_{i=1}^{k} P_i = \mathbb{1}$, so the tuple $(P_1, \ldots, P_k)$ lies in our set.

Conversely, let $(P_1, \ldots, P_k)$ be a $k$-tuple of self-adjoint projections with $\sum_{i=1}^{k} P_i = \mathbb{1}$. By Lemma 11.2.14, $P_i P_j = 0$ if $i \neq j$, so we can apply the bijection in Theorem 11.1.7 to this tuple to get a direct sum decomposition $H = H_1 \oplus \cdots \oplus H_k$. By definition, the vector space $H_i = \operatorname{Im} P_i$. If $v \in H_i$, $w \in H_j$ with $i \neq j$, then

$$\langle v, w\rangle = \langle P_i v, P_j w\rangle = \langle v, P_i P_j w\rangle = \langle v, 0\rangle = 0,$$

so $H_i \perp H_j$. We conclude that $H = H_1 \oplus \cdots \oplus H_k$ is a Hilbert space direct sum as desired. □

## 11.3 Projective measurement

**Axiom 6.** *Let $H$ be a Hilbert space, let $\mathcal{O}$ be a finite set, and let $\{P_i\}_{i \in \mathcal{O}}$ be a complete family of self-adjoint projections indexed by $\mathcal{O}$, i.e. a family $\{P_i\}_{i \in \mathcal{O}}$ with $\sum_i P_i = \mathbb{1}$ and $P_i^* = P_i = P_i^2$ for all $1 \leq i \leq k$. Then there is a measurement associated to $\{P_i\}_{i \in \mathcal{O}}$, in which*

- *the possible outcomes of the measurement are the elements of $\mathcal{O}$,*
- *the probability of getting outcome $i$ when the system is in state $|\psi\rangle$ is*

$$\langle \psi|P_i|\psi\rangle = \| P_i |\psi\rangle \|^2, \text{ and}$$

- *the state after measuring outcome $i$ will be*
$$\frac{1}{\|P_i\left|\psi\right\rangle\|}P_i\left|\psi\right\rangle.$$

*$\{P_i\}_{i\in\mathcal{O}}$ is called a **projective measurement with outcome set $\mathcal{O}$**.*

We need to show that $\|P_i\left|\psi\right\rangle\|^2$ can be interpreted as a probability: indeed, $\|P_i\left|\psi\right\rangle\|^2 \geq 0$, and when $\left|\psi\right\rangle$ is a state,

$$\sum_{i=1}^{k}\|P_i\left|\psi\right\rangle\|^2 = \langle\psi|\psi\rangle = 1$$

by Lemma 11.2.13.

Projective measurement generalizes measurement in a basis. Indeed, suppose that $\mathcal{B} = \{\left|x_i\right\rangle : 1 \leq i \leq n\}$ is an orthonormal basis for a Hilbert space $H$. Let $P_i = \left|x_i\right\rangle\left\langle x_i\right|$. By Lemma 11.2.9, $P_i$ is a projection.

**Exercise 11.3.1.** *Show that $\{P_i\}_{1\leq i\leq n}$ is a complete family of self-adjoint projections.*

The probability of measuring outcome $i$ from state $\left|\psi\right\rangle$ is

$$\langle\psi|P_i|\psi\rangle = |\left\langle x_i|\psi\right\rangle|^2,$$

and the state after measuring outcome $i$ is

$$\frac{P_i\left|\psi\right\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}} = \frac{\langle x_i|\psi\rangle}{|\left\langle x_i|\psi\right\rangle|}\left|x_i\right\rangle.$$

So the measurement $\{P_i\}_{i=1}^n$ is equivalent to measurement in basis $\mathcal{B}$.

Finally, we can return to the case of what happens in tensor products:

**Axiom 7.** *Let $\{P_i\}_{i\in\mathcal{O}_1}$ be a projective measurement on $H_A$, and $\{Q_j\}_{j\in\mathcal{O}_2}$ be a projective measurement on $H_B$. Then the **joint measurement** on $H_A\otimes H_B$ is $\{P_i\otimes Q_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$.*

**Exercise 11.3.2.** *Show that $\{P_i\otimes Q_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is a projective measurement.*

**Exercise 11.3.3.** *Let $\mathcal{B}_1$ be a basis for $H_1$, and $\mathcal{B}_2$ be a basis for $H_2$. Show that the projective measurement*

$$\{\left|x\right\rangle\left\langle x\right| \otimes \left|y\right\rangle\left\langle x\right| : \left|x\right\rangle \in \mathcal{B}_1, \left|y\right\rangle \in \mathcal{B}_2\}$$

*is equivalent to measuring in basis*

$$\{\left|x\right\rangle\left|y\right\rangle : \left|x\right\rangle \in \mathcal{B}_1, \left|y\right\rangle \in \mathcal{B}_2\}$$

*for $H_1 \otimes H_2$.*

We can think of leaving a register unchanged as measuring in the projective measurement $\{\mathbb{1}\}$ containing only the identity operator.

**Example 11.3.4.** *Suppose we want to measure $H_A$ in basis $\mathcal{B}$ and leave $H_B$ untouched. The projective measurement for basis $\mathcal{B}$ is $\{|x\rangle\langle x|\}_{|x\rangle\in\mathcal{B}}$, so the joint measurement on $H_A \otimes H_B$ would be*

$$\{|x\rangle\langle x| \otimes \mathbb{1}\}_{|x\rangle\in\mathcal{B}}.$$

# Chapter 12

# Observables and the uncertainty principle

Let $\mathcal{O}$ be a finite set of outcomes, and let $(p_a)_{a\in\mathcal{O}}$ be a probability distribution on this set. Recall that a **(real-valued) random variable** is a function $X : \mathcal{O} \to \mathbb{R}$. The expected value of the random variable with respect to the probability distribution $(p_a)_{a\in\mathcal{O}}$ is

$$\mathbb{E}(X) = \sum_{a\in\mathcal{O}} X(a) \cdot p(a).$$

Random variables are often used to express numerical payoffs, as in the following simple example.

**Example 12.0.1.** *Consider a game where you roll a* 6*-sided die. If you roll a* 1*, you lose* 1 *dollar. If you roll a* 2*, nothing changes, If you roll a* 3*, you gain* 1 *dollar, and if you roll a* 4 *or higher, then you gain* 2 *dollars. This game could be modelled by taking* $\mathcal{O} = \{1, 2, 3, 4, 5, 6\}$ *for the possible outcomes of a dice roll, and* $p_a = 1/6$ *for* $a \in \mathcal{O}$ *to represent a fair die. The payoffs are given by the random variable* $X : \mathcal{O} \to \mathbb{R}$ *with* $X(1) = -1$*,* $X(2) = 0$*,* $X(3) = 1$*, and* $X(i) = 2$ *for* $i = 4, 5, 6$*. The expected value of* $X$ *is*

$$\mathbb{E}(X) = (-1) \cdot (1/6) + 0 \cdot (1/6) + 1 \cdot (1/6) + 2 \cdot (1/6) + 2 \cdot (1/6) + 2 \cdot (1/6) = 1.$$

*Thus if we play this game many times, we expect to gain* 1 *dollar per game played.*

There are lots of random variables in physics. Any measurement where the outcome is a real number can be regarded as a random variable. For instance, if we measure the distance a javelin is thrown in a competition, the distance travelled by the javelin can be regarded as a random variable. The probability distribution comes from the state of the system, which involves the javelin thrower (his or her training and actions leading up to the moment of release), but also things like the positions and speed of all the air molecules in the path of the javelin, none of which we know precisely. Other measurements (distance travelled, speed, energy, momentum, etc.) of pretty much every physical system can be regarded as a random variable in exactly the same way.

From this point of view, we can think of random variables in physics as measurements where the outcome is a real number. This suggests a definition of random variables in quantum probability: we can say that a random variable is a projective measurement $\{P_a : a \in \mathcal{O}\}$ such that $\mathcal{O}$ is a subset of real numbers. Since the probability of measuring outcome $a \in \mathcal{O}$ when the system is in state $|\psi\rangle$ is $\langle\psi|P_a|\psi\rangle$, the expected value of this random variable with respect to a state $|\psi\rangle$ is

$$\sum_{a\in\mathcal{O}} a \cdot \langle\psi|P_a|\psi\rangle = \langle\psi|\sum_{a\in\mathcal{O}} P_a|\psi\rangle\,. \tag{12.0.1}$$

While this is a reasonable starting definition of random variable, it can be put in a more compact form called an observable, which is what we're going to study in this section. For this, we start by reviewing some facts about eigenvectors and diagonalizability.

## 12.1 Eigenvectors and the spectral theorem

**Definition 12.1.1.** *Let $T : V \to V$ be a linear operator, and let $\lambda \in \mathbb{C}$. The $\lambda$-eigenspace of $T$ is the subspace*

$$E_\lambda(T) = \{v \in V : Tv = \lambda v\}.$$

*If $E_\lambda(T) \neq 0$, then $\lambda$ is said to be an **eigenvalue** of $T$. The non-zero elements of $E_\lambda(T)$ are called **eigenvectors** of $T$ (with eigenvalue $\lambda$).*

*$T$ is said to be **diagonalizable** if and only if there is a basis $\mathcal{B}$ for $V$ in which every element of $V$ is an eigenvector.*

There are a number of different characterizations of diagonalizable operators. We summarize some of the most important:

**Theorem 12.1.2.** *Let $T : V \to V$ be a linear operator on a vector space $V$ with eigenvalues $\lambda_1, \ldots, \lambda_k$. Then the following are equivalent:*

*(a) $T$ is diagonalizable, i.e. $V$ has a basis of consisting of eigenvectors of $T$.*

*(b) There is a basis $\mathcal{B}$ of $V$ such that $[T]_{\mathcal{B},\mathcal{B}}$ is a diagonal matrix.*

*(c) $\sum_{i=1}^{k} \dim E_{\lambda_i}(T) = \dim V$.*

*(d) $V = E_{\lambda_1}(T) \oplus \cdots \oplus E_{\lambda_k}(T)$.*

*Proof.* Parts (a)-(c) should be familiar from linear algebra, but (d) might be new, so we will sketch the proof of the equivalence of (d) with (a)-(c). If $V = E_{\lambda_1}(T) \oplus \cdots \oplus E_{\lambda_k}(T)$, and $\mathcal{B}_i$ is a basis of $E_{\lambda_i}(T)$, then $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{B}_i$ is a basis of $V$ consisting of eigenvectors of $T$, so (d) implies (a).

Conversely, suppose (c) holds, and let

$$W = \operatorname{span} \bigcup_{i=1}^{k} E_{\lambda_i}(T).$$

Suppose

$$v \in E_{\lambda_i} \cap \operatorname{span} \bigcup_{j \neq i} E_{\lambda_j}(T)$$

is a non-zero vector. Let $w_1, \ldots, w_m$ be a shortest possible sequence of vectors such that each $w_\ell$ belongs to $E_{\lambda_{j_\ell}}(T)$ for some $j_\ell \neq i$, and such that $v = w_1 + \ldots + w_m$. (Although this sequence is not unique, clearly it is possible to write $v$ in this way, so it makes sense to choose a shortest possible sequence, i.e. one where $m$ is as small as possible.) It is a fun exercise to show that by choosing the shortest possible sequence, $w_1, \ldots, w_m$ will be linearly independent. Then

$$\lambda v = T(v) = T(w_1 + \ldots + w_m) = \lambda_{j_1} w_1 + \ldots + \lambda_{j_m} w_m.$$

Then

$$\lambda w_1 + \ldots + \lambda w_m = \lambda v = \lambda_{j_1} w_1 + \ldots + \lambda_{j_m} w_m.$$

But then linear independence implies that $\lambda = \lambda_{j_\ell}$ for all $1 \leq \ell \leq m$. Since the numbers $\lambda_1, \ldots, \lambda_k$ are distinct, this is a contradiction. We conclude that

$$E_{\lambda_i} \cap \operatorname{span} \bigcup_{j \neq i} E_{\lambda_j}(T) = 0$$

for all $1 \leq i \leq k$. Hence

$$W = \bigoplus_{i=1}^{k} E_{\lambda_i}(T).$$

But by condition (c),

$$\dim W = \sum_{i=1}^{k} \dim E_{\lambda_i}(T) = \dim V,$$

so (c) implies (d). □

Because we can characterize diagonalizability in terms of direct sums, we can also characterize diagonalizability in terms of projections. This characterization is often the most useful in quantum information:

**Corollary 12.1.3.** *Let $T : V \to V$ be a linear operator. Then $T$ is diagonalizable if and only if*

$$T = \sum_{i=1}^{k} \lambda_i P_i \tag{12.1.1}$$

*for a complete family of non-zero orthogonal projections $\{P_1, \dots, P_k\}$ and distinct numbers $\lambda_1, \dots, \lambda_k$. Furthermore, if $T$ is an operator of this form, then $\lambda_1, \dots, \lambda_k$ are the eigenvalues of $T$, and $P_i$ is the projection onto the $i$th coordinate in the direct sum decomposition $V = E_{\lambda_1}(T) \oplus \cdots \oplus E_{\lambda_k}(T)$.*

*Proof.* Suppose $T$ is diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_k$ (listed without repetitions). Let $P_i$ be the projection onto the $i$th coordinate in the direct sum decomposition $V = E_{\lambda_1}(T) \oplus \cdots \oplus E_{\lambda_k}(T)$. By definition, $E_{\lambda_i}(T) \neq 0$, so $P_i \neq 0$. Thus $\{P_1, \dots, P_k\}$ is a complete family of non-zero orthogonal projections. If $v \in V$, then $P_i v \in E_{\lambda_i}(T)$, so $TP_i v = \lambda_i P_i v$. Hence

$$Tv = TP_1 v + \ldots + TP_k v = \lambda_1 P_1 v + \ldots \lambda_k P_k v.$$

So

$$T = \sum_{i=1}^{k} \lambda_i P_i.$$

Conversely, suppose $T = \sum_{i=1}^{k} \lambda_i P_i$ for some complete family of non-zero orthogonal projections $\{P_1, \dots, P_k\}$ and distinct numbers $\lambda_1, \dots, \lambda_k$. Let $V_i = \operatorname{Im} P_i$, so that $V = V_1 \oplus \cdots \oplus V_k$. If $v \in V_i$, then $P_j v = 0$ for $j \neq i$, so $Tv = \lambda_i P_i v = \lambda_i v$. So $V_i \subseteq E_{\lambda_i}(T)$. Since $P_i \neq 0$, $V_i \neq 0$, and hence $\lambda_i$ is an eigenvalue of $T$.

On the other hand, suppose $Tv = \lambda v$ for some non-zero vector $v$. Since $P_j T = \lambda_j P_j$,

$$\lambda P_j v = P_j T v = \lambda_j P_j v,$$

implying that

$$(\lambda - \lambda_j)P_j v = 0.$$

If $\lambda \neq \lambda_j$, then $P_j v = 0$. As a result, if $\lambda \neq \lambda_j$ for all $1 \leq j \leq k$, then $v = P_1 v + \ldots + P_k v = 0$, a contradiction. So $\lambda = \lambda_i$ for some $i$, and since $P_j v = 0$ for $j \neq i$, $v \in V_i$. We conclude that $\lambda_1, \ldots, \lambda_k$ is a complete list of eigenvalues of $T$, and $V_i = E_{\lambda_i}(T)$ for all $1 \leq i \leq k$. Since $V = E_{\lambda_1}(T) \oplus \cdots \oplus E_{\lambda_k}(T)$, $T$ is diagonalizable. □

Suppose

$$T = \sum_{i=1}^{k} \lambda_i P_i$$

for a complete family of orthogonal projections, but either the numbers $\lambda_1, \ldots, \lambda_k$ are not distinct, or $P_i = 0$ for some $i$. In the former case, we can assume without loss of generality that $\lambda_{k-1} = \lambda_k$. Then $\{P_1, \ldots, P_{k-2}, P_{k-1} + P_k\}$ is a complete family of orthogonal projections, and

$$T = \lambda_1 P_1 + \ldots + \lambda_{k-2} P_{k-2} + \lambda_{k-1}(P_{k-1} + P_k),$$

a sum with one fewer terms than the sum we started with. If $P_i = 0$ for some $i$, then we can assume without loss of generality that $P_k = 0$. Once again, $\{P_1, \ldots, P_{k-1}\}$ is a complete family of orthogonal projections, and

$$T = \lambda_1 P_1 + \ldots + \lambda_{k-1} P_{k-1},$$

a sum with one fewer terms. We can continue this process until we get

$$T = \sum_{i=1}^{k'} \tilde{\lambda}_i \tilde{P}_i$$

where $\{\tilde{P}_1, \ldots, \tilde{P}_k\}$ is a complete family of non-zero orthogonal projections, and $\tilde{\lambda}_1, \ldots, \tilde{\lambda}_k$ is a distinct list of numbers. Hence $T$ is diagonalizable.

**Definition 12.1.4.** *If $T$ is diagonalizable, then an expression*

$$T = \sum_{i=1}^{k} \lambda_i P_i,$$

*where $\{P_1, \ldots, P_k\}$ is a complete family of non-zero orthogonal projections and $\lambda_1, \ldots, \lambda_k$ is a list of distinct complex numbers, is called a* ***spectral decomposition*** *of $T$. The projections $P_1, \ldots, P_k$ appearing in the spectral decomposition are called the* ***spectral projections****.*

The set of eigenvalues of a linear operator $T$ is also called the **spectrum** of $T$, hence the term "spectral decomposition". Corollary 12.1.3 states that if $T = \sum_{i=1}^k \lambda_i P_i$ is a spectral decomposition, then $\lambda_1, \ldots, \lambda_k$ are the eigenvalues of $T$, and $P_1, \ldots, P_k$ are the projections onto the eigenspaces, so the spectral decomposition of $T$ is unique up to reorderings of factors. For this reason, we often speak of *the* spectral decomposition of a diagonalizable operator.

**Example 12.1.5.** *Let $T$ be diagonalizable, with spectral decomposition $T = \sum_{i=1}^k \lambda_i P_i$. Then $\mathrm{tr}(T) = \sum_{i=1}^k \lambda_i \, \mathrm{tr}(P_i)$, and since $\mathrm{tr}(P_i) = \dim \mathrm{Im}\, P_i = \dim E_{\lambda_i}(T)$, we conclude that*

$$\mathrm{tr}(T) = \sum_{i=1}^k \lambda_i \cdot \dim E_{\lambda_i}(T).$$

*In other words, the trace of a diagonalizable operator is the sum of the eigenvalues of $T$, counted with multiplicity. This is also easy to calculate from the matrix formula for trace.*

For applications in quantum probability, we are interested in diagonalizable operators $T$ on Hilbert spaces $V$ for which the projections $\{P_1, \ldots, P_k\}$ in the spectral decomposition

$$T = \sum_{i=1}^k \lambda_i P_i$$

are self-adjoint. By Theorem 11.2.11 and Corollary 12.1.3, this is the case if and only if the direct sum decomposition

$$V = E_{\lambda_1}(T) \oplus \cdots \oplus E_{\lambda_k}(T)$$

is an orthogonal direct sum. When this happens, $T$ is said to be **unitarily diagonalizable**. As a parallel to Theorem 12.1.2, we list some equivalent characterizations of unitarily diagonalizable operators:

**Theorem 12.1.6.** *Let $T : V \to V$ be a linear operator on a Hilbert space $V$ with eigenvalues $\lambda_1, \ldots, \lambda_k$. Then the following are equivalent:*

*(a) $V$ has an orthonormal basis consisting of eigenvectors of $T$.*

*(b) There is an orthonormal basis $\mathcal{B}$ of $V$ such that $[T]_{\mathcal{B},\mathcal{B}}$ is diagonal.*

*(c) $V = E_{\lambda_1}(T) \oplus \cdots \oplus E_{\lambda_k}(T)$ as a Hilbert space.*

*(d)* $T = \sum_{i=1}^{k} \lambda_i P_i$*, where* $\{P_1, \dots, P_k\}$ *is a complete family of non-zero self-adjoint projections.*

All of these properties are fairly difficult to test for by hand. One of the most important theorems in linear algebra is the *spectral theorem*, which gives a much simpler characterization of unitarily diagonalizable operators:

**Definition 12.1.7.** *Let* $H$ *be a Hilbert space. An operator* $T : H \to H$ *is* ***normal*** *if* $TT^* = T^*T$*.*

**Theorem 12.1.8** (Spectral theorem)**.** $T$ *is unitarily diagonalizable if and only if* $T$ *is normal.*

In particular, $T$ is normal if and only if $T$ has a spectral decomposition

$$T = \sum_{i=1}^{k} \lambda_i P_i$$

where $P_1, \dots, P_k$ are self-adjoint. The adjoint of $T$ is

$$T^* = \sum_{i=1}^{k} \overline{\lambda_i} P_i,$$

which is another normal operator with eigenvalues $\overline{\lambda_1}, \dots, \overline{\lambda_k}$. If $\lambda_1, \dots, \lambda_k$ are real, then $T = T^*$, so $T$ is self-adjoint. Conversely, self-adjoint operators are always normal, since if $T = T^*$, then $TT^* = T^2 = T^*T$. It turns out that self-adjoint operators are exactly the normal operators with real eigenvalues:

**Lemma 12.1.9.** *A normal operator* $T$ *has real eigenvalues if and only if* $T^* = T$*. As a result,* $T$ *is self-adjoint if and only if* $T$ *has a spectral decomposition*

$$T = \sum_{i=1}^{k} \lambda_i P_i$$

*where* $\lambda_1, \dots, \lambda_k$ *are distinct real numbers, and* $\{P_1, \dots, P_k\}$ *is a complete family of non-zero self-adjoint projections.*

*Proof.* We've already shown that a normal operator with real eigenvalues is self-adjoint. Suppose that $T^* = T$. Let $T = \sum_i \lambda_i P_i$ be the spectral decomposition of $T$, so that $T^* = \sum_i \overline{\lambda_i} P_i$. Then

$$\lambda_i P_i = P_i T = P_i T^* = \overline{\lambda_i} P_i$$

for all $1 \leq i \leq k$. Since $P_i \neq 0$, we conclude that $\overline{\lambda_i} = \lambda_i$. □

**Example 12.1.10.** *Continuing Example 12.1.5, we see that if $T$ is self-adjoint, then* $\operatorname{tr}(T) \in \mathbb{R}$.

If we ask for the eigenvalues $\lambda_1, \ldots, \lambda_k$ in Lemma 12.1.9 to be ordered (say in increasing order), then the spectral decomposition of a self-adjoint operator will be unique (without having to worry about reordering of the eigenvalues). So we can conclude from Lemma 12.1.9 that:

**Corollary 12.1.11.** *For any finite subset $\mathcal{O} \subset \mathbb{R}$, spectral decomposition gives a bijection between complete families of non-zero self-adjoint projections $\{P_a : a \in \mathcal{O}\}$ indexed by $\mathcal{O}$, and self-adjoint operators $T$ with spectrum (set of eigenvalues) $\mathcal{O}$.*

**Exercise 12.1.12.** *Extend Corollary 12.1.11 by showing that spectral decomposition gives a bijection between complete families of (possibly zero) self-adjoint projections $\{P_a : a \in \mathcal{O}\}$, and self-adjoint operators $T$ with eigenvalues contained in $\mathcal{O}$.*

## 12.2 Observables

We started out with a provisional definition of a real-valued random variable as a projective measurement $\{P_a : a \in \mathcal{O}\}$ on $H$ where the index set $\mathcal{O}$ is contained in $\mathbb{R}$. However, Corollary 12.1.11 states that such a measurement can be expressed just by giving a self-adjoint operator on $H$, a much more compact representation. To distinguish random variables in this form from random variables in regular probability, we use a new term:

**Definition 12.2.1.** *An **(real-valued) observable** on a Hilbert space $H$ is a self-adjoint operator $T : H \to H$.*

**Exercise 12.2.2.** *Show that*

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

*are observables on $H = \mathbb{C}^2$, and find their spectral decomposition.*

It might seem funny to have another name for self-adjoint operators, but when we use the term observable for a self-adjoint operator $T$, we indicate that we should think of $T$ as specifying a projective measurement via the spectral decomposition. The outcome set of this projective measurement is the set of eigenvalues of $T$.

**Lemma 12.2.3.** *Let $T$ be an observable on $H$. The expected value of the observable $T$ on state $|\psi\rangle$ is*

$$\langle\psi|T|\psi\rangle\,,$$

*and the variance is*

$$\langle\psi|T^2|\psi\rangle - (\langle\psi|T|\psi\rangle)^2$$

*Proof.* Suppose $T$ has spectral decomposition $T = \sum_{\lambda\in\mathcal{O}} \lambda P_\lambda$, where $\mathcal{O}$ is the set of eigenvalues of $T$, and $P_\lambda$ is the orthogonal projection onto $E_\lambda(T)$. As in Equation (12.0.1), the probability of measuring outcome $\lambda$ is $\langle\psi|P_\lambda|\psi\rangle$, so that the expected value is

$$\sum_{\lambda\in\mathcal{O}} \lambda\,\langle\psi|P_\lambda|\psi\rangle = \langle\psi|\sum_{\lambda\in\mathcal{O}} \lambda P_\lambda|\psi\rangle = \langle\psi|T|\psi\rangle\,.$$

The variance of a random variable $X$ is defined to be $\mathbb{E}(X^2) - \mathbb{E}(X)^2$. Thus the variance of the observable $T$ is

$$\sum_{\lambda\in\mathcal{O}} \lambda^2\,\langle\psi|P_\lambda|\psi\rangle - (\langle\psi|T|\psi\rangle)^2,$$

where

$$\sum_{\lambda\in\mathcal{O}} \lambda^2\,\langle\psi|P_\lambda|\psi\rangle = \langle\psi|\sum_{\lambda\in\mathcal{O}} \lambda^2 P_\lambda|\psi\rangle = \langle\psi|T^2|\psi\rangle\,.$$

□

This proof uses the following exercise:

**Exercise 12.2.4.** *Suppose $T$ is a diagonalizable operator with spectral decomposition $T = \sum_{i=1}^k \lambda_i P_i$. Show that $T^n = \sum_{i=1}^k \lambda_i^n P_i$ for all $n \geq 1$.*

The variance of a random variable is $\mathbb{E}(X^2) - \mathbb{E}(X)^2$, but this is also equal to $\mathbb{E}((X-\mu)^2)$, where $\mu = \mathbb{E}(X)$. Consequently, this also holds for observables. Indeed, if $T$ is an observable with expectation $\mu = \langle\psi|T|\psi\rangle$, then

$$\langle\psi|(T-\mu)^2|\psi\rangle = \langle\psi|T^2|\psi\rangle - 2\mu\,\langle\psi|T|\psi\rangle + \mu^2\,\langle\psi|\psi\rangle = \langle\psi|T^2|\psi\rangle - \mu^2. \quad (12.2.1)$$

If $T$ is self-adjoint, then we can also think of the expectation $\langle\psi|T|\psi\rangle$ as a hermitian form evaluated at $|\psi\rangle$:

**Exercise 12.2.5.** *Suppose $T : H \to H$ is linear, and let $\mathcal{B}$ be an orthonormal basis of $H$. Show that*

$$H \times H \to \mathbb{C} : (u, v) \mapsto \langle u, Tv\rangle$$

*is a sesquilinear form with matrix $[T]_{\mathcal{B},\mathcal{B}}$, and that this form is hermitian if and only if $T$ is self-adjoint.*

It's worth asking whether normal elements also have a place in quantum probability, since there is a bijection between normal elements and projective measurements indexed by finite subsets of $\mathbb{C}$. In fact, we can think of normal elements as the analogue of complex-valued random variables.

**Definition 12.2.6.** *A* ***(complex-valued) observables*** *on a Hilbert space $H$ is a normal operator $T : H \to H$.*

By default, we'll use the term observable to refer to a real-valued observable.

## 12.3 The uncertainty principle

Now that we've defined observables, we can look at one of the defining features of quantum mechanics: the uncertainty principle. First, we need the following definition:

**Definition 12.3.1.** *Let $S$ and $T$ be linear operators on a Hilbert space $H$. The* ***commutator*** *of $S$ and $T$ is*

$$[S, T] := ST - TS,$$

*while the* ***anticommutator*** *is*

$$\{S, T\} := ST + TS.$$

*$S$ and $T$ are said to* ***commute*** *if $[S, T] = 0$ (or equivalently if $ST = TS$), and* ***anticommute*** *if $\{S, T\} = 0$ (or equivalently if $ST = -TS$).*

There are a number of different versions of the uncertainty principle; we'll prove the following:

**Theorem 12.3.2** (Schrödinger's uncertainty principle)**.** *Let $X$ and $Y$ be two observables on a Hilbert space $H$, and let $|\psi\rangle$ be a state in $H$. Let $\mu_X$ and $\mu_Y$ be the expected values of $X$ and $Y$ respectively with state $|\psi\rangle$, and let $\sigma_X^2$ and $\sigma_Y^2$ be the variances. Then*

$$\sigma_X^2\sigma_Y^2 \geq |\,\langle\psi|\frac{1}{2}\{X, Y\} - \mu_X\mu_Y\mathbb{1}|\psi\rangle\,|^2 + |\,\langle\psi|\frac{1}{2}[X, Y]|\psi\rangle\,|^2.$$

*Proof.* Let $\tilde{X} = X - \mu_X\mathbb{1}$ and $\tilde{Y} = Y - \mu_Y\mathbb{1}$. Then

$$\tilde{X}^* = X^* - \overline{\mu}\mathbb{1} = X - \mu\mathbb{1} = \tilde{X},$$

and $\tilde{Y}^* = \tilde{Y}$ similarly. By Equation (12.2.1),

$$\sigma_X^2 = \langle\psi|\tilde{X}^2|\psi\rangle \text{ and } \sigma_Y^2 = \langle\psi|\tilde{Y}^2|\psi\rangle\,.$$

Using the Cauchy-Schwarz inequality and the fact that $\tilde{X}$ is self-adjoint, we get

$$|\left\langle\psi|\tilde{X}\tilde{Y}|\psi\right\rangle|^2 = |\langle\tilde{X}\,|\psi\rangle\,,\tilde{Y}\,|\psi\rangle\rangle|^2 \leq \|\tilde{X}\,|\psi\rangle\,\|^2\|\tilde{Y}\,|\psi\rangle\,\|^2 = \sigma_X^2\sigma_Y^2.$$

Let $z = \langle\psi|\tilde{X}\tilde{Y}|\psi\rangle$. Then

$$|z|^2 = (|\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 = \left|\frac{z+\overline{z}}{2}\right|^2 + \left|\frac{z-\overline{z}}{2}\right|^2.$$

Now for any operator $A$ and vector $v$, $\overline{\langle v, Av\rangle} = \langle Av, v\rangle = \langle v, A^*v\rangle$. Since $(\tilde{X}\tilde{Y})^* = \tilde{Y}^*\tilde{X}^* = \tilde{Y}\tilde{X}$,

$$z+\overline{z} = \langle\psi|\tilde{X}\tilde{Y}|\psi\rangle + \overline{\langle\psi|\tilde{X}\tilde{Y}|\psi\rangle} = \langle\psi|\tilde{X}\tilde{Y}|\psi\rangle + \langle\psi|\tilde{Y}\tilde{X}|\psi\rangle = \langle\psi|\{\tilde{X},\tilde{Y}\}|\psi\rangle\,.$$

We can then calculate

$$\{\tilde{X},\tilde{Y}\} = (X-\mu_X\mathbb{1})(Y-\mu_Y\mathbb{1})+(Y-\mu_Y\mathbb{1})(X-\mu_X\mathbb{1}) = XY+YX-2\mu_XY-2\mu_YX+2\mu_X\mu_Y\mathbb{1},$$

so

$$\begin{aligned}\frac{z+\overline{z}}{2} &= \langle\psi|\frac{1}{2}\{X,Y\}|\psi\rangle - \mu_X\left\langle\psi|Y|\psi\right\rangle - \mu_Y\left\langle\psi|X|\psi\right\rangle + \mu_X\mu_Y\\ &= \langle\psi|\frac{1}{2}\{X,Y\}|\psi\rangle - \mu_X\mu_Y\\ &= \langle\psi|\frac{1}{2}\{X,Y\} - \mu_X\mu_Y\mathbb{1}|\psi\rangle\,.\end{aligned}$$

Similarly

$$\frac{z-\overline{z}}{2} = \frac{1}{2}\Big(\langle\psi|\tilde{X}\tilde{Y}|\psi\rangle - \langle\psi|\tilde{Y}\tilde{X}|\psi\rangle\Big) = \langle\psi|\frac{1}{2}[\tilde{X},\tilde{Y}|\psi\rangle\,,$$

and we can calculate that

$$[\tilde{X},\tilde{Y}] = (X-\mu_X\mathbb{1})(Y-\mu_Y\mathbb{1}) - (Y-\mu_Y\mathbb{1})(X-\mu_X\mathbb{1}) = XY-YX = [X,Y].$$

So putting everything together, we see that

$$|\left\langle\psi|\frac{1}{2}\{X,Y\} - \mu_X\mu_Y\mathbb{1}|\psi\right\rangle|^2 + |\left\langle\psi|\frac{1}{2}[X,Y]|\psi\right\rangle|^2 = |z|^2 \leq \sigma_X^2\sigma_Y^2.$$

□

The Schrödinger uncertainty relation implies the simpler Robertson uncertainty relation:

**Corollary 12.3.3.** *Let $X$ and $Y$ be two observables on a Hilbert space $H$, and let $|\psi\rangle$ be a state in $H$. Let $\sigma_X^2$ and $\sigma_Y^2$ be the variances with state $|\psi\rangle$ of $X$ and $Y$ respectively. Then*

$$\sigma_X \sigma_Y \geq |\, \langle\psi|\frac{1}{2}[X, Y]|\psi\rangle \,|.$$

In particular, the Robertson uncertainty relation tells us that if $X$ and $Y$ don't commute, then there is always a state such that $\sigma_X \sigma_Y > 0$.

**Exercise 12.3.4.** *(a) Show that if $T : H \to H$ is linear, then*

$$\langle\psi|T|\psi\rangle = 0 \textit{ for all states } |\psi\rangle \in H$$

*if and only if $T = 0$.*

*(b) Suppose $X$ and $Y$ are observables on a Hilbert space $H$ with $[X, Y] \neq 0$. Use part (a) to show that there is a state $|\psi\rangle \in H$ such that $\sigma_X$ and $\sigma_Y$ are both non-zero, where $\sigma_X^2$ and $\sigma_Y^2$ are the variances of $X$ and $Y$ respectively.*

In the most famous application of the uncertainty relation, $X$ is the position operator and $Y$ is the momentum operator. In this case, $[X, Y] = i\hbar\mathbb{1}$ for a positive constant $\hbar$ called the *reduced Planck constant*. In this case, the Robertson uncertainty relation states that

$$\sigma_X \sigma_Y \geq |\, \langle\psi|\frac{i\hbar\mathbb{1}}{2}|\psi\rangle \,| = \frac{\hbar}{2}$$

for any state $|\psi\rangle$. So as the uncertainty about $\sigma_X$ gets close to zero, the uncertainty $\sigma_Y$ about $Y$ must rise accordingly, and vice-versa. Unfortunately, this is not a feature of quantum mechanics we can see in finite-dimensional systems:

**Exercise 12.3.5.** *Let $X$ and $Y$ be observables on a finite-dimensional Hilbert space.*

*(a) Show that $i[X, Y]$ is a real-valued observable with $\operatorname{tr}(i[X, Y]) = 0$.*

*(b) Show that if $Z$ is a real-valued observable with $\operatorname{tr}(Z) = 0$, then there is a state $|\psi\rangle$ with $\langle\psi|Z|\psi\rangle = 0$.*

*(c) Conclude that there is a state $|\psi\rangle$ with $\langle\psi|[X,Y]|\psi\rangle = 0$.*

The Schrödinger uncertainty relation is not always the strongest relation we can prove on the uncertainties:

**Exercise 12.3.6.** *Let $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be operators on $\mathbb{C}^2$.*

*(a) Show that $Z$ and $X$ are observables, and that the anticommutator $\{X, Z\} = 0$.*

*(b) Show that $\sigma_X^2 \sigma_Z^2 = 0$ on a state $|\psi\rangle \in \mathbb{C}^2$ if and only if $|\psi\rangle$ is an eigenvalue of $X$ or $Z$.*

*(c) Show that $\sigma_X^2 + \sigma_Z^2 \geq 1$ for all states $|\psi\rangle \in \mathbb{C}^2$.*

## 12.4 Compatible measurements

If $X$ and $Y$ are non-commuting observables, then the uncertainty principle gives a quantitative lower bound on the product $\sigma_X^2 \sigma_Y^2$ of the variances of $X$ and $Y$ for certain states. We can also look at what it means for $X$ and $Y$ to commute qualitatively. This is connected to the order that we apply measurements in. To see this, first suppose that $P = \{P_i\}_{i \in \mathcal{O}_1}$ and $Q = \{Q_j\}_{j \in \mathcal{O}_2}$ are two projective measurements on a Hilbert space $H$. If the system is in state $|\psi\rangle$, and we apply measurement $Q$, then we get outcome $j \in \mathcal{O}_2$ with probability $\|Q_j |\psi\rangle \|^2$, after which the system will be in state

$$\frac{Q_j |\psi\rangle}{\|Q_j |\psi\rangle \|}.$$

If we then apply measurement $P$, we'll get outcome $i \in \mathcal{O}_1$ with probability

$$\left\| P_i \frac{Q_j |\psi\rangle}{\|Q_j |\psi\rangle \|} \right\|^2 = \frac{\|P_i Q_j |\psi\rangle \|^2}{\|Q_j |\psi\rangle \|^2},$$

and the state after measurement will be

$$\frac{\|Q_j |\psi\rangle \|}{\|P_i Q_j |\psi\rangle \|} \frac{P_i Q_j |\psi\rangle}{\|Q_j |\psi\rangle \|} = \frac{P_i Q_j |\psi\rangle}{\|P_i Q_j |\psi\rangle \|}.$$

Thinking about this process as a black box, we see that we get outcome $(i, j) \in \mathcal{O}_1 \times \mathcal{O}_2$ with probability

$$\|Q_j |\psi\rangle \|^2 \cdot \frac{\|P_i Q_j |\psi\rangle \|^2}{\|Q_j |\psi\rangle \|^2} = \|P_i Q_j |\psi\rangle \|^2,$$

and the state after measurement will be

$$\frac{P_iQ_j\left|\psi\right\rangle}{\|P_iQ_j\left|\psi\right\rangle\|}.$$

On the other hand, if we apply measurement $P$ first and then measurement $Q$, by symmetry we'll get outcome $(i,j)\in\mathcal{O}_1\times\mathcal{O}_2$ with probability

$$\|Q_jP_i\left|\psi\right\rangle\|^2,$$

and the state after measurement will be

$$\frac{Q_jP_i\left|\psi\right\rangle}{\|Q_jP_i\left|\psi\right\rangle\|}.$$

When is measuring in $Q$ and then $P$ the same as measuring in $P$ and then $Q$ in all states $\left|\psi\right\rangle$? From our calculations, this happens if and only if

$$\|P_iQ_j\left|\psi\right\rangle\| = \|Q_jP_i\left|\psi\right\rangle\| \text{ and } \frac{P_iQ_j\left|\psi\right\rangle}{\|P_iQ_j\left|\psi\right\rangle\|} = \frac{Q_jP_i\left|\psi\right\rangle}{\|Q_jP_i\left|\psi\right\rangle\|}$$

for all states $\left|\psi\right\rangle$. Clearly these two conditions are equivalent to having

$$P_iQ_j\left|\psi\right\rangle = Q_jP_i\left|\psi\right\rangle$$

for all states (and hence all vectors) $\left|\psi\right\rangle\in H$. But this happens if and only if $P_iQ_j=Q_jP_i$ for all $i$ and $j$.

**Definition 12.4.1.** *We say that two projective measurements $\{P_i\}_{i\in\mathcal{O}_1}$ and $\{Q_j\}_{j\in\mathcal{O}_2}$ on a Hilbert space $H$ are **compatible** if, for all input states in $H$, measuring with $Q$ and then with $P$ gives the same probability distribution on outcomes and output states as measuring with $P$ and then with $Q$. The two measurements **commute** if $[P_i,Q_j]=0$ for all $i\in\mathcal{O}_1$, $j\in\mathcal{O}_2$.*

In the argument above, we've proven the following proposition:

**Proposition 12.4.2.** *Two projective measurements on a Hilbert space $H$ are compatible if and only if they commute.*

We can also characterize compatible measurements without looking at the output state:

**Exercise 12.4.3.** *Suppose $P=\{P_i\}_{i\in\mathcal{O}_1}$ and $Q=\{Q_j\}_{j\in\mathcal{O}_2}$ are projective measurements on a Hilbert space $H$. Show that $P$ and $Q$ are compatible if and only if whenever we measure in $P$, then measure in $Q$, and then measure in $P$ again, the first measurement in $P$ always gives the same outcome as the last measurement in $P$.*

This characterization of compatibility in terms of outcomes only is useful if we want to verify that two measurements are compatible, since we can't see the output state of a measurement directly.

Notice that measurement with $Q$ and then with $P$ is a measurement process, since it returns an outcome, and our description of this measurement process satisfies the criterion we gave in Chapter 4, since we've given a set of possible outcomes $\mathcal{O}_1 \times \mathcal{O}_2$, a probability distribution over outcomes, and a way of determining the output state of the system, given the outcome of the measurement. When $P$ and $Q$ commute, we can think of this process as measuring $P$ and $Q$ together, without having to specify which measurement is performed first. It turns out that in this case, we can also describe this measurement process as a projective measurement:

**Proposition 12.4.4.** *If $\{P_i\}_{i\in\mathcal{O}_1}$ and $\{Q_j\}_{j\in\mathcal{O}_2}$ are projective measurements on a Hilbert space $H$, then $\{P_iQ_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is a projective measurement if and only if $\{P_i\}_{i\in\mathcal{O}_1}$ and $\{Q_j\}_{j\in\mathcal{O}_2}$ are compatible. If they are compatible, then $\{P_iQ_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is equivalent to the process of applying both measurements.*

For the proof, we need the following lemma:

**Lemma 12.4.5.**

1. *If $P$ and $Q$ are commuting projections on a vector space $V$, then $PQ$ is also a projection.*

2. *If $V$ is a Hilbert space and $P$ and $Q$ are self-adjoint projections, then $PQ$ is self-adjoint if and only if $PQ = QP$.*

*Proof.* If $P$ and $Q$ commute, then $(PQ)^2 = PQPQ = P^2Q^2 = PQ$. If $P$ and $Q$ are self-adjoint, $(PQ)^* = Q^*P^* = QP$, so $(PQ)^* = PQ$ if and only if $PQ = QP$. □

*Proof of Proposition 12.4.4.* Suppose $\{P_iQ_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is a projective measurement. Then $P_iQ_j$ is self-adjoint, so the measurements are compatible by Lemma 12.4.5.

Suppose the measurements are compatible. By Lemma 12.4.5, $\{P_iQ_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is a family of self-adjoint projections. We can add that

$$\sum_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2} P_iQ_j = \left(\sum_{i\in\mathcal{O}_1} P_i\right)\left(\sum_{j\in\mathcal{O}_2} Q_j\right) = \mathbb{1},$$

so $\{P_iQ_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is indeed a projective measurement. On state $|\psi\rangle$, applying this measurement will give outcome $(i,j)$ with probability

$$\|P_iQ_j\,|\psi\rangle\,\|^2,$$

after which the state will be

$$\frac{P_i Q_j \left|\psi\right\rangle}{\|P_i Q_j \left|\psi\right\rangle\|}.$$

We've already observed that this is the same as measuring with both $Q$ and $P$. □

When do two observables $X$ and $Y$ specify compatible measurements? The answer turns out that this happens if and only if $X$ and $Y$ commute. To prove this, we need the following standard lemma which shows how to find the spectral projections of a diagonalizable operator $T$ in terms of $T$:

**Lemma 12.4.6.** *Let $T$ be a diagonalizable operator on a Hilbert space $H$ with spectral decomposition*

$$T = \sum_{i=1}^{k} \lambda_i P_i.$$

*Then*

$$P_i = \frac{\prod_{j\neq i}(T - \lambda_j \mathbb{1})}{\prod_{j\neq i}(\lambda_i - \lambda_j)}.$$

*Proof.* Since we haven't specified an order on the eigenvalues, it's enough to prove the formula for $i = 1$. Since

$$T - \lambda_j \mathbb{1} = \sum_{\ell=1}^{k} (\lambda_\ell - \lambda_j) P_\ell,$$

$$\begin{aligned}\prod_{j=2}^{k}(T - \lambda_j \mathbb{1}) &= \left(\sum_{\ell_2=1}^{k}(\lambda_{\ell_2} - \lambda_2)P_{\ell_2}\right)\left(\sum_{\ell_3=1}^{k}(\lambda_{\ell_3} - \lambda_3)P_{\ell_3}\right)\cdots\left(\sum_{\ell_k=1}^{k}(\lambda_{\ell_k} - \lambda_k)P_{\ell_k}\right)\\ &= \sum_{\ell_2=1}^{k}\sum_{\ell_3=1}^{k}\cdots\sum_{\ell_k=1}^{k}(\lambda_{\ell_2} - \lambda_2)\cdots(\lambda_{\ell_k} - \lambda_k)P_{\ell_2}\cdots P_{\ell_k}.\end{aligned}$$

But $P_i P_j = 0$ if $i \neq j$, so $P_{\ell_2}\cdots P_{\ell_k} = 0$ unless $\ell_2 = \ell_3 = \ldots = \ell_k$. So we can write

$$\prod_{j=2}^{k}(T - \lambda_j \mathbb{1}) = \sum_{\ell=1}^{k}(\lambda_l - \lambda_2)(\lambda_l - \lambda_3)\cdots(\lambda_l - \lambda_k)P_\ell.$$

But if $\ell \neq 1$, then $\lambda_\ell - \lambda_\ell$ occurs in the product $(\lambda_\ell - \lambda_2) \cdots (\lambda_\ell - \lambda_k)$, and hence this product is 0. So we conclude that

$$\prod_{j=2}^{k} (T - \lambda_j \mathbb{1}) = (\lambda_1 - \lambda_2)(\lambda_1 - \lambda_3) \cdots (\lambda_1 - \lambda_k) P_1.$$

□

**Proposition 12.4.7.** *Let $X$ and $Y$ be observables on a Hilbert space $H$, with spectral decompositions*

$$X = \sum_{i=1}^{m} \lambda_i P_i \text{ and } Y = \sum_{j=1}^{n} \delta_j Q_j$$

*respectively. Then $\{P_i\}_{i=1}^m$ and $\{Q_j\}_{j=1}^n$ are compatible if and only if $X$ and $Y$ commute.*

*Proof.* Suppose $\{P_i\}_{i=1}^m$ and $\{Q_j\}_{j=1}^n$ are compatible, so $[P_i, Q_j] = 0$ for all $1 \leq i \leq m$, $1 \leq j \leq n$. Then

$$XY = \sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_i \delta_j P_i Q_j = \sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_i \delta_j Q_j P_i = \sum_{j=1}^{n} \delta_j Q_j \sum_{i=1}^{m} \lambda_i P_i = YX.$$

Conversely, suppose $XY = YX$. Given $1 \leq i \leq m$ and $1 \leq j \leq n$, let

$$\Lambda = \prod_{k \neq i} (\lambda_i - \lambda_k) \text{ and } \Delta = \prod_{\ell \neq j} (\delta_\ell - \delta_j).$$

For any $1 \leq k \leq m$ and $1 \leq \ell \leq n$,

$$\begin{aligned} (X - \lambda_k \mathbb{1})(Y - \delta_\ell \mathbb{1}) &= XY - \lambda_k X - \delta_\ell Y + \lambda_k \delta_\ell \mathbb{1} \\ &= YX - \lambda_k X - \delta_\ell Y + \lambda_k \delta_\ell \mathbb{1} \\ &= (Y - \delta_\ell \mathbb{1})(X - \lambda_k \mathbb{1}). \end{aligned}$$

So $(X - \lambda_k \mathbb{1}) \prod_{\ell \neq j} (Y - \delta_\ell \mathbb{1}) = \prod_{\ell \neq j} (Y - \delta_\ell \mathbb{1})(X - \lambda_k \mathbb{1})$, and ultimately

$$P_i Q_j = \Delta^{-1} \prod_{k \neq i} (X - \lambda_k \mathbb{1}) \Lambda^{-1} \prod_{\ell \neq j} (Y - \delta_\ell \mathbb{1}) = \Lambda^{-1} \prod_{\ell \neq j} (Y - \delta_\ell \mathbb{1}) \Delta^{-1} \prod_{k \neq i} (X - \lambda_k \mathbb{1}) = Q_j P_i.$$

We conclude that the measurements specified by $X$ and $Y$ are compatible. □

There is one more way to understand compatible measurements, and that is in terms of simultaneous diagonalizability.

**Definition 12.4.8.** *Let $\mathcal{S}$ be a subset of $\operatorname{Lin}(V, V)$ for some vector space $V$. We say that $\mathcal{S}$ is **simultaneously diagonalizable** if there is a basis $\mathcal{B}$ of $V$ such that for $\mathcal{B}$ is a subset of the eigenvectors of $T$ for every $T \in \mathcal{S}$. If $V$ is a Hilbert space, we say that $\mathcal{S}$ is **simultaneously unitarily diagonalizable** if there is an orthonormal basis satisfying this condition.*

**Example 12.4.9.** *Consider the linear transformations $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ on $\mathbb{C}^2$. Then $\{e_1, e_2\}$ is an orthonormal basis for $\mathbb{C}^2$, and $e_1$ and $e_2$ are eigenvectors of both $\mathbb{1}$ and $Z$, so $\{\mathbb{1}, Z\}$ is jointly unitarily diagonalizable.*

*Note that $e_2$ is an eigenvector of both $\mathbb{1}$ and $Z$, but the eigenvector corresponding to $e_2$ doesn't have to be the same for both operators.*

You might have seen in a previous linear algebra course that a subset $\mathcal{S}$ of $\operatorname{Lin}(V, V)$ is jointly diagonalizable if and only if all the elements of $\mathcal{S}$ are diagonalizable, and the elements pairwise commute. This theorem can be proven easily for a finite number of linear operators using spectral decompositions. We show how to do this for two observables:

**Theorem 12.4.10.** *Let $X$ and $Y$ be observables on a Hilbert space $H$. Then the following are equivalent:*

*(a) $X$ and $Y$ are simultaneously unitarily diagonalizable.*

*(b) There is a complete family of self-adjoint projections $\{P_1, \ldots, P_n\}$ and scalars $\alpha_i, \beta_i \in \mathbb{R}$, $1 \leq i \leq n$, such that*

$$X = \sum_{i=1}^{n} \alpha_i P_i \text{ and } Y = \sum_{i=1}^{n} \beta_i P_i.$$

*(c) $X$ and $Y$ commute.*

*Proof.* Suppose (a) holds, so there is an orthonormal basis

$$\mathcal{B} = \{|v_1\rangle, \ldots, |v_n\rangle\}$$

of $H$ such that the elements of $\mathcal{B}$ are eigenvectors of both $X$ and $Y$. Let $P_i = |v_i\rangle \langle v_i|$, and note that $P_i$ is a projection by Corollary 11.2.7. Using Corollary 11.2.7 again, $\sum_i P_i$ is the orthogonal projection onto $H$, and hence is the identity operator. So $\{P_1, \ldots, P_n\}$ is a complete family of self-adjoint projections. Suppose $\alpha_i$ is the eigenvalue of $|v_i\rangle$ for $X$. Then

$$P_i |v_j\rangle = \langle v_i | v_j\rangle |v_i\rangle = \delta_{ij} |v_i\rangle,$$

so

$$X \sum_{j=1}^{n} c_j \left|v_j\right\rangle = \sum_{j=1}^{n} c_i j \alpha_j \left|v_j\right\rangle = \left(\sum_{i=1}^{n} \alpha_i P_i\right) \left(\sum_{j=1}^{n} c_j \left|v_j\right\rangle\right)$$

for any scalars $c_1, \ldots, c_n$. We conclude that

$$X = \sum_{i=1}^{n} \alpha_i P_i,$$

and similarly

$$Y = \sum_{i=1}^{n} \beta_i P_i,$$

where $\beta_i$ is the eigenvalue of $\left|v_i\right\rangle$ for $Y$. Hence (a) implies (b).

Now suppose (b) holds. Let $\mathcal{B}_i$ be an orthonormal basis for $\operatorname{Im} P_i$. If $\left|v\right\rangle \in \mathcal{B}_i$, then $X\left|v\right\rangle = \alpha_i \left|v\right\rangle$ and $Y\left|v\right\rangle = \beta_i \left|v\right\rangle$. Since $H = \operatorname{Im} P_1 \oplus \ldots \oplus \operatorname{Im} P_n$, $\bigcup_{i=1}^{n} \mathcal{B}_i$ is an orthonormal basis for $H$, in which every vector is an eigenvector of both $X$ and $Y$. So (a) holds.

Continuing with the assumption that (b) holds, since $P_iP_j = 0$ for $i \neq j$ we have that

$$XY = \sum_{i,j} \alpha_i \beta_j P_i P_j = \sum_{i,j} \alpha_i \beta_i P_i = \sum_{i,j} \alpha_i \beta_j P_j P_i = YX,$$

so (c) holds as well.

Finally, suppose (c) holds. Let $X = \sum_{i=1}^{k} \lambda_i P_i$ and $Y = \sum_{j=1}^{\ell} \delta_j Q_j$ be the spectral decompositions. Since $X$ and $Y$ commute,

$$\{P_iQ_j : 1 \leq i \leq k, 1 \leq j \leq \ell\}$$

is a complete family of self-adjoint projections, by Propositions 12.4.4 and 12.4.7. Let $\alpha_{ij} = \lambda_i$ and $\beta_{ij} = \delta_j$. Then

$$X = \sum_{i,j} \alpha_{ij} P_i Q_j \text{ and } Y = \sum_{i,j} \beta_{ij} P_i Q_j,$$

so (b) holds. □

The expressions for $X$ and $Y$ in part (b) of this theorem is sometimes called a joint spectral decomposition. Note that it is not unique, and is not necessarily the same as the spectral decomposition of $X$ or $Y$, since we haven't required the eigenvalues $\lambda_i$ and $\delta_i$ to be unique. The proof of the theorem shows that one way to get a joint spectral decomposition of $X$ and $Y$ is to take the projective measurement corresponding to measuring both $X$ and $Y$.

Although we've only looked at the case of two observables, all the arguments can be adapted to the case of $k$ observables:

**Exercise 12.4.11.** *Let $X_1, \ldots, X_k$ be observables on a Hilbert space $H$. Extend the arguments in this section to show that the following are equivalent:*

*(a)* $[X_i, X_j] = 0$ *for all* $1 \leq i, j \leq k$.

*(b) If we apply all of these measurements in some order, then the distribution on outcomes and output states that we get is independent of the order chosen.*

*(c)* $\{X_1, \ldots, X_k\}$ *is simultaneously unitarily diagonalizable.*

*(d) There is a complete family of self-adjoint projections* $\{P_1, \ldots, P_m\}$, *and scalars* $\lambda_{ij} \in \mathbb{R}$, $1 \leq i \leq k$, $1 \leq j \leq m$, *such that*

$$X_i = \sum_{j=1}^{m} \lambda_{ij} P_j \textit{ for all } 1 \leq i \leq k.$$

# Chapter 13

# Entanglement and Bell's theorem

We've seen that a system with two quantum registers, given by Hilbert spaces $H_1$ and $H_2$, has Hilbert space $H_1 \otimes H_2$. This axiom applies even if the registers are in distant locations. We also have an axiom stating that, if we measure the first system with projective measurement $\{P_i\}_{i \in \mathcal{O}_1}$, and the second system with projective measurement $\{Q_j\}_{j \in \mathcal{O}_2}$, then the joint measurement on $H_1 \otimes H_2$ is $\{P_i \otimes Q_j\}_{(i,j) \in \mathcal{O}_1 \times \mathcal{O}_2}$.

What happens if we do a measurement like this? If the system is in state $|\psi_1\rangle \otimes |\psi_2\rangle$, then the probability of getting outcome $(i, j)$ from the joint measurement is

$$\langle\psi_1| \langle\psi_2| P_i \otimes Q_j |\psi_1\rangle |\psi_2\rangle = \langle\psi_1|P_i|\psi_1\rangle \langle\psi_1|Q_j|\psi_2\rangle,$$

the probability of getting outcome $i$ times the probability of getting outcome $j$. With a product state, the outcomes are independent, which is what we'd expect from two independent labs in two different locations.

However, not all states on $H_1 \otimes H_2$ are product states. We've also seen that the system $H_1 \otimes H_2$ can contain entangled states like

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathbb{C}\{0,1\} \otimes \mathbb{C}\{0,1\}.$$

To see why entanglement is interesting, suppose $H_1 = H_2 = \mathbb{C}\{0,1\}$, and let $P_0 = Q_0 = |0\rangle\langle 0|$, $P_1 = Q_1 = |1\rangle\langle 1|$, so that $\{P_0, P_1\}$ is measurement in the computational basis. Let $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then the probability of getting outcome $(0,0)$ is

$$\frac{1}{2}\left(\langle 00| + \langle 11|\right) |0\rangle\langle 0| \otimes |0\rangle\langle 0| \left(|00\rangle + |11\rangle\right) = \frac{1}{2}\left(\langle 00| + \langle 11|\right) |00\rangle\langle 00| \left(|00\rangle + |11\rangle\right) = \frac{1}{2}.$$

Similarly, the probability of getting outcome $(0, 1)$ is

$$\frac{1}{2}\left(\langle 00| + \langle 11|\right)|0\rangle\langle 0| \otimes |1\rangle\langle 1|\left(|00\rangle + |11\rangle\right) = \frac{1}{2}\left(\langle 00| + \langle 11|\right)|01\rangle\langle 01|\left(|00\rangle + |11\rangle\right) = 0.$$

Filling in the rest of the table, we get that

| $i$ | $j$ | $\langle\psi\|P_i \otimes Q_j\|\psi\rangle$ |
|---|---|---|
| 0 | 0 | 1/2 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1/2 |

(A faster way to see this is to apply Exercise 11.3.3.) In other words, the outcomes are totally correlated, so the results of the measurements are not independent. This is why we say that the state is entangled. We might find this surprising for measurements made in two separate labs. If the labs are on adjacent floors of a building, we might try to explain this by saying that the labs aren't insulated from each other, and the measurements are interferring with each other. However, we might find this behaviour very startling if the labs are in distant locations.

Of course, such behaviour is not unique to quantum mechanics. There are lots of examples of physical systems and states where measurement outcomes can be correlated without referring to quantum mechanics. For instance, suppose every morning we record someone's sock colour. We can regard each foot as a subsystem of a joint system, and record the colour for each foot independently. However, we wouldn't be suprised if most of the time the socks are the same colour. Clearly this person is just picking out matched socks when they get dressed in the morning.

What if we did the same measurement with two seemingly unconnected people, recording the colour of the sock from the left foot of the first person, and the right foot of the second person. Now we'd be pretty surprised if the sock colours were always the same. But if we found out the people were married, then we'd have an explanation: the married couple pick out socks of the same colour each morning. This would be a little eccentric, but not startling from a physics point of view. Even if there's no such readily available explanation, we could imagine that there's an explanation of this form (maybe the people choose their sock colour according to the weather forecast, which they get from the same website).

Correlations of this type can be explained well by what are called **local hidden variable (LHV)** models. In an LHV model, we assume that any quantity that we can measure is determined by the values of a collection of variables, which we may or may not be able to measure directly. These variables are local, in the sense that they reside in a particular location, and can be read or changed by entities in the same location. For instance, we might think of the velocity of a particular particle as residing in that particle, so the velocity is only affected by forces at the location of the particle.

For our sock example, we might have a variable for each sock. In our model for the married couple, we imagine that they choose their sock colour when they are in the same location, after which point the sock colour is fixed. Two people choosing their sock colour based on the weather forecast might never be in the same location. However, we could still give a LHV model for this situation by adding a variable for the weather forecast, which they both have access to when they check the forecast website. (Of course, we have to explain why accessing the website counts as being in the same location as the weather forecast variable. If we wanted to be really strict, we could make a model that includes all the electrons, photons, etc. that are involved in accessing the website, to make that clear.)

For the entangled state $|\psi\rangle$ above, if we only measure in the computational basis, then there's no problem coming up with LHV models that can explain our measurement results: it's just a special case of our sock scenario, with two possible colours for the sock, colour 0 and colour 1. It makes sense to ask whether there are correlations that can arise from entangled states which can't be described with LHV models. In this chapter, we'll look at a framework for answering this type of question first introduced by John Bell. We'll use a modern version of Bell's framework called nonlocal games. In particular, we'll prove Bell's theorem that there are correlations which arise from entanglement that can't be described with LHV models.

## 13.1 Nonlocal games

A nonlocal game is a simple game we can use to study entanglement. In a nonlocal game, we have two players, called Alice and Bob, and a referee. The referee sends a question $x$ (drawn from a finite set $\mathcal{I}_A$) to Alice, and a question $y$ (drawn from another finite set $\mathcal{I}_B$) to Bob. Alice replies with an answer $a$ (drawn from a finite set $\mathcal{O}_A$), and Bob replies with an answer $b$ (drawn from a finite set $\mathcal{O}_B$). The referee looks at $x$, $y$, $a$, and $b$, and then decides whether the players win or lose. Hence a non-local game is specified by

- finite sets $\mathcal{O}_A$, $\mathcal{O}_B$, $\mathcal{I}_A$, and $\mathcal{I}_B$ giving the possible answers and questions for the players,
- a function $V : \mathcal{O}_A \times \mathcal{O}_B \times \mathcal{I}_A \times \mathcal{I}_B \to \{0,1\}$ specifying the winning condition, where 1 corresponds to a win, and 0 to a loss, and
- a probability distribution $\pi$ on $\mathcal{I}_A \times \mathcal{I}_B$ giving the probability that the referee asks question $(x, y)$.

The rules of the game (even the probability distribution $\pi$) are public, and thus are known to the players Alice and Bob, who want to cooperate to win. Thus they can look at the rules ahead of time, and decide on a strategy. However, the game is complicated by the fact that during the game, the players are separated by cannot communicate while the game is in progress. In particular, Alice does not know which question Bob receives or what he answers, and similarly Bob does not know Alice's question or answer. In practice, the referee can prevent Alice and Bob from communicating by placing them far apart, and then requiring their answers immediately after giving them their questions. If the time between the referee and giving them their questions and receiving their answers is shorter than the time it would take to travel from Alice to Bob at the speed of light, then any communication would contradict the law of relativity that no signal can travel faster than the speed of light.

What can the players do in a nonlocal game? If we assume that any strategy can be described by a LHV model, then the players answers will be completely determined by the input they receive, and some hidden variable taking values in set $\Lambda$. Thus a **LHV strategy** for a nonlocal game consists of

- a set $\Lambda$ giving the possible values of the hidden variable,
- two functions $a : \mathcal{I}_A \times \Lambda \to \mathcal{O}_A$ and $b : \mathcal{I}_B \times \Lambda \to \mathcal{O}_B$ giving Alice and Bob's answers for each input and value of the hidden variable, and
- a probability distribution $\{r_\lambda\}_{\lambda \in \Lambda}$ describing the distribution of the hidden variable.

The winning probability for a nonlocal game $(\mathcal{O}_A, \mathcal{O}_B, \mathcal{I}_A, \mathcal{I}_B, V, \pi)$ with such a strategy $\mathcal{S}$ is

$$\omega(\mathcal{S}) := \sum_{\lambda \in \Lambda} r_\lambda \sum_{(i,j) \in \mathcal{I}_A \times \mathcal{I}_B} \pi(i,j) V(a(i,\lambda), b(j,\lambda), i, j),$$

since $V(a, b, i, j)$ is the probability that Alice and Bob win given that they receive inputs $(i, j)$ and return outputs $(a, b)$.

**Definition 13.1.1.** *The **classical winning probability** of a nonlocal game $\mathcal{G} = (\mathcal{O}_A, \mathcal{O}_B, \mathcal{I}_A, \mathcal{I}_B, V, \pi)$ is*

$$\omega_c(\mathcal{G}) := \sup_{\mathcal{S}} \ \omega(\mathcal{S}),$$

*where the supremum is over LHV strategies $\mathcal{S}$ for $\mathcal{G}$.*

An LHC strategy is said to be **deterministic** if $|\Lambda| = 1$. In this case, there's no point in writing $a$ and $b$ as a function of $\Lambda$, or in giving the probability distribution over $\Lambda$, so a deterministic strategy $\mathcal{S}$ just consists of two functions $a : \mathcal{I}_A \to \mathcal{O}_A$ and $b : \mathcal{I}_A \to \mathcal{O}_B$, and the winning probability of the strategy will be

$$\omega(\mathcal{S}) := \sum_{(i,j) \in \mathcal{I}_A \times \mathcal{I}_B} \pi(i,j) V(a(i), b(j), i, j).$$

**Proposition 13.1.2.** *If $\mathcal{G}$ is a nonlocal game, then $\omega_c(\mathcal{G})$ is attained by a deterministic strategy, i.e. there is a deterministic strategy $\mathcal{S}$ such that $\omega_c(\mathcal{G}) = \omega(\mathcal{S})$.*

*Proof.* Suppose $\mathcal{G} = (\mathcal{O}_A, \mathcal{O}_B, \mathcal{I}_A, \mathcal{I}_B, V, \pi)$, and let $\mathcal{S} = (\Lambda, a, b, r)$ be an LHV strategy for $\mathcal{G}$. For each $\lambda \in \Lambda$, let $\mathcal{S}_\lambda$ be the deterministic strategy $(a_\lambda, b_\lambda)$, where $a_\lambda(i) = a(i, \lambda)$ and $b_\lambda(j) = b(j, \lambda)$. Then

$$\omega(\mathcal{S}) = \sum_{\lambda \in \Lambda} r_\lambda \sum_{(i,j) \in \mathcal{I}_A \times \mathcal{I}_B} \pi(i,j) V(a(i,\lambda), b(j,\lambda), i, j) = \sum_{\lambda \in \Lambda} r_\lambda \omega(\mathcal{S}_\lambda) \leq \sup_{\lambda \in \Lambda} \omega(\mathcal{S}_\lambda).$$

Thus

$$\sup_{\mathcal{S} \text{ deterministic}} \omega(\mathcal{S}) \leq \omega_c(\mathcal{G}) := \sup_{\mathcal{S} \text{ LHC}} \omega(\mathcal{S}) \leq \sup_{\mathcal{S} \text{ deterministic}} \omega(\mathcal{S}),$$

so we see that $\omega_c(\mathcal{G})$ is the supremum of winning probabilities $\omega(\mathcal{S})$ over deterministic strategies $\mathcal{S}$. But $\mathcal{I}_A$, $\mathcal{I}_B$, $\mathcal{O}_A$, and $\mathcal{O}_B$ are finite, so there are only finitely many functions $\mathcal{I}_A \to \mathcal{O}_A$ and $\mathcal{I}_A \to \mathcal{I}_B$, and hence only finitely many deterministic strategies. Since a supremum over a finite set is always attained, we conclude that there is a deterministic strategy $\mathcal{S}$ with $\omega_c(\mathcal{G}) = \omega(\mathcal{S})$. □

**Exercise 13.1.3.** *Suppose Alice and Bob are allowed to use randomness to pick their answer, so instead of having functions $a$ and $b$ giving their answer, we instead have probability distributions $a(i, \lambda)$ and $b(j, \lambda)$ over $\mathcal{O}_A$ and $\mathcal{O}_B$ respectively. Show that Alice and Bob cannot do better than $\omega_c(\mathcal{G})$ with such a strategy.*

What are the possible strategies allowed by quantum probability? Since Alice and Bob are physically separated during the game, we must have Hilbert spaces $H_A$ and $H_B$ for Alice and Bob's subsystems respectively. The state of the system at the beginning of the game is some unit vector $|\psi\rangle \in H_A \otimes H_B$. The questions and answers are inputs and outputs to the system. Once they get their intput, they have to produce an output, and this can be thought of as a measurement. Thus a **quantum strategy $\mathcal{S}$** for a nonlocal game $\mathcal{G} = (\mathcal{O}_A, \mathcal{O}_B, \mathcal{I}_A, \mathcal{I}_B, V, \pi)$ consists of

- Hilbert spaces $H_A$ and $H_B$,
- for each $i \in \mathcal{I}_A$, a projective measurements $\{P_a^i\}_{a \in \mathcal{O}_A}$,
- for each $j \in \mathcal{I}_B$, a projective measurement $\{Q_b^j\}_{b \in \mathcal{O}_B}$, and
- a state $|\psi\rangle \in H_A \otimes H_B$.

Since the probability of getting outcome $(a, b)$ on input $(i, j)$ is

$$\langle\psi| P_a^i \otimes Q_b^j |\psi\rangle \,,$$

the winning probability on strategy $\mathcal{S}$ is

$$\omega(\mathcal{S}) = \sum_{(i,j) \in \mathcal{I}_A \times \mathcal{I}_B} \pi(i,j) \sum_{(a,b) \in \mathcal{O}_A \times \mathcal{O}_B} V(a,b,i,j) \, \langle\psi| P_a^i \otimes Q_b^j |\psi\rangle \,.$$

**Definition 13.1.4.** *The **quantum winning probability** of a nonlocal game $\mathcal{G} = (\mathcal{O}_A, \mathcal{O}_B, \mathcal{I}_A, \mathcal{I}_B, V, \pi)$ is*

$$\omega_q(\mathcal{G}) := \sup_{\mathcal{S}} \ \omega(\mathcal{S}),$$

*where the supremum is over quantum strategies.*

## 13.2 The CHSH game

Consider the nonlocal game CHSH $= (\mathcal{O}_A, \mathcal{O}_B, \mathcal{I}_A, \mathcal{I}_B, V, \pi)$ with

- $\mathcal{I}_A = \mathcal{I}_B = \{0, 1\}$,
- $\mathcal{O}_A = \mathcal{O}_B = \{1, -1\}$,
- winning function

$$V(a,b,i,j) = \begin{cases} 1 & ab = (-1)^{ij} \\ 0 & \text{otherwise} \end{cases},$$

- and $\pi(i,j) = \frac{1}{4}$ for all $i, j \in \{0,1\}$.

Although this winning condition looks complicated, it simply says that when $i = j = 1$, the players win when $a \neq b$, while otherwise the players win when $a = b$. The probability distribution is $\pi(i,j) = 1/4$ for all $i, j$, so all questions are asked with equal probability. This game is called the **CHSH game**, after its inventors Clauser, Horne, Shimony, and Holt.

**Proposition 13.2.1.** *$\omega_c(\text{CHSH}) = 3/4$.*

*Proof.* By Proposition 13.1.2, we only need to check deterministic strategies. Since there are $2^2 = 4$ possible functions from $\{0,1\} \to \{0,1\}$, there are $4 \cdot 4 = 16$ possible deterministic strategies, and we can check them all by hand. For instance, if the players always output 1 on every input, then the winning probability will be

$$\frac{1}{4}(V(1,1,0,0) + V(1,1,0,1) + V(1,1,1,0) + V(1,1,1,1)) = \frac{3}{4}.$$

We leave it as an exercise to verify that no other deterministic strategy does better than 3/4. □

**Proposition 13.2.2.** *$\omega_q(\text{CHSH}) \geq \frac{1}{2} + \frac{1}{2\sqrt{2}}$.*

To prove this proposition, all we need to do is give a quantum strategy that achieves $\frac{1}{2} + \frac{1}{2\sqrt{2}}$. However, it is a bit nicer to use the following lemma, and give the measurements of the strategy in terms of observables:

**Lemma 13.2.3.** *Suppose*

$$\mathcal{S} = \big(H_A, H_B, \{\{P^i_1, P^i_{-1}\} \mid i = 0,1\}, \{\{Q^j_1, Q^j_{-1}\} \mid j = 0,1\}, |\psi\rangle\big)$$

*is a quantum strategy for the CHSH game. Let*

$$A_i = P^i_1 - P^i_{-1} \text{ and } B_j = Q^j_1 - Q^j_{-1}$$

*be the observable corresponding to measurements $\{P^i_{\pm 1}\}$ and $\{Q^j_{\pm 1}\}$ respectively. Then $\omega(\mathcal{S}) = (\beta(\mathcal{S}) + 1)/2$, where*

$$\beta(\mathcal{S}) := \frac{1}{4}\langle\psi| A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1 |\psi\rangle$$

The number $\beta(\mathcal{S})$ is called the **winning bias** of the strategy.

*Proof.* Since

$$P_1^i \otimes Q_1^j + P_1^i \otimes Q_{-1}^j + P_{-1}^i \otimes Q_1^j + P_{-1}^i \otimes Q_{-1}^j = \mathbb{1},$$

we have that

$$P_1^i \otimes Q_1^j + P_1^i \otimes Q_{-1}^j = \mathbb{1} - P_{-1}^i \otimes Q_1^j - P_{-1}^i \otimes Q_{-1}^j,$$

and hence

$$\begin{aligned} 2(P_1^i \otimes Q_1^j + P_{-1}^i \otimes Q_{-1}^j) &= (P_1^i \otimes Q_1^j + P_{-1}^i \otimes Q_{-1}^j) + (\mathbb{1} - P_1^i \otimes Q_{-1}^j + P_{-1}^i \otimes Q_1^j) \\ &= (P_1^i - P_{-1}^i) \otimes (Q_1^j - Q_{-1}^j) + \mathbb{1} \\ &= A_i \otimes B_j + \mathbb{1}. \end{aligned}$$

Also

$$2(P_1^i \otimes Q_{-1}^j + P_{-1}^i \otimes Q_1^j) = 2\mathbb{1} - 2(P_1^i \otimes Q_1^j + P_{-1}^i \otimes Q_{-1}^j) = \mathbb{1} - A_i \otimes B_j.$$

So

$$\begin{aligned} \omega(\mathcal{S}) &= \frac{1}{4} \sum_{i,j \in \{0,1\}} \sum_{a,b \in \{\pm 1\}} V(a,b,i,j) \langle \psi | P_a^i \otimes Q_b^j | \psi \rangle \\ &= \frac{1}{4} \langle \psi | \left( P_1^0 \otimes Q_1^0 + P_{-1}^0 \otimes Q_{-1}^0 \right) + \left( P_1^0 \otimes Q_1^1 + P_{-1}^0 \otimes Q_{-1}^1 \right) \\ &\qquad + \left( P_1^1 \otimes Q_1^0 + P_{-1}^1 \otimes Q_{-1}^0 \right) + \left( P_1^1 \otimes Q_{-1}^1 + P_{-1}^1 \otimes Q_1^1 \right) | \psi \rangle \\ &= \frac{1}{4} \langle \psi | \frac{1}{2}(A_0 \otimes B_0 + \mathbb{1}) + \frac{1}{2}(A_0 \otimes B_1 + \mathbb{1}) \\ &\qquad + \frac{1}{2}(A_1 \otimes B_0 + \mathbb{1}) + \frac{1}{2}(\mathbb{1} - A_0 \otimes B_1) \\ &= \frac{1}{8} \langle \psi | A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1 + 4\mathbb{1} | \psi \rangle \\ &= \frac{1}{2}(\beta(\mathcal{S}) + 1). \end{aligned}$$

□

*Proof of Proposition 13.2.2.* Let $Z$ and $X$ be the observables on $\mathbb{C}\{0,1\}$ with matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

respectively in the computational basis. This means that

$$Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle, X|0\rangle = |1\rangle, \text{ and } X|1\rangle = |0\rangle.$$

By Exercise 12.2.2, these are observables with eigenvalues ±1. Let

$$A_0 = Z, A_1 = X, B_0 = \frac{Z+X}{\sqrt{2}}, \text{ and } B_1 = \frac{Z-X}{\sqrt{2}}.$$

We can also check, using the matrices of $B_0$ and $B_1$ in the computational basis, that both are observables with eigenvalues $\{\pm 1\}$. Hence $A_i$ and $B_j$, $i, j \in \{0,1\}$, specify projective measurements with outcome set $\{\pm 1\}$.

Let $\mathcal{S}$ be the strategy with Hilbert spaces $H_A = H_B = \mathbb{C}\{0,1\}$, measurements given by $A_i$ and $B_j$, $i, j \in \{0,1\}$, and state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Then

$$\begin{aligned}\beta(\mathcal{S}) &= \frac{1}{4}\langle\psi|A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1|\psi\rangle \\ &= \frac{1}{4\sqrt{2}}\langle\psi|Z \otimes (Z+X) + Z \otimes (Z-X) + X \otimes (Z+X) - X \otimes (Z-X)|\psi\rangle \\ &= \frac{1}{4\sqrt{2}}\langle\psi|2Z \otimes Z + 2X \otimes X|\psi\rangle = \frac{1}{2\sqrt{2}}\langle\psi|Z \otimes Z + X \otimes X|\psi\rangle .\end{aligned}$$

Using the formulas for $Z$ and $X$, we can calculate that

$$Z \otimes Z\,|\psi\rangle = \frac{|00\rangle + (-1)^2\,|11\rangle}{\sqrt{2}} = |\psi\rangle$$

and

$$X \otimes X\,|\psi\rangle = \frac{|11\rangle + |00\rangle}{\sqrt{2}} = |\psi\rangle ,$$

so

$$\beta(\mathcal{S}) = \frac{1}{2\sqrt{2}}\left(\langle\psi|Z \otimes Z|\psi\rangle + \langle\psi|X \otimes X|\psi\rangle\right) = \frac{1}{2\sqrt{2}}\left(\langle\psi|\psi\rangle + \langle\psi|\psi\rangle\right) = \frac{1}{\sqrt{2}},$$

and

$$\omega(\mathcal{S}) = \frac{1}{2} + \frac{\beta\mathcal{S}}{2} = \frac{1}{2} + \frac{1}{2\sqrt{2}}.$$

□

Since $\frac{1}{2} + \frac{1}{2\sqrt{2}} > \frac{3}{4}$, we get:

**Corollary 13.2.4** (Bell's theorem)**.** *There are nonlocal games $\mathcal{G}$ for which $\omega_q(\mathcal{G}) > \omega_c(\mathcal{G})$.*

In other words, Bell's theorem states that for some nonlocal games, we can do better with entanglement than with LHV strategies. There have been many experiments done to verify Bell's theorem, including some with the CHSH game. Thus we can say (assuming that relativity is correct and it is not possible to communicate faster than the speed of light) that there are physical systems whose states cannot be described with LHV models.

**Exercise 13.2.5.** *Use Lemma 13.2.3 to show that* $\omega_q(\mathrm{CHSH}) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$.

# Chapter 14

# Density matrices and generalized measurements

## 14.1 Coarse-graining and ensembles of states

Consider the quantum state

$$|\psi\rangle = |0\rangle + |1\rangle + |2\rangle + 2\,|3\rangle$$

in the Hilbert space $H = \mathbb{C}\{0,1,2,3\}$. If we measure this state in the computational basis, then we get outcomes $i = 0, 1, 2$ with probability $1/7$, and outcome 3 with probability $4/7$ (this reflects the fact that before using our state in calculations, we must normalize it by dividing by $\sqrt{1+1+1+2^2} = \sqrt{7}$).

Suppose when we measure this state, we are not interested in exactly what outcome we get, but only whether the outcome belongs to group $A = \{0,1\}$, or group $B = \{2,3\}$. If we imagine measurement as being done by a device where we hit a button, and then look at a screen which shows one of 0, 1, 2, or 3, then we can just as well imagine a new device where we modify the screen, so that if it would have showed 0 or 1, it now shows $A$, and if it would have showed 2 or 3, it now shows $B$.

We can think of this new device as an abstract measurement process which, on state $|\psi\rangle$, returns outcome $A$ with probability $2/7$, and outcome $B$ with probability $5/7$. However, an abstract measurement process should include a rule for determining the state after measurement. If we only know whether the outcome is $A$ or $B$, then we cannot determine the state exactly. To allow us to express the rule for determining the state, we need a new definition:

**Definition 14.1.1.** *An* ***ensemble of states*** *in a Hilbert space $H$ is a finite* *collection*

$$\{(p_i, |\psi_i\rangle) : i \in I\},$$

*where* $|\psi_i\rangle$ *is a state in* $H$ *for all* $i \in I$, $p_i \in \mathbb{R}_{\geq 0}$ *for all* $i \in I$, *and*

$$\sum_{i \in I} p_i = 1.$$

In other words, an ensemble of states is a probability distribution on a finite set of states. (If we are willing to work with probability distributions on infinite sets, then it's easy to generalize this concept to infinite ensembles as well.) We use ensembles whenever we have a situation where we prepare or get different quantum states with different probabilities. If $I = \{1, \ldots, k\}$, then often we write ensembles as

$$\{p_1 : |\psi_1\rangle, p_2 : |\psi_2\rangle, \ldots, p_k : |\psi_k\rangle\}.$$

A single unit vector $|\psi\rangle$ in a Hilbert space can be thought of as the ensemble $\{1 : |\psi\rangle\}$. Ensembles of this form are said to be **pure**.

In our example, if we get outcome $A$, then the state is either $|0\rangle$ or $|1\rangle$, with equal probability. So we can say that the output state after measuring $A$ is the ensemble $\{1/2 : |0\rangle, 1/2 : |1\rangle\}$. Similarly, if the output is $B$, then the output state is the ensemble $\{1/5 : |2\rangle, 4/5 : |3\rangle\}$.

In general, if we have an abstract measurement process with outcome set $\mathcal{O}$, and $\{\mathcal{O}_i : i \in I\}$ is a partition of $\mathcal{O}$, then we can make a new measurement process whose outcome set is $I$, by returning outcome $i \in I$ whenever the outcome of the original process is in $\mathcal{O}_i$. The state after measuring outcome $i \in I$ will be an ensemble of the states for outcome $o \in \mathcal{O}_i$. This process of making a new measurement by discarding information is called **coarse-graining** the original measurement.

**Example 14.1.2.** *Let* $H = \mathbb{C}\{1, 2, 3, 4\}$. *Measurement in the computational basis (call this process* $\mathcal{M}$*) has outcome set* $\mathcal{O} = \{1, 2, 3, 4\}$. *Suppose we partition* $\mathcal{O}$ *into* $\mathcal{O}_A = \{1, 2\}$ *and* $\mathcal{O}_B = \{3, 4\}$. *The coarse-graining of* $\mathcal{M}$ *with respect to this partition is the measurement process in which we first measure in the computational basis to get outcome* $a$, *output either* $A$ *if* $a \in \mathcal{O}_A$ *or* $B$ *if* $a \in \mathcal{O}_B$, *and then forget* $a$.

*If we measure* $|\psi\rangle = |1\rangle + |2\rangle + |3\rangle$ *with this coarse-grained measurement, we'll get outcome* $A$ *with probability* $2/3$ *and outcome* $B$ *with probability* $1/3$. *If we get outcome* $B$, *then the state after measurement must be* $|3\rangle$, *but if we get outcome* $A$ *then the state after measurement has an equal probability of being in state* $|1\rangle$ *or* $|2\rangle$. *So we can describe the state after measurement with the ensemble* $\{1/2 : |1\rangle, 1/2 : |2\rangle\}$.

The ensemble $E = \{1/2 : |0\rangle, 1/2 : |1\rangle\}$ of states in $\mathbb{C}\{0,1\}$ is in state $|0\rangle$ with probability 1/2, and in state $|1\rangle$ with probability 1/2. So measuring this ensemble in the computational basis gives outcome 0 with probability 1/2, and outcome 1 with probability 1/2. So ensemble $E$ should remind us of the state $|0\rangle + |1\rangle$. However, being in superposition of $|0\rangle$ and $|1\rangle$ is very different from in ensemble $E$:

**Exercise 14.1.3.** *Show that measuring the ensemble $E$ with respect to the Hadamard basis $\{|+\rangle, |-\rangle\}$ gives outcomes $+$ and $-$ with equal probability. Observe that this is different from measuring $|+\rangle = |0\rangle + |1\rangle$ in the Hadamard basis.*

The idea of just returning whether outcome is in $A$ or $B$ is also similar to performing the projective measurement $\{P_A, P_B\}$, where

$$\operatorname{Im} P_A = \operatorname{span}\{|0\rangle, |1\rangle\} \text{ and } \operatorname{Im} P_B = \operatorname{span}\{|2\rangle, |3\rangle\}.$$

Given a state $|\psi\rangle$, this projective measurement will give outcomes $A$ and $B$ with the same probability as measuring in the computational basis and coarse-graining the measurement as described above. However, the outcome states won't be the same. For instance, if we measure $|\psi\rangle = |0\rangle + |1\rangle + |2\rangle + 2|3\rangle$ and get outcome $A$ from the projective measurement, then the state after measurement will be $|0\rangle + |1\rangle$. So Exercise 14.1.3 shows that the projective measurement is different than the coarse-grained measurement. So we can't get out of using ensembles by using projective measurements.

## 14.2 Generalized measurements

In this chapter, we're going to cover density matrices, which are a compact way to work with ensembles. However, before getting to density matrices, note that we have a similar situation going on with measurements, where by combining measurements we can make abstract measurement operators which are not projective measurements. For instance, in Section 12.4, we looked at measuring with a projective measurement $\{Q_j\}_{j \in \mathcal{O}_2}$, followed by measuring with a projective measurement $\{P_i\}_{i \in \mathcal{O}_1}$. This is an abstract measurement process with outcome set $\mathcal{O}_1 \times \mathcal{O}_2$, where we get outcome $(i, j)$ on state $|\psi\rangle$ with probability

$$\frac{\|P_i Q_j |\psi\rangle\|}{\|Q_j |\psi\rangle\|} \cdot \|Q_j |\psi\rangle\| = \|\|P_i Q_j |\psi\rangle\|^2,$$

and the state after measurement will be

$$\frac{P_i Q_j \left|\psi\right\rangle}{\left\| P_i Q_j \left|\psi\right\rangle \right\|}.$$

In Proposition 12.4.4, we showed that $\{P_i Q_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is a projective measurement if and only if $\{P_i\}_{i\in\mathcal{O}_1}$ and $\{Q_j\}_{j\in\mathcal{O}_2}$ are compatible. But even if they're not compatible, we should be able to perform a sequence of measurements. For that reason, we make the following definition:

**Definition 14.2.1.** *A* ***generalized measurement*** *with outcome set $\mathcal{O}$ on a Hilbert space $H$ is a family $\{A_i\}_{i\in\mathcal{O}}$ where each $A_i$ is a linear transformation $H \to H$, and*

$$\sum_{i\in\mathcal{O}} A_i^* A_i = \mathbb{1}.$$

We think of a generalized measurement process $\{A_i\}_{i\in\mathcal{O}}$ as the abstract measurement process with outcome set $\mathcal{O}$, where the probability of measuring outcome $i$ on state $\left|\psi\right\rangle$ is

$$\left\| A_i \left|\psi\right\rangle \right\|^2 = \left\langle \psi \middle| A_i^* A_i \middle| \psi \right\rangle,$$

and the state after measuring outcome $i$ will be

$$\frac{A_i \left|\psi\right\rangle}{\left\| A_i \left|\psi\right\rangle \right\|}.$$

To see where the condition that $\sum_{i\in\mathcal{O}} A_i^* A_i = \mathbb{1}$ comes from:

**Exercise 14.2.2.** *Show that $\sum_{i\in\mathcal{O}} \left\| A_i \left|\psi\right\rangle \right\|^2 = 1$ for all states $\left|\psi\right\rangle \in H$ if and only if $\sum_{i\in\mathcal{O}} A_i^* A_i = \mathbb{1}$.*

In other words, the condition $\sum_{i\in\mathcal{O}} A_i^* A_i = \mathbb{1}$ is exactly the condition needed to get that $\left\| A_i \left|\psi\right\rangle \right\|^2$ defines a probability distribution on $\mathcal{O}$ for all states $\left|\psi\right\rangle$.

**Exercise 14.2.3.** *Show that if $\{P_i\}_{i\in\mathcal{O}_1}$ and $\{Q_j\}_{j\in\mathcal{O}_2}$ are projective measurements on a Hilbert space $H$, then $\{P_i Q_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is a generalized measurement, and the corresponding abstract measurement process is equivalent to measuring in $\{Q_j\}_{j\in\mathcal{O}_2}$, followed by $\{P_i\}_{i\in\mathcal{O}_1}$.*

Generalized measurements capture both types of processes we've learned about so far. Indeed, projective measurements are clearly generalized measurements. And if $U$ is a unitary operator, then $U^* U = \mathbb{1}$, so $\{U\}$ is a generalized measurement (with an outcome set of size 1). If we measure in $\{U\}$ (let's say the outcome set is $\{\varepsilon\}$), then we get outcome $\varepsilon$ with probability 1 irregardless of the input state $|\psi\rangle$, and the state after measurement will be $U|\psi\rangle$. Since we don't gain any information from the measurement, no information leaves the system, and so this measurement is equivalent to closed time evolution by $U$.

It turns out that if we combine generalized measurements, then we also get a generalized measurement:

**Proposition 14.2.4.** *Let $\{A_i\}_{i\in\mathcal{O}_1}$ and $\{B_j\}_{j\in\mathcal{O}_2}$ be generalized measurements. Then $\{A_iB_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is a generalized measurement, corresponding to measuring in $\{B_j\}_{j\in\mathcal{O}_2}$ and then in $\{A_i\}_{i\in\mathcal{O}_1}$.*

*Proof.* To see that $\{A_iB_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$ is a generalized measurement, we just need to calculate

$$\begin{aligned}\sum_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}(A_iB_j)^*A_iB_j &= \sum_{j\in\mathcal{O}_2}\sum_{i\in\mathcal{O}_1}B_j^*A_i^*A_iB_j \\ &= \sum_{j\in\mathcal{O}_2}B_j^*\left(\sum_{i\in\mathcal{O}_1}A_i^*A_i\right)B_j \\ &= \sum_{j\in\mathcal{O}_2}B_j^*B_j = \mathbb{1}.\end{aligned}$$

If the system starts in state $|\psi\rangle$, and we measure in $\{B_j\}_{j\in\mathcal{O}_2}$, we get $j$ with probability $\|B_j|\psi\rangle\|^2$, after which the state will be

$$\frac{B_j|\psi\rangle}{\|B_j|\psi\rangle\|}.$$

If we then measure in $\{A_i\}_{i\in\mathcal{O}}$, we'll get outcome $i$ with probability

$$\left\|\frac{A_iB_j|\psi\rangle}{\|B_j|\psi\rangle\|}\right\|^2 = \frac{\|A_iB_j|\psi\rangle\|^2}{\|B_j|\psi\rangle\|^2},$$

so the overall probability of getting $(i,j)\in\mathcal{O}_1\times\mathcal{O}_2$ will be

$$\|B_j|\psi\rangle\|^2\cdot\frac{\|A_iB_j|\psi\rangle\|^2}{\|B_j|\psi\rangle\|^2} = \|A_iB_j|\psi\rangle\|^2,$$

and the state after measurement will be

$$\frac{\|B_j|\psi\rangle\|}{\|A_iB_j|\psi\rangle\|}\cdot\frac{A_iB_j|\psi\rangle}{\|B_j|\psi\rangle\|} = \frac{A_iB_j|\psi\rangle}{\|A_iB_j|\psi\rangle\|}.$$

Hence measuring in $\{B_j\}_{j\in\mathcal{O}_2}$ and then in $\{A_i\}_{i\in\mathcal{O}_1}$ is equivalent to measuring in $\{A_iB_j\}_{(i,j)\in\mathcal{O}_1\times\mathcal{O}_2}$. □

As a result of Proposition 14.2.4, everything we can do by combining projective measurements and unitary operations is a generalized measurement. There are still limits to what we can express with a generalized measurement, however. For instance, if we apply a generalized measurement to a pure ensemble, then the state after measurement is also a pure ensemble, so there's no way to represent coarse-grained measurements as a generalized measurement.

## 14.3 Positive semidefinite operators

Given a basis $\mathcal{B}$ for an $n$-dimensional space $V$, and an $n \times n$ matrix $M$, we know that we can specify a sesquilinear form on $V$ by $(x, y) = [x]^*_{\mathcal{B}} M [y]_{\mathcal{B}}$. We can think of a form defined in this way as the pullback of the sesquilinear form defined by $M$ on $\mathbb{C}^n$ by the isomorphism $V \to \mathbb{C}^n$ given by $\mathcal{B}$. More generally, if $T : V \to W$ is a linear transformation, and we have a sesquilinear form on $V$, then the pullback gives us a form on $V$.

If $H$ is a Hilbert space, and $T : H \to H$ is a linear transformation, then we have another way to define a sesquilinear form on $H$ from $T$:

**Lemma 14.3.1.** *Let $T : H \to H$ be a linear transformation on a Hilbert space $H$. Then*

$$(x, y) = \langle x, Ty \rangle$$

*is a sesquilinear form on $H$. Furthermore, if $\mathcal{B}$ is an orthonormal basis, then the matrix of $(,)$ with respect to $\mathcal{B}$ is $[T]_{\mathcal{B},\mathcal{B}}$.*

*Proof.* Since $\mathcal{B}$ is orthonormal,

$$(x, y) = \langle x, Ty \rangle = [x]^*_{\mathcal{B}} [Ty]_{\mathcal{B}} = [x]^*_{\mathcal{B}} [T]_{\mathcal{B},\mathcal{B}} [y]_{\mathcal{B}}.$$

By Theorem 3.1.11, $(,)$ is sesquilinear, and $[T]_{\mathcal{B},\mathcal{B}}$ is the matrix of $(,)$. □

**Definition 14.3.2.** *A linear transformation $T : H \to H$ on a Hilbert space $H$ is **hermitian** (resp. **positive semidefinite**) if the associated sesquilinear form $(x, y) = \langle x, Ty \rangle$ is hermitian (resp. positive semidefinite).*

Although it would be straightforward to define "positive" linear transformations to be those where the associated form is positive definite, often the term positive is used synonymously with positive semidefinite. We don't use the term positive to avoid any confusion.

By Theorem 3.1.11 and Lemma 14.3.1, we get immediately that $T$ is hermitian (resp. positive semidefinite) if and only if $[T]_{\mathcal{B},\mathcal{B}}$ is hermitian (resp. positive semidefinite) in some orthonormal basis $\mathcal{B}$ (in which case it will be hermitian or positive semidefinite in all orthonormal bases). We know that a matrix $M$ is hermitian if and only if $M^* = M$, and also $[T]^*_{\mathcal{B},\mathcal{B}} = [T^*]_{\mathcal{B},\mathcal{B}}$, the matrix of the adjoint of $T$, by Lemma 5.2.1. Consequently:

**Lemma 14.3.3.** *$T : H \to H$ is hermitian if and only if $T$ is self-adjoint.*

*Proof.* $T$ is hermitian if and only if $[T]_{\mathcal{B},\mathcal{B}} = [T]^*_{\mathcal{B},\mathcal{B}} = [T^*]_{\mathcal{B},\mathcal{B}}$, which occurs if and only if $T = T^*$. □

As a consequence of Lemma 14.3.3, the terms hermitian and self-adjoint are used interchangeably. Notably, in the definition of hermitian and positive semidefinite operators, and the proof of Lemma 14.3.3, we get a strong connection between the world of linear transformations, and the world of forms.

Since positive semidefinite forms are hermitian, a positive semidefinite operator also has to be hermitian. If we expand the definition a bit more, a linear transformation $T : H \to H$ is positive semidefinite if and only if $T$ is hermitian, and

$$\langle x, Tx \rangle \geq 0$$

for all $x \in H$. Using the spectral theorem, we can say more:

**Theorem 14.3.4.** *Let $T : H \to H$ be a self-adjoint operator on a Hilbert space $H$. Then the following are equivalent:*

*(a) $T$ is positive semidefinite.*

*(b) All the eigenvalues of $T$ are non-negative.*

*(c) There is a linear transformation $A : H \to H$ such that $T = A^*A$.*

*Proof.* Suppose $T$ is positive semidefinite. Since $T$ is self-adjoint, $T$ is diagonalizable, with real eigenvalues. Suppose $\lambda$ is an eigenvalue of $T$. Let $v$ be a unit vector in $E_\lambda(T)$. Then

$$0 \leq \langle v, Tv \rangle = \langle v, \lambda v \rangle = \lambda.$$

So all eigenvalues of $T$ are non-negative, and (a) implies (b).

Suppose $T$ is a linear transformations with all eigenvalues non-negative. Let $T = \sum_{i=1}^k \lambda_i P_i$ be the spectral decomposition of $T$, and let

$$A = \sum_{i=1}^k \sqrt{\lambda_i} P_i.$$

Then $A^* = A$, and

$$A^*A = \sum_{1\leq i,j\leq k} \sqrt{\lambda_i}\sqrt{\lambda_j}P_iP_j = \sum_{i=1}^{k} \lambda_i P_i = T,$$

since $P_iP_j = 0$ if $i \neq j$ and $P_i^2 = P_i$. So (b) implies (c).

Finally, if $T = A^*A$, and $x \in H$, then

$$\langle x, Tx\rangle = \langle x, A^*Ax\rangle = \langle Ax, Ax\rangle = \|Ax\|^2 \geq 0.$$

So $T$ is positive semidefinite, and we conclude that (c) implies (a). □

The set of hermitian and positive semidefinite operators are used so often that it's convenient to have some notation for them:

**Definition 14.3.5.** *Let $H$ be a Hilbert space. The set of hermitian operators on $H$ is denoted by* $\mathrm{Lin}(H,H)_h$*, and the set of positive semidefinite operators on $H$ is denoted by* $\mathrm{Lin}(H,H)_+$*.*

**Exercise 14.3.6.**

*(a) Show that* $\mathrm{Lin}(H,H)_h$ *is an $\mathbb{R}$-linear subspace of* $\mathrm{Lin}(H,H)$ *for every Hilbert space $H$, but not a $\mathbb{C}$-linear subspace when $H$ is non-zero.*

*(b) Show that* $\mathrm{Lin}(H,H)_+$ *is a* ***convex cone*** *of the $\mathbb{R}$-vector space* $\mathrm{Lin}(H,H)_+$*, meaning that if $S, T \in \mathrm{Lin}(H,H)_+$, and $\lambda_1, \lambda_2 \geq 0$, then $\lambda_1 S + \lambda_2 T \in$* $\mathrm{Lin}(H,H)_+$*.*

## 14.4 Density matrices

What if we apply a generalized measurement $\{A_i\}_{i=1}^k$ to an ensemble of states $\{p_j : |\psi_j\rangle\}_{j=1}^m$ on a Hilbert space $H$. If the system happens to be in state $|\psi_j\rangle$ then we get outcome $i$ with probability $\langle\psi_j|A_i^*A_i|\psi_j\rangle$, and the state after measurement will be $A_i|\psi_j\rangle/\|A_i|\psi_j\rangle\|$. Since the system is in state $|\psi_j\rangle$ with probability $p_j$, we get outcome $i$ with probability

$$\sum_{j=1}^{m} p_j \langle\psi_j|A_i^*A_i|\psi_j\rangle,$$

and the state of the system after measuring outcome $i$ can be described as an ensemble of states

$$\left\{q_j : \frac{A_i|\psi_j\rangle}{\|A_i|\psi_j\rangle\|}\right\}_{j=1}^{m}.$$

For the probabilities $q_j$, it is tempting to say that $q_j = p_j$, since this is the probability that the system is in state $|\psi_j\rangle$ before measurement, and if the system is in state $|\psi_j\rangle$ and we measure outcome $i$, then the state after measurement will be $\frac{A_i|\psi_j\rangle}{\|A_i|\psi_j\rangle\|}$. However, this isn't correct because some outcomes $i$ may be more likely with one state in the ensemble than another. As a result, the outcome of the measurement may give us information about the state of the system before measurement, and we have to incorporate this information into $q_j$.

**Example 14.4.1.** *Suppose the system* $\mathbb{C}\{0,1\}$ *is in an ensemble of states* $\{1/2 : |0\rangle, 1/2 : |1\rangle\}$*, and we measure in the computational basis, getting outcome* $|0\rangle$*. Then we know the state of the original system was* $|0\rangle$*, and the ensemble describe the state of the system after measurement is* $\{1 : |0\rangle\}$*, rather than the nonsensical*

$$\left\{1/2 : |0\rangle, 1/2 : \frac{\vec{0}}{0}\right\}.$$

The correct way to think about $q_j$ is as the probability that the system was in state $|\psi_j\rangle$, given that the outcome of the measurement is $i$. From the rules of probability, this is

$$q_j := \frac{\Pr(\text{system starts in state } |\psi_j\rangle \text{ and outcome is } i)}{\Pr(\text{outcome of the measurement is } i)} = \frac{p_j \langle\psi_j|A_i^* A_i|\psi_j\rangle}{\sum_{j=1}^m p_j \langle\psi_j|A_i^* A_i|\psi_j\rangle}.$$

It would be nice to have a more compact expression for the probability of measuring outcome $i$. For this purpose, let $C : H \otimes H^* \to \mathbb{C}$ be the contraction operator from Proposition 9.4.1, and let $S : H \otimes H^* \to H^* \otimes H$ be the swap isomorphism. Then

$$\langle\psi_j|A_i^* A_i|\psi_j\rangle = C \langle\psi_j| \otimes (A_i^* A_i |\psi_j\rangle) = CSA_i^* A_i |\psi_j\rangle \otimes \langle\psi_j|.$$

Recall from Exercise 9.4.3 that $A_i^* A_i |\psi_j\rangle \langle\psi_j| = (A_i^* A_i \otimes \mathbb{1})(|\psi_j\rangle\langle\psi_j|)$ is the product of $A_i^* A_i$ with $|\psi_j\rangle\langle\psi_j|$ as operators $H \to H$. By Proposition 9.4.7, we conclude that

$$\langle\psi_j|A_i^* A_i|\psi_j\rangle = \operatorname{tr}(A_i^* A_i |\psi_j\rangle\langle\psi_j|),$$

and hence the probability of measuring outcome $i$ is

$$\sum_{j=1}^m p_j \operatorname{tr}(A_i^* A_i |\psi_j\rangle\langle\psi_j|) = \operatorname{tr}\left(A_i^* A_i \sum_{j=1}^k p_j |\psi_j\rangle\langle\psi_j|\right).$$

If we set

$$\rho = \sum_{j=1}^{k} p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|,$$

then we can write this probability compactly as $\operatorname{tr}(A_i^* A_i \rho)$.

**Definition 14.4.2.** *The* ***density matrix*** *(or* ***density operator****) of an ensemble of states $\{p_j : |\psi_j\rangle\}_{j=1}^m$ on a Hilbert space $H$ is the linear transformation $\rho : H \to H$ with*

$$\rho = \sum_{j=1}^{m} p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|.$$

**Lemma 14.4.3.** *Let $|\psi_j\rangle$, $1 \leq j \leq m$ be a collection of states in a Hilbert space $H$, and let $\lambda_j$, $1 \leq j \leq m$ be a collection of non-negative scalars. Define $\rho : H \to H$ by*

$$\rho = \sum_{j=1}^{m} \lambda_j \left|\psi_j\right\rangle \left\langle\psi_j\right|.$$

*Then $\rho$ is positive semidefinite and* $\operatorname{tr}\rho = \sum_{j=1}^m \lambda_j$.

*Proof.* If $|\phi\rangle \in H$, then

$$\langle\phi|\rho|\phi\rangle = \sum_{j=1}^{m} \lambda_j \left\langle\phi|\psi_j\right\rangle \left\langle\psi_j|\phi\right\rangle = \sum_{j=1}^{m} \lambda_j |\left\langle\phi|\psi_j\right\rangle|^2 \geq 0,$$

since $\lambda_j \geq 0$ for all $1 \leq j \leq m$.

Using the contraction formula for the trace, we get that

$$\operatorname{tr}\rho = \sum_{j=1}^{m} \lambda_j \left\langle\psi_j|\psi_j\right\rangle = \sum_{j=1}^{m} \lambda_j.$$

□

Lemma 14.4.3 makes it easy to determine whether a linear transformation is a density matrix:

**Proposition 14.4.4.** *Let $H$ be a Hilbert space, and $\rho : H \to H$ a linear transformation. Then $\rho$ is the density matrix of an ensemble of states if and only if $\rho$ is positive semidefinite and* $\operatorname{tr}\rho = 1$.

*Proof.* Lemma 14.4.3 shows that if $\rho = \sum_{j=1}^{k} p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|$ is the density matrix of an ensemble of states $\{p_j : \left|\psi_j\right\rangle\}$ then $\rho$ is positive semidefinite, and $\operatorname{tr}\rho = \sum_{j=1}^{k} p_j = 1$.

Conversely, suppose that $\rho$ is positive semidefinite with $\operatorname{tr}\rho = 1$. By Theorem 14.3.4, $\rho$ is diagonalizable with non-negative eigenvalues. Let

$$\rho = \sum_{j=1}^{k} \lambda_j P_j$$

be the spectral decomposition of $\rho$. Choose an orthonormal basis $\mathcal{B}_j$ for each $\operatorname{Im} P_j$, $1 \leq j \leq k$, and let $\mathcal{B} = \bigcup_j \mathcal{B}_j$. Then

$$\rho = \sum_{j=1}^{k} \sum_{\left|x\right\rangle \in \mathcal{B}_j} \lambda_j \left|x\right\rangle \left\langle x\right| = \sum_{\left|x\right\rangle \in \mathcal{B}} \lambda_{\left|x\right\rangle} \left|x\right\rangle,$$

where $\lambda_{\left|x\right\rangle} = \lambda_j$ if $\left|x\right\rangle \in \mathcal{B}_j$. By Lemma 14.4.3,

$$\sum_{\left|x\right\rangle \in \mathcal{B}} \lambda_{\left|x\right\rangle} = \operatorname{tr}\rho = 1,$$

so $\{\lambda_{\left|x\right\rangle} : \left|x\right\rangle\}$ is an ensemble of states, and $\rho$ is the density matrix of this ensemble. □

Because of Proposition 14.4.4, we say that $\rho : H \to H$ is a **density matrix** if $\rho$ is positive semidefinite and $\operatorname{tr}\rho = 1$. Although Proposition 14.4.4 states that every density matrix is the density matrix of some ensemble, the proof shows something stronger: every density matrix is the density matrix of an ensemble of states, where the states form an orthonormal basis for $H$. Of course, the states in an ensemble are not required to form an orthonormal basis of $H$; they don't even have to be orthogonal. So different ensembles can have the same density matrix.

**Exercise 14.4.5.** *Give an explicit example of two different ensembles on a Hilbert space $H$ with the same density matrix.*

Suppose that two ensembles have the same density matrix $\rho$. Any sequence of measurements and unitary operations that we can apply to these two ensembles can be turned into a generalized measurement $\{A_i\}_{i \in \mathcal{O}}$. Since the probability of getting outcome $i$ is

$$\operatorname{tr}(A_i^* A_i \rho)$$

for both ensembles, we can't tell these ensembles apart with a generalized measurement.

What about the state of the system after measurement? If we start with ensemble $E_1 = \{p_j : |\psi_j\rangle\}_{j=1}^m$ on a Hilbert space $H$, and get outcome $i$ from measuring with generalized measurement $\{A_i\}_{i=1}^k$, then the state after measurement can be described by the ensemble

$$E_2 = \left\{ \frac{p_j \| A_i |\psi_j\rangle \|^2}{\operatorname{tr}(A_i^* A_i \rho)} : \frac{A_i |\psi_j\rangle}{\| A_i |\psi_j\rangle \|} \right\}_{j=1}^m .$$

Consider $|\phi\rangle = A_i |\psi_j\rangle$ for some $i$. As a linear operator, $|\phi\rangle\langle\phi|$ sends $|\gamma\rangle$ to

$$\langle\phi|\gamma\rangle |\phi\rangle = A_i |\psi_j\rangle \langle\psi_j| A_i^* |\gamma\rangle ,$$

so

$$|\phi\rangle\langle\phi| = A_i |\psi_j\rangle \langle\psi_j| A_i^*.$$

As a result, the density matrix of $E_2$ is

$$\begin{aligned}\sum_{j=1}^m \frac{p_j \| A_i |\psi_j\rangle \|^2}{\operatorname{tr}(A_i^* A_i \rho)} \cdot \frac{1}{\| A_i |\psi_j\rangle \|^2} A_i |\psi_j\rangle \langle\psi_j| A_i^* &= \frac{1}{\operatorname{tr}(A_i^* A_i \rho)} A_i \left( \sum_{j=1}^m p_j |\psi_j\rangle \langle\psi_j| \right) A_i^* \\ &= \frac{A_i \rho A_i^*}{\operatorname{tr}(A_i^* A_i \rho)},\end{aligned}$$

where

$$\rho = \sum_{j=1}^m p_j |\psi_j\rangle \langle\psi_j|$$

is the density matrix of $E_1$.

This means that to calculate the density matrix of $E_2$, we only need the density matrix of $E_1$. In particular, if $E_1'$ is another ensemble with density matrix $\rho$, and $E_2'$ is the ensemble after measuring with $\{A_i\}_{i=1}^m$ getting outcome $i$, then $E_2'$ has the same density matrix $\frac{A_i \rho A_i^*}{\operatorname{tr}(A_i^* A_i \rho)}$ as $E_2$. Note that this is what we'd expect from our finding that it's not possible to tell $E_1$ and $E_1'$ apart with a generalized measurement. Indeed, if it was possible for $E_2'$ to have a different density matrix from $E_2$, then we might be able to tell these two density matrices apart with a generalized measurement. Since the combination of two generalized measurements is a generalized measurement, this would mean that we could tell $E_1$ and $E_1'$ apart with a generalized measurement, contradicting our finding above.

Since we can't tell ensembles with the same density matrix apart, we should think of two such ensembles as being physically equivalent. So describing a physical system with an ensemble is redundant: the density matrix provides a better description. Thus we extend the notion of state given in Axiom 2 with the following definition:

**Definition 14.4.6.** *A **mixed state** on a Hilbert space $H$ is a density matrix $\rho$ on $H$. A mixed state of the form $|\psi\rangle\langle\psi|$ for some $|\psi\rangle \in H$ is called a **pure state**.*

The state of the system can be described by a mixed state whenever it can be described by an ensemble of states, and so sometimes the term mixed state is often used to refer to density matrices and ensembles of states interchangeably, with the idea being that density matrices and ensembles are just two different ways to represent the underlying mixed state of the system.

Using the rules given in this section, we can work completely in terms of mixed states. We summarize these rules in the following proposition for later reference:

**Proposition 14.4.7.** *Suppose a Hilbert space is in mixed state $\rho$. Then*

- *the probability of measuring outcome $i$ from generalized measurement $\{A_i\}_{i=1}^k$ is $\operatorname{tr}(A_i^* A_i \rho)$, and*
- *the state after measurement will be the mixed state $A_i \rho A_i^* / \operatorname{tr}(A_i^* A_i \rho)$.*

**Exercise 14.4.8.** *Let $A$ be an observable on a Hilbert space $H$, and let $\rho$ be a density matrix on $H$. Show that the expected value of $A$ when the system is in state $\rho$ is $\operatorname{tr}(A\rho)$.*

To distinguish the original notion of states in Axiom 2 from mixed states, we sometimes refer to unit vectors as **vector states**. As mentioned in Section 14.1, if the state of a system can be described by a vector state $|\psi\rangle$, then it can also be described by the ensemble $\{1 : |\psi\rangle\}$, and hence by the density matrix $\rho = |\psi\rangle\langle\psi|$. Pure states are precisely the density matrices of this form. However, note that the mapping $|\psi\rangle \mapsto |\psi\rangle\langle\psi|$ from vector states to pure states is not injective: it's possible to have $|\psi\rangle\langle\psi| = |\psi'\rangle\langle\psi'|$ for two different unit vectors $|\psi\rangle$ and $|\psi'\rangle$. While this might initially seem like a problem, it's actually a feature:

**Exercise 14.4.9.** *Let $H$ be a Hilbert space.*

*(a) Show that $|\psi\rangle\langle\psi| = |\psi'\rangle\langle\psi'|$ for $|\psi\rangle, |\psi'\rangle \in H$ if and only if $|\psi\rangle$ and $|\psi'\rangle$ differ by a global phase.*

(b) *Show that a density matrix $\rho$ is equal to $|\psi\rangle\langle\psi|$ for some $|\psi\rangle \in H$ if and only if $\rho$ has rank* 1.

In other words, while the mapping $|\psi\rangle \mapsto |\psi\rangle\langle\psi|$ is not a bijection between vector states and pure states, we do get a bijection $[|\psi\rangle] \mapsto |\psi\rangle\langle\psi|$ between equivalence classes of vector states up to global phase and pure states. Thus we can use density matrices when we want to work with vector states up to global phase.

## 14.5 POVMs

Let $\{A_i\}$ be a generalized measurement, and let $M_i := A_i^* A_i$. If the system is in mixed state $\rho$, then the probability of getting outcome $i$ is $\mathrm{tr}(M_i\rho)$. If we only care about these probabilities, and not the state of the system after measurement, then the matrices $M_i$ capture everything we need to know about the measurement. There are lots of situations where we discard, lose access to, or are just done with a system, and don't care about the system after measurement. Theses types of measurements are sometimes called **destructive measurements**, to distinguish them from measurements where the state after measurement is significant. This motives the following definition:

**Definition 14.5.1.** *A **positive operator-valued measure (POVM)** with outcome set $\mathcal{O}$ on a Hilbert space $H$ is a family $\{M_i\}_{i\in\mathcal{O}}$ of positive semidefinite operators on $H$ such that*

$$\sum_{i\in\mathcal{O}} M_i = \mathbb{1}.$$

*If the system is in state $\rho$, then the **probability of measuring outcome $i \in \mathcal{O}$ with POVM** $\{M_i\}_{i\in\mathcal{O}}$ is*

$$\mathrm{tr}(M_i\rho).$$

*The state of the system after measurement is unspecified (and often the system is regarded as inaccessible).*

The term "positive-operator valued measure" comes from measure theory, where a measure on a finite set $\mathcal{O}$ correspond to probability distributions $\{p_i\}_{i\in\mathcal{O}}$ on $\mathcal{O}$. A POVM is like a probability distribution, but rather than assigning a non-negative real number to each element of $\mathcal{O}$, we assign a positive semidefinite operator. POVMs are also sometimes called **POVM measurements**, although this sounds a bit strange when you expand the acronym.

It's clear that we can get a POVM $\{M_i\}_{i\in\mathcal{O}}$ from any generalized measurement $\{A_i\}_{i\in\mathcal{O}}$ by setting $M_i := A_i^*A_i$. Conversely, if $M_i$ is a positive semidefinite operator, then $M_i = A_i^*A_i$ for some operator $A_i$ by Theorem 14.3.4. So every POVM is the POVM of a generalized measurement. However, this generalized measurement is not unique (which is part of why the state after measurement isn't specified by a POVM).

**Exercise 14.5.2.** *(a) Find two operators $A$ and $B$ on a Hilbert space $H$ such that $A^*A = B^*B$, but $A \neq \lambda B$ for any $\lambda \in \mathbb{C}$.*

*(b) Use part (a) to find an example of two generalized measurements $\{A_i\}_{i\in\mathcal{O}}$ and $\{B_i\}_{i\in\mathcal{O}}$ on a Hilbert space $H$, along with a vector state $|\psi\rangle \in H$, such that $A_i^*A_i = B_i^*B_i$ for all $i \in \mathcal{O}$, but $A_i |\psi\rangle \langle\psi| A_i^* \neq B_i |\psi\rangle \langle\psi| B_i^*$ for some $i \in \mathcal{O}$.*

One of the nice features of POVMs is that they work well with coarse-graining. Let $\mathcal{O}$ be a set of outcomes, and let $\{\mathcal{O}_i : i \in I\}$ be a partition of $\mathcal{O}$. Suppose $\{M_j\}_{j\in\mathcal{O}}$ is a POVM on $H$. If the system is in mixed state $\rho$, then the probability of getting outcome an outcome $j \in \mathcal{O}_i$ is

$$\sum_{j\in\mathcal{O}_i} \operatorname{tr}(M_j\rho) = \operatorname{tr}\left(\left(\sum_{j\in\mathcal{O}_i} M_j\right)\rho\right).$$

Let $N_i := \sum_{j\in\mathcal{O}_i} M_j$. Then $N_i$ is positive semidefinite by Exercise 14.3.6, and

$$\sum_{i\in I} N_i = \sum_{i\in I}\sum_{j\in\mathcal{O}_j} M_j = \sum_{j\in\mathcal{O}} M_j = \mathbb{1},$$

so $\{N_i\}_{i\in I}$ is a POVM. We call this the **coarse-graining of $\{M_j\}_{j\in\mathcal{O}}$ by the partition** $\{\mathcal{O}_i : i \in I\}$, since the probability of getting outcome $i \in \mathcal{I}$ with this POVM is the same as the probability of getting outcome $j \in \mathcal{O}_i$ from $\{M_j\}_{j\in\mathcal{O}}$.

# Chapter 15

# The no-communication theorem

Although we're studying the abstract mathematical properties of quantum probability, the point of quantum probability is to model physical scenarios. And as shown by nonlocal games like CHSH game, there are advantages to using quantum probability as a modelling language over classical probability.

In the CHSH game, we considered a physical system consisting of two subsystems $H_A$ and $H_B$ in distant locations. This system can be in an entangled state like $|\psi\rangle = |00\rangle + |11\rangle$ (for $H_A = H_B = \mathbb{C}\{0, 1\}$). If we're modelling the joint system (for instance, modelling strategies for the CHSH game) then it makes sense that our model would use states like $|00\rangle + |11\rangle$ that refer to both subsystems. However, what if the subsystems do not know about each other: say system $H_B$ does not know about system $H_A$. As an outside observer, we may be able to see that the state of $H_A \otimes H_B$ is best captured by an entangled state. But what about people at location $B$? Do they need to know about location $A$ to model the physics at their location? Presumably not; otherwise, we would have to consider the possibility of entanglement with an external system for any modelling task with quantum mechanics. Since quantum mechanics is widely used without this concern, [1] we should expect that anyone located at system $B$ will be able to model the physics they see at that location strictly in terms of $H_B$. As an outside observer, this raises the question: if we know that the state of the system $H_A \otimes H_B$ is $|\psi\rangle$, then what state on $H_B$ describes the outcome of measurements at $H_B$?

For the answer to this question, we need to go to mixed states (so we might as well assume that we start with a mixed state in $H_A \otimes H_B$). The answer is then given by the partial trace.

[1] Although in fact, frequently we do want to consider interaction with an unknown external system. For instance, this is a common situation in quantum cryptography.

## 15.1 Partial trace

The key to going from a system $H_A \otimes H_B$ to $H_B$ is:

**Definition 15.1.1.** *Suppose $V_A$ and $V_B$ are $\mathbb{F}$-vector spaces. Let*

$$\psi : \mathrm{Lin}(V_A \otimes V_B, V_A \otimes V_B) \to \mathrm{Lin}(V_A, V_A) \otimes \mathrm{Lin}(V_B, V_B)$$

*be the natural isomorphism from Section 9.5, and let $\phi : \mathbb{F} \otimes V_B \to V_B$ be the natural map from Proposition 9.1.1. Then the* ***partial trace with respect to*** *$V_A$ (or* ***over*** *$V_A$) is the map*

$$\phi \circ (\mathrm{tr}_{H_A} \otimes \mathbb{1}) \circ \psi : \mathrm{Lin}(V_A \otimes V_B, V_A \otimes V_B) \to \mathrm{Lin}(V_B, V_B).$$

*The partial trace is sometimes denoted by $\mathrm{tr}_A$ or $\mathrm{tr}_{V_A}$.*

Although the definition of the partial trace is abstract, we can easily calculate the partial trace for specific examples using the contraction formula for the trace.

**Example 15.1.2.** *Let $H_A = \mathbb{C}\{1, \ldots, m\}$ and $H_B = \mathbb{C}\{1, \ldots, n\}$. Since $H_A \otimes H_B$ is spanned by $|i\rangle\,|j\rangle$ for $1 \le i \le m$, $1 \le j \le n$, we can write any element of $\mathrm{Lin}(H_A \otimes H_B, H_A \otimes H_B$ as*

$$\sum_{1\le i,k\le m}\ \sum_{1\le j,\ell\le n} a_{ij,kl}\,|i\rangle\,|j\rangle\,\langle k|\,\langle \ell|\,.$$

*When we think of linear transformations as tensors, the isomorphism $\mathrm{Lin}(H_A\otimes H_B, H_A \otimes H_B) \cong \mathrm{Lin}(H_A, H_A) \otimes \mathrm{Lin}(H_B, H_B)$ sends*

$$|i\rangle\,|j\rangle\,\langle k|\,\langle \ell| \in H_A \otimes H_B \otimes H_A^* \otimes H_B^*$$

*to*

$$|i\rangle\,\langle k|\,|j\rangle\,\langle \ell| \in H_A \otimes H_A^* \otimes H_B \otimes H_B^*.$$

*Since $\mathrm{tr}(|i\rangle\,\langle k|) = \langle k|i\rangle = \delta_{ki}$ by the contraction formula, we get that*

$$\mathrm{tr}_A\left(\sum_{1\le i,k\le m}\ \sum_{1\le j,\ell\le n} a_{ij,k\ell}\,|i\rangle\,|j\rangle\,\langle k|\,\langle \ell|\right) = \sum_{1\le k\le m} a_{ij,i\ell}\,|j\rangle\,\langle \ell|\,.$$

*More generally,*

$$\mathrm{tr}_A\left(\sum_{i=1}^{N} |\alpha_i\rangle\,|\beta_i\rangle\,\langle\gamma_i|\,\langle\delta_i|\right) = \sum_{i=1}^{n} \langle\gamma_i|\alpha_i\rangle\,|\beta_i\rangle\,\langle\delta_i|$$

*for any collection of vectors $|\alpha_i\rangle\,, |\gamma_i\rangle \in H_A$ and $|\beta_i\rangle\,, |\delta_i\rangle \in H_B$.*

**Theorem 15.1.3.** *Let $V_A$, $V_B$ be Hilbert spaces, and suppose*

$$\widetilde{\operatorname{tr}} : \operatorname{Lin}(V_A \otimes V_B, V_A \otimes V_B) \to \operatorname{Lin}(V_B, V_B)$$

*is linear. Then the following are equivalent:*

*(a)* $\widetilde{\operatorname{tr}}$ *is equal to the partial trace* $\operatorname{tr}_A$ *over* $V_A$*.*

*(b)* $\widetilde{\operatorname{tr}}((\mathbb{1} \otimes M)\rho) = M\widetilde{\operatorname{tr}}(\rho)$ *for all* $M \in \operatorname{Lin}(V_B, V_B)$ *and* $\rho \in \operatorname{Lin}(V_A \otimes V_B, V_A \otimes V_B)$*.*

*(c)* $\widetilde{\operatorname{tr}}(\rho(\mathbb{1} \otimes M)) = \widetilde{\operatorname{tr}}(\rho)M$ *for all* $M \in \operatorname{Lin}(V_B, V_B)$ *and* $\rho \in \operatorname{Lin}(V_A \otimes V_B, V_A \otimes V_B)$*.*

*(d)* $\operatorname{tr}(\mathbb{1} \otimes M\rho) = \operatorname{tr}(M\widetilde{\operatorname{tr}}(\rho))$ *for every* $M \in \operatorname{Lin}(V_B, V_B)$ *and* $\rho \in \operatorname{Lin}(V_A \otimes V_B, V_A \otimes V_B)$*.*

*Proof.* Because vectors of the form $u \otimes v$ span $V_A \otimes V_B$, vectors of the form

$$u \otimes v \otimes f \otimes g \in (V_A \otimes V_B) \otimes (V_A \otimes V_B)^* \cong \operatorname{Lin}(V_A \otimes V_B, V_A \otimes V_B)$$

for $u \in V_A$, $f \in V_A^*$, $v \in V_B$, $g \in V_B^*$ span $\operatorname{Lin}(V_A \otimes V_B, V_A \otimes V_B)$. When thinking about linear transformations as tensors, the isomorphism $\operatorname{Lin}(V_A \otimes V_B, V_A \otimes V_B) \to \operatorname{Lin}(V_A, V_A) \otimes \operatorname{Lin}(V_B, V_B)$ sends

$$u \otimes v \otimes f \otimes g \mapsto u \otimes f \otimes v \otimes g \in V_A \otimes V_A^* \otimes V_B \otimes V_B^*.$$

Using the contraction formula for tr, we get that

$$\operatorname{tr}_A(u \otimes v \otimes f \otimes g) = f(u)v \otimes g \in V_B \otimes V_B^*.$$

If $M \in \operatorname{Lin}(V_B, V_B)$, then

$$\operatorname{tr}_A((\mathbb{1} \otimes M)(u \otimes v \otimes f \otimes g)) = \operatorname{tr}_A(u \otimes Mv \otimes f \otimes g) = f(u)Mv \otimes g = M \operatorname{tr}_A(u \otimes v \otimes f \otimes g).$$

We conclude that $\operatorname{tr}_A((\mathbb{1} \otimes M)\rho) = M \operatorname{tr}_A(\rho)$ holds for $\rho$ in a spanning set when $M$ is fixed. Since both sides are linear functions of $\rho$, (a) implies (b).

That (a) implies (c) is similar. Taking traces of both sides, we see that either of (b) or (c) implies (d) as well. So to finish the proof, we just need to show that (d) implies (a). Choose a basis $\{v_1, \ldots, v_n\}$ for $V_B$, and let $\{v^1, \ldots, v^n\}$ be the dual basis. Observe that, considered as elements of $\operatorname{Lin}(V_B, V_B)$,

$$\operatorname{tr}((v_i \otimes v^j)(v_k \otimes v^\ell)) = v^j(v_k) \operatorname{tr}(v_i \otimes v^\ell) = v^\ell(v_i)v^j(v_k) = \delta_{(i,j),(k,\ell)}.$$

Set $\rho = u \otimes v_p \otimes f \otimes v^q$ for some $u \in V_A$, $f \in V_A^*$, and $1 \leq p, q \leq n$. Let

$$\widetilde{\operatorname{tr}}(\rho) = \sum_{1 \leq k, \ell \leq n} a_{k\ell} v_k \otimes v^\ell.$$

Then

$$\begin{aligned} a_{ij} &= \operatorname{tr}((v_j \otimes v^i)\widetilde{\operatorname{tr}}(\rho)) \\ &= \operatorname{tr}((\mathbb{1} \otimes (v_j \otimes v^i))\rho) \\ &= v^i(v_p) \operatorname{tr}(u \otimes v_j \otimes f \otimes v^q) \\ &= v^i(v_p)(f \otimes v^q)(u \otimes v_j) \\ &= f(u)v^i(v_p)v^q(v_j) = f(u)\delta_{(i,j),(p,q)}. \end{aligned}$$

In other words,

$$\widetilde{\operatorname{tr}}(\rho) = f(u)v_p \otimes v^q = \operatorname{tr}_A(\rho).$$

Extending linearly, we see that $\widetilde{\operatorname{tr}} = \operatorname{tr}_A$. □

Although conditions (b) and (c) in Theorem 15.1.3 are equivalent, it's not true that $\operatorname{tr}_A((\mathbb{1} \otimes M)\rho) = \operatorname{tr}_A(\rho(\mathbb{1} \otimes M))$:

**Exercise 15.1.4.** *Find Hilbert spaces $H_A$ and $H_B$, $M \in \operatorname{Lin}(H_B, H_B)$, and $\rho \in \operatorname{Lin}(H_A \otimes H_B, H_A \otimes H_B)$ such that*

$$\operatorname{tr}_A((\mathbb{1} \otimes M)\rho) \neq \operatorname{tr}_A(\rho(\mathbb{1} \otimes M)).$$

We can immediately apply Theorem 15.1.3 to quantum states. Although we haven't stated this as an axiom or theorem, it should be clear that if $\{A_i\}_{i \in \mathcal{O}}$ is a generalized measurement on $H_B$, then $\{\mathbb{1} \otimes A_i\}_{i \in \mathcal{O}}$ is the generalized measurement on $H_A \otimes H_B$ for measuring $H_B$, and leaving $H_A$ unchanged. Note that $(\mathbb{1} \otimes A_i)^*(\mathbb{1} \otimes A_i) = \mathbb{1} \otimes A_i^* A_i$.

**Corollary 15.1.5.** *Let $H_A$ and $H_B$ be Hilbert spaces, and let $\rho$ be a mixed state on $H_A \otimes H_B$. Then $\operatorname{tr}_A(\rho)$ is a state on $H_B$, such that if $\{A_i\}_{i \in \mathcal{O}}$ is a generalized measurement on $H_B$, then*

$$\operatorname{tr}((\mathbb{1} \otimes A_i^* A_i)\rho) = \operatorname{tr}(A_i^* A_i \operatorname{tr}_A(\rho))$$

*for all $i \in \mathcal{O}$. Furthermore, if $\operatorname{tr}((\mathbb{1} \otimes A_i^* A_i)\rho) \neq 0$, then*

$$\operatorname{tr}_A \left( \frac{(\mathbb{1} \otimes A_i)\rho(\mathbb{1} \otimes A_i^*)}{\operatorname{tr}((\mathbb{1} \otimes A_i^* A_i)\rho)} \right) = \frac{A_i \rho A_i^*}{\operatorname{tr}(A_i^* A_i \rho)}.$$

*Proof.* To show that $\operatorname{tr}_A(\rho)$ is a state on $H_B$, suppose $|\psi\rangle \in H_B$. Let $\{|\phi_i\rangle\}_{i=1}^m$ be an orthonormal basis for $H_A$, so that $\mathbb{1} = \sum_{i=1}^m |\phi_i\rangle \langle\phi_i|$. Then

$$\begin{aligned}\langle\psi| \operatorname{tr}_A(\rho)|\psi\rangle &= \operatorname{tr}(|\psi\rangle \langle\psi| \operatorname{tr}_A(\rho)) \\ &= \operatorname{tr}((\mathbb{1} \otimes |\psi\rangle \langle\psi|)\rho) \\ &= \sum_{i=1}^{m} \operatorname{tr}(|\phi_i\rangle \langle\phi_i| \, |\psi\rangle \langle\psi| \, \rho) \qquad = \langle\phi_i| \, \langle\psi| \, \rho \, |\phi_i\rangle \, |\psi\rangle \geq 0.\end{aligned}$$

So $\operatorname{tr}_A(\rho)$ is positive semidefinite. Also

$$\operatorname{tr}(\operatorname{tr}_A(\rho)) = \operatorname{tr}(\rho) = 1.$$

The rest of the corollary follows from conditions (b)-(d) of Theorem 15.1.3. □

In other words, if $\rho$ is a mixed state on $H_A \otimes H_B$, then measuring $\rho$ with $\{\mathbb{1} \otimes A_i\}$ gives the same measurement outcomes as measuring $\operatorname{tr}_A(\rho)$ with $\{A_i\}$. Furthermore, if $\rho_i$ is the state after measuring $\rho$ and getting outcome $i$, then $\operatorname{tr}_A(\rho_i)$ is the state after measuring $\operatorname{tr}_A(\rho)$ and getting outcome $i$. This means that we can think of the partial trace $\operatorname{tr}_A(\rho)$ as *the* state associated to $\rho$ on $H_B$.

**Exercise 15.1.6.** *Show that if $H_A$ and $H_B$ are (finite-dimensional) Hilbert spaces, then $\operatorname{tr}_A$ is the unique linear operator $\operatorname{Lin}(H_A \otimes H_B, H_A \otimes H_B) \to \operatorname{Lin}(H_B, H_B)$ such that $\operatorname{tr}_A((\mathbb{1} \otimes A_i^* A_i)\rho) = \operatorname{tr}(A_i^* A_i \operatorname{tr}_A(\rho))$.*

We can also define the partial trace of a vector state.

**Definition 15.1.7.** *Let $|\psi\rangle$ be a (vector state) on a tensor product $H_A \otimes H_B$ of Hilbert spaces. The* ***partial trace of*** $|\psi\rangle$ ***over*** $H_A$ *is $\operatorname{tr}_A(|\psi\rangle \langle\psi|)$.*

As the following example shows, the partial trace of a vector state is not necessarily a pure state.

**Example 15.1.8.** *Let $|\psi\rangle = |00\rangle + |11\rangle \in \mathbb{C}\{0,1\} \otimes \mathbb{C}\{0,1\}$, regarded as a state. Then the partial trace of $|\psi\rangle$ over $A$ is*

$$\begin{aligned}&\operatorname{tr}_A(\frac{1}{2}(|00\rangle \langle00| + |00\rangle \langle11| + |11\rangle \langle00| + |11\rangle \langle11|)) \\ &\qquad = \frac{1}{2}(\langle0|0\rangle \, |0\rangle \langle0| + \langle0|1\rangle \, |0\rangle \langle1| + \langle1|0\rangle \, |1\rangle \langle0| + \langle1|1\rangle \, |1\rangle \langle1|) \\ &\qquad = \frac{1}{2}(|0\rangle \langle0| + |1\rangle \langle1|) = \frac{1}{2}\mathbb{1}\end{aligned}$$

*(the normalizalization $\frac{1}{2}$ comes from the normalization of $|\psi\rangle$).*

It's not a coincidence that we used an entangled state for this example:

**Exercise 15.1.9.** *Let $|\psi\rangle \in \mathbb{C}\{1,\dots,m\} \otimes \mathbb{C}\{1,\dots,n\}$. Show that $|\psi\rangle$ is entangled if and only if the partial trace of $|\psi\rangle$ over $\mathbb{C}\{1,\dots,m\}$ is not a pure state.*

## 15.2 The no communication theorem

The partial trace allows us to resolve a very confusing aspect of quantum probability. Returning to the beginning of the chapter, suppose we have a system consisting of two distant subsystems $H_A = \mathbb{C}\{0,1\}$ and $H_B = \mathbb{C}\{0,1\}$, and the system is in state $|\psi\rangle = |00\rangle + |11\rangle$. If we measure the first register in the computational basis and get outcome $|i\rangle$, then the state of $H_A \otimes H_B$ collapses to $|i\rangle\,|i\rangle$. If the measurement is completed faster than it would take a signal to travel from location $A$ to location $B$ at the speed of light, then it seems like we've violated a tenet of relativity: information shouldn't travel faster than the speed of light.

However, does anything change at location $B$ when we perform a measurement at location $A$? To answer this question, we don't care that the state of the system $H_A \otimes H_B$ changes. What we want to know is what happens at $H_B$, and the state at $H_B$ is given by the partial trace. Before we do the measurement, $H_B$ is in state

$$\mathrm{tr}_A(|\psi\rangle\,\langle\psi|) = \frac{1}{2}\mathbb{1}.$$

After we do the measurement, the state of the global system will be $|i\rangle\,|i\rangle$, so $H_B$ will be in the pure state

$$\mathrm{tr}_A(|i\rangle\,|i\rangle\,\langle i|\,\langle i|) = \langle i|i\rangle\,|i\rangle\,\langle i| = |i\rangle\,\langle i|\,,$$

which is physically equivalent to being in state $|i\rangle$. However, this is only the state of the system if we know the outcome of the measurement. Crucially, this information shouldn't be known at location $B$. If the outcome of the measurement is inaccessible, then $H_B$ will be in states $|0\rangle$ and $|1\rangle$ with probability 1/2 each. In other words, the system is in an ensemble of states $\{1/2 : |0\rangle\,, 1/2 : |1\rangle\}$. The density matrix of this ensemble is

$$\frac{1}{2}\left(|0\rangle\,\langle 0| + |1\rangle\,\langle 1|\right) = \frac{1}{2}\mathbb{1},$$

the same as before the measurement. So measuring at $A$ doesn't change the state of $B$, exactly as we would expect.

Let's prove this holds in general. First, we need need a lemma about mixing density matrices together.

**Lemma 15.2.1** (Mixing density matrices)**.** *Let $\rho_i$, $1, \dots, n$ be a collection of density matrices on a Hilbert space $H$. If the system is in state $\rho_i$ with probability $p_i$, then the density matrix for the state of the system is*

$$\sum_{i=1}^{n} p_i \rho_i.$$

*Proof.* Let $N = \dim H$. For each $1 \leq i \leq n$, write

$$\rho_i = \sum_{j=1}^{N} \lambda_{ij} \left|\psi_j\right\rangle \left\langle\psi_j\right|,$$

where

$$\{\left|\psi_j\right\rangle : 1 \leq j \neq N\}$$

is a basis of eigenvectors of $\rho_i$. Being in state $\rho_i$ is equivalent to being in ensemble

$$\{\lambda_{ij} : \left|\psi_j\right\rangle\}_{j=1}^{N}.$$

So if the system is in state $\rho_i$ with probability $p_i$, then the whole system is in ensemble

$$\{p_i\lambda_{ij} : \left|\psi_j\right\rangle\}_{1 \leq i \leq n, 1 \leq j \leq N}.$$

The density matrix of this ensemble is

$$\sum_{i=1}^{n} \sum_{j=1}^{N} p_i \lambda_{ij} \left|\psi_j\right\rangle \left\langle\psi_j\right| = \sum_{i=1}^{n} p_i \rho_i.$$

□

Note that this is a bit of new style of argument for us, because we haven't formally defined what it means to be in an ensemble of density matrices. Instead, we use the intuition we've built up to conclude that being in an ensemble of density matrices is the same as being in an "ensemble of ensembles." If we wanted, we could make this intuitive argument more rigorous by following a similar path to what we've done in previous chapters:

**Exercise 15.2.2.** *Define a notion of "ensembles of mixed states", and derive the rules for performing a generalized measurement on an ensemble of mixed states. Show that measuring the ensemble $\{p_i : \rho_i\}$ with generalized measurement $\{A_j\}_{j \in \mathcal{O}}$ gives the same distribution on outcomes as measuring the density matrix $\sum_i p_i \rho_i$.*

Of course, as long as we understand how to turn the intuitive approach of Lemma 15.2.1 into the formal approach of Exercise 15.2.2, then the intuitive approach of Lemma 15.2.1 isn't less rigorous at all. So as you continue in quantum probability, you'll see arguments like Lemma 15.2.1 more frequently. In fact, we'll give another one right now:

**Corollary 15.2.3.** *If we measure a density matrix $\rho$ on Hilbert space $H$ with generalized measurement $\{A_i\}_{i\in\mathcal{O}}$, but don't reveal the outcome of the measurement, then the system after measurement will be in state*

$$\sum_{i\in\mathcal{O}} A_i\rho A_i^*.$$

*Proof.* After doing the measurement, we'll be in state $A_i\rho A_i^* / \operatorname{tr}(A_i^* A_i \rho)$ with probability $\operatorname{tr}(A_i^* A_i\rho)$. However, we need to make sure we don't divide by zero, so let $\mathcal{O}' = \{i \in \mathcal{O} : \operatorname{tr}(A_i^* A_i\rho) \neq 0\}$. Then we can say that, after measurement, the system is in ensemble

$$\{\operatorname{tr}(A_i^* A_i\rho) : A_i\rho A_i^* / \operatorname{tr}(A_i^* A_i\rho)\}_{i\in\mathcal{O}'},$$

and hence has density matrix

$$\sum_{i\in\mathcal{O}'} \operatorname{tr}(A_i^* A_i\rho)\frac{A_i\rho A_i^*}{\operatorname{tr}(A_i^* A_i\rho)} = \sum_{i\in\mathcal{O}'} A_i\rho A_i^*.$$

If $i \notin \mathcal{O}'$, note that $A_i\rho A_i^*$ is positive, so the eigenvalues of $A_i\rho A_i^*$ are nonnegative. Let $\lambda_1, \ldots, \lambda_n$ be a list of the eigenvectors of $A_i\rho A_i^*$, counted with multiplicity (so $n = \dim H$). By computing the trace in a basis of eigenvectors, we see that $\operatorname{tr}(A_i\rho A_i^*) = \sum_{j=1}^n \lambda_j$. But $\operatorname{tr}(A_i\rho A_i^*) = \operatorname{tr}(A_i^* A_i\rho) = 0$, so we conclude that $\lambda_j = 0$ for all $1 \leq j \leq n$, and hence $A_i\rho A_i^* = 0$. Thus

$$\sum_{i\in\mathcal{O}'} A_i\rho A_i^* = \sum_{i\in\mathcal{O}} A_i\rho A_i^*.$$

□

This brings us to the main theorem of this chapter:

**Theorem 15.2.4** (No communication theorem)**.** *Let $H_A$ and $H_B$ be Hilbert spaces, let $\{A_i\}_{i=1}^k$ be a generalized measurement on $H_A$, and let $\rho$ be a mixed state on $H_A \otimes H_B$. Let $\rho'$ be the state after measuring $H_A \otimes H_B$ with $\{A_i \otimes \mathbb{1}\}_{i=1}^k$, without revealing the measurement outcome. Then*

$$\operatorname{tr}_A(\rho') = \operatorname{tr}_A(\rho).$$

In other words, the no communication theorem states that, until the measurement result is revealed, the state on $H_B$ doesn't change at all when we measure $H_A$. If we assume that the measurement result can't travel from location $A$ to location $B$ faster than the speed of light, then there's no conflict with relativity.

*Proof.* Suppose $\rho = |u\rangle\,|v\rangle\,\langle x|\,\langle y|$ for $|u\rangle\,,|x\rangle \in H_A$ and $|v\rangle\,,|y\rangle \in H_B$.

$$\begin{aligned}
\operatorname{tr}_A\left(\sum_{i\in\mathcal{O}}(A_i\otimes\mathbb{1})\rho(A_i^*\otimes\mathbb{1})\right) &= \sum_{i\in\mathcal{O}}\operatorname{tr}(A_i\,|u\rangle\,\langle x|\,A_i^*)\,|v\rangle\,\langle y| \\
&= \sum_{i\in\mathcal{O}}\langle x|A_i^*A_i|u\rangle\,|v\rangle\,\langle y| \\
&= \langle x|\sum_{i\in\mathcal{O}}A_i^*A_i|u\rangle\,|v\rangle\,\langle y| \\
&= \langle x|u\rangle\,|v\rangle\,\langle y| = \operatorname{tr}_A(\rho).
\end{aligned}$$

Extending linearly, we see that

$$\operatorname{tr}_A\left(\sum_{i\in\mathcal{O}}(A_i\otimes\mathbb{1})\rho(A_i^*\otimes\mathbb{1})\right) = \operatorname{tr}_A(\rho)$$

for all $\rho \in \operatorname{Lin}(H_A\otimes H_B)$. The theorem then follows from Corollary 15.2.3. □

# Chapter 16

# Abstract states and Gleason's theorem

We started with one type of state, vector states, and two types of operations, unitary operations and measurement in a basis. To this, we added mixed states, projective measurements, generalized measurements, and POVMs. At this point we should be asking if we're finally done, or if the notions of state and operation will need to be extended yet again at some point. As we mentioned in Chapter 14, generalized measurements aren't closed under coarse-graining, so the operations we've defined so far don't capture everything. The most general class of operations are quantum channels, and these are bit beyond the scope of this book. However, in this chapter we'll use the Frobenius inner product to show that, under some reasonable conditions, mixed states are the most general form of state we can define while keeping the framework we've already developed. We'll also show that POVMs are the most general form of operation in which a measurement is performed and the system is thrown out afterwards.

## 16.1 Abstract states

Let's try to figure out what a state could be in the abstract. We've already seen that obesrvables take the place of random variables in quantum probability theory. In particular, it makes sense to talk about the expected value of the observable $X$ when the system is in a given state. If the system is in mixed state $\rho$, then this expected value is $\mathrm{tr}(X\rho)$ by Exercise 14.4.8. This is a linear function of the observable $X$, which matches with what we might expect from classical probability, where expectation is a linear function of random variables.

If we want to preserve this feature of quantum probability, then whatever notion of state we use, a state should give us a linear expectation functional.

Rather than trying to capture all features that a state should have, we can just try to figure out what functionals can arise in this way. The function $X \mapsto \operatorname{tr}(X\rho)$ makes sense for any operator $X$, but not all operators are observables. However, the set of real-valued observables on a Hilbert space $H$ is $\operatorname{Lin}(H,H)_h$, which is an $\mathbb{R}$-vector space. The expected value of a real-valued observable should also be real, so our expectation functionals should be elements of $\operatorname{Lin}(H,H)_h^* = \operatorname{Lin}_{\mathbb{R}}(\operatorname{Lin}(H,H)_h, \mathbb{R})$, the $\mathbb{R}$-linear dual to $\operatorname{Lin}(H,H)_h$. However, it turns out that any element of $\operatorname{Lin}(H,H)_h^*$ can be extended uniquely to an element of $\operatorname{Lin}(H,H)^* = \operatorname{Lin}_{\mathbb{C}}(\operatorname{Lin}(H,H), \mathbb{C})$, the $\mathbb{C}$-linear dual to all operators:

**Exercise 16.1.1.** *Let $H$ be a Hilbert space.*

*(a) Show that for every operator $T \in \operatorname{Lin}(H,H)$, there are unique elements $A, B \in \operatorname{Lin}(H,H)_h$ such that $T = A + iB$. (A and B are called the* ***real and imaginary parts of*** *$T$).*

*(b) Let $f$ be an $\mathbb{R}$-linear function $\operatorname{Lin}(H,H)_h \to \mathbb{R}$. Prove that there is a unique $\mathbb{C}$-linear function $\tilde{f} : \operatorname{Lin}(H,H) \to \mathbb{C}$ such that $\tilde{f}|_{\operatorname{Lin}(H,H)_h} = f$.*

*(c) Show that the map*

$$\operatorname{Lin}(H,H)_h^* \to \{f \in \operatorname{Lin}(H,H)^* : f(\operatorname{Lin}(H,H)_h) \subseteq \mathbb{R}\} : f \mapsto \tilde{f}$$

*(where $\tilde{f}$ is the unique function associated to $f$ from part (b)) is a bijection.*

So we'll think of our expectation functionals as elements $f \in \operatorname{Lin}(H,H)^*$ such that $f(T) \in \mathbb{R}$ for all $T \in \operatorname{Lin}(H,H)_h$. We can add more conditions to this. For instance, if $T$ has only positive eigenvalues, then as an observable it only takes positive values, so we'd expect $f(T) \geq 0$ — in other words, we should have $f(T) \geq 0$ for all $T \in \operatorname{Lin}(H,H)_+$. Also, $\mathbb{1}$ is the observable which just takes constant value 1, so we should definitely have $f(\mathbb{1}) = 1$. It seems like we should keep going, but it turns out that these weak conditions will be all we need, and we can now define:

**Definition 16.1.2.** *Let $H$ be a Hilbert space. A linear functional $f \in \operatorname{Lin}(H,H)^*$ is* ***positive*** *if $f(T) \geq 0$ for all $T \in \operatorname{Lin}(H,H)_+$. An* ***abstract state*** *on $H$ is a positive linear functional $f$ such that $f(\mathbb{1}) = 1$.*

The condition $f(T) \geq 0$ means in particular that $f(T) \in \mathbb{R}$ (or otherwise the comparison wouldn't make sense). It seems like we've forgotten about the condition that $f(T) \in \mathbb{R}$ when $T \in \mathrm{Lin}(H,H)_h$, but this is actually implied by the condition that $f(T) \geq 0$ for all $T \in \mathrm{Lin}(H,H)_+$.

**Exercise 16.1.3.** *Let $H$ be a Hilbert space.*

*(a) Use the spectral decomposition to show that for every operator $T \in \mathrm{Lin}(H,H)_h$, there are unique operators $A, B \in \mathrm{Lin}(H,H)_+$ such that $T = A - B$ and $H = (\ker A)^\perp \oplus (\ker B)^\perp \oplus \ker T$. (A and B are called the* ***positive and negative parts of*** *$T$).*

*(b) Suppose $f$ is an element $\mathrm{Lin}(H,H)^*$ such that $f(T) \geq 0$ for all $T \in \mathrm{Lin}(H,H)_+$. Use part (a) to show that $f(T) \in \mathbb{R}$ for all $T \in \mathrm{Lin}(H,H)_h$.*

Now, $\mathrm{Lin}(H,H)$ is a Hilbert space with the Frobenius inner product, so every element $f \in \mathrm{Lin}(H,H)^*$ is of the form

$$T \mapsto \langle S, T\rangle_F = \mathrm{tr}(S^*T)$$

for some unique $S \in \mathrm{Lin}(H,H)^*$. We'd like to know which operators $S$ correspond to abstract states $f$. The condition $f(\mathbb{1}) = 1$ is immediate: it holds if and only if $\mathrm{tr}(S^*) = 1$. For positivity, we first need to characterize when $f(T) \in \mathbb{R}$ for all $T \in \mathrm{Lin}(H,H)_h$).

**Theorem 16.1.4.** *Given $S \in \mathrm{Lin}(H,H)$, define $f \in \mathrm{Lin}(H,H)^*$ by $f(T) = \langle S, T\rangle_F$. Then the following are equivalent:*

*(i) $f(T) \in \mathbb{R}$ for all $f \in \mathrm{Lin}(H,H)_h$,*

*(ii) $\overline{f(T)} = f(T^*)$ for all $T \in \mathrm{Lin}(H,H)$, and*

*(iii) $S \in \mathrm{Lin}(H,H)_h$.*

*Proof.* Suppose (i) is true and that $T \in \mathrm{Lin}(H,H)$. By Exercise 16.1.1, we can write $T = A + iB$ where $A, B \in \mathrm{Lin}(H,H)_h$. Then $f(A), f(B) \in \mathbb{R}$ and $T^* = A - iB$, so

$$\overline{f(T)} = \overline{f(A) + if(B)} = f(A) - if(B) = f(A - iB) = f(T^*).$$

We conclude (ii) holds.

Next, suppose condition (ii) holds and that $|x\rangle, |y\rangle \in H$. Then

$$\langle S\,|x\rangle, |y\rangle\rangle = \langle x|S^*|y\rangle = \mathrm{tr}(S^*\,|y\rangle\langle x|) = f(|y\rangle\langle x|) = \overline{f(|x\rangle\langle y|)}$$

$$= \overline{\operatorname{tr}(S^* |x\rangle \langle y|)} = \overline{\langle y|S^*|x\rangle} = \overline{\langle S\,|y\rangle\,, |x\rangle\rangle} = \langle |x\rangle\,, S\,|y\rangle\rangle.$$

Since this holds for all $|x\rangle\,, |y\rangle$, we conclude that $S^* = S$, so (iii) holds.

Finally, if condition (iii) holds and $T \in \operatorname{Lin}(H, H)_h$, then

$$\overline{f(T)} = \overline{\operatorname{tr}(S^*T)} = \overline{\operatorname{tr}(T^*S)} = \overline{\langle T, S\rangle_F} = \langle S, T\rangle_F = f(T),$$

so $f(T) \in \mathbb{R}$ for all $T \in \operatorname{Lin}(H, H)_h$. Thus all three conditions are equivalent. □

Now we can characterize positive linear functionals.

**Theorem 16.1.5.** *Given $S \in \operatorname{Lin}(H, H)$, define $f \in \operatorname{Lin}(H, H)^*$ by $f(T) = \langle S, T\rangle_F$. Then $f(T) \geq 0$ for all $T \in \operatorname{Lin}(H, H)_+$ if and only if $S \in \operatorname{Lin}(H, H)_+$.*

*Proof.* Suppose $S, T \in \operatorname{Lin}(H, H)_+$. By Theorem 14.3.4, there are operators $A, B \in \operatorname{Lin}(H, H)$ such that $S = A^*A$ and $T = B^*B$. Then

$$\begin{aligned} f(T) &= \langle S, T\rangle_F = \operatorname{tr}(S^*T) = \operatorname{tr}(A^*AB^*B) \\ &= \operatorname{tr}(BA^*AB^*) = \operatorname{tr}((AB^*)^*(AB^*)) = \langle AB^*, AB^*\rangle_F \geq 0. \end{aligned}$$

Conversely, suppose that $f(T) \geq 0$ for all $T \in \operatorname{Lin}(H, H)_+$. By Exercise 16.1.3, $f(T) \in \mathbb{R}$ for all $T \in \operatorname{Lin}(H, H)_h$, so $S^* = S$. If $|x\rangle \in H$, then $|x\rangle \langle x| \in \operatorname{Lin}(H, H)_+$, so

$$0 \leq f(|x\rangle \langle x|) = \operatorname{tr}(S\,|x\rangle \langle x|) = \langle x|S|x\rangle\,.$$

We conclude that $S$ is positive semidefinite. □

Recall from Exercise 14.3.6 that $\operatorname{Lin}(H, H)_+$ is a convex cone. In general, if $C$ is a convex cone in a Hilbert space $H$, the dual cone to $C$ is

$$\{v \in H : \langle v, c\rangle \geq 0 \text{ for all } c \in C\}.$$

With this terminology, Theorem 16.1.5 states that $\operatorname{Lin}(H, H)_+$ is a self-dual cone.

We can now characterize abstract states.

**Corollary 16.1.6.** *Given a density matrix $\rho$, define $f_\rho \in \operatorname{Lin}(H, H)^*$ by $f_\rho(T) = \operatorname{tr}(T\rho)$. Then the function*

$$\rho \mapsto f_\rho$$

*is a bijection between density matrices and abstract states. In particular, every abstract state is of the form $f_\rho$ for a unique density matrix $\rho$.*

*Proof.* We know that the map $S \mapsto f_S \in \mathrm{Lin}(H,H)^*$, where $f_S(T) = \mathrm{tr}(S^*T)$, is an antilinear isomorphism, and in particular a bijection. By Theorem 16.1.5, $f_\rho$ is positive if and only if $\rho \in \mathrm{Lin}(H,H)_+$, in which case $\rho^* = \rho$ and hence

$$\mathrm{tr}(\rho^*T) = \mathrm{tr}(\rho T) = \mathrm{tr}(T\rho).$$

Finally, when $\rho^* = \rho$, $f(\mathbb{1}) = 1$ if and only if $\mathrm{tr}(\rho) = 1$. So $f_\rho$ is an abstract state if and only if $\rho$ is a density matrix. □

We conclude that abstract states must come from the mixed states we've already defined.

## 16.2 Destructive measurements and POVMs

We can analyze destructive measurements similarly. Recall that destructive measurements are measurements $\mathcal{M}$ where we get some outcome drawn from a set $\mathcal{O}$, and then discard the system afterwards (so the state of the system after measurement is irrelevant). Such a measurement is completely determined by the probability of getting outcome $i \in \mathcal{O}$ on state $\rho$. To formalize this, let

$$\mathrm{Density}(H) = \{\rho \in \mathrm{Lin}(H,H)_+ : \mathrm{tr}(\rho) = 1\}$$

denote the set of density matrices on $H$. We can think of an abstract destructive measurement $\mathcal{M}$ with outcome set $\mathcal{O}$ on a Hilbert space $H$ as a collection $\{\mathcal{M}_i\}_{i\in\mathcal{O}}$, where each $\mathcal{M}_i$ is a function $\mathrm{Density}(H) \to \mathbb{R}$. As with abstract states, we can write down conditions that an abstract destructive measurement should satisfy. For instance, we should have $\mathcal{M}_i(\rho) \geq 0$ for all $\rho \in \mathrm{Density}(H)$ and $1 \leq i \leq n$, and

$$\sum_{i=1}^{n} \mathcal{M}_i(\rho) = 1$$

for all $\rho \in \mathrm{Density}(H)$.

On the other hand, it doesn't make sense to require that the functions $\mathcal{M}_i$ are linear, since the set $\mathrm{Density}(H)$ is not a subspace of $\mathrm{Lin}(H,H)$, or even a convex cone. However, by Exercise 14.3.6, $\mathrm{Density}(H)$ is a convex set, in the sense that if $\rho_1, \ldots, \rho_n \in \mathrm{Density}(H)$, and $\{\lambda_j\}_{j=1}^n$ is a probability distribution on $\{1, \ldots, n\}$, $n \geq 1$, then

$$\rho = \sum_{j=1}^{n} \lambda_j \rho_j \in \mathrm{Density}(H).$$

By Lemma 15.2.1, $\rho$ is the mixed state we get by picking state $\rho_j$ with probability $\lambda_j$. Consequently, the probability $\mathcal{M}_i(\rho)$ of measuring outcome $i$ when the system is in state $\rho$ should be

$$\sum_{j=1}^{n} \lambda_j \mathcal{M}_i(\rho_j).$$

**Lemma 16.2.1.** *Let $f : \mathrm{Density}(H) \to \mathbb{R}$ be a function such that*

$$f\left(\sum_{i=1}^{n} \lambda_i \rho_i\right) = \sum_{i=1}^{n} \lambda_i f(\rho_i)$$

*for all $n \geq 1$, $\rho_1, \ldots, \rho_n \in \mathrm{Density}(H)$, and probability distributions $\{\lambda_i\}_{i=1}^{n}$ on $\{1, \ldots, n\}$. Then there is a unique linear function $\tilde{f} \in \mathrm{Lin}(H, H)$ such that $\tilde{f}(\rho) = f(\rho)$ for all $\rho \in \mathrm{Density}(H)$.*

*Proof.* By Exercise 16.1.1, we only need to show that there is a unique $\mathbb{R}$-linear function $\tilde{f} \in \mathrm{Lin}(H, H)_h^*$ such that $\tilde{f}(\rho) = f(\rho)$. For book-keeping purposes, define

$$R : \mathrm{Lin}(H, H)_+ \to \mathrm{Density}(H) : T \mapsto \begin{cases} \frac{T}{\mathrm{tr}(T)} & T \neq 0 \\ \frac{\mathbb{1}}{\mathrm{tr}(\mathbb{1})} & T = 0 \end{cases}.$$

From the spectral decomposition, we can see that $\rho \in \mathrm{Lin}(H, H)_+$ is zero if and only if $\mathrm{tr}(\rho) = 0$, so $R$ is well-defined. With this notation, we get that $T = \mathrm{tr}(T) R(T)$ for all $T \in \mathrm{Lin}(H, H)_+$. Define

$$\tilde{f}(T) = \mathrm{tr}(A) \cdot f(R(A)) - \mathrm{tr}(B) \cdot f(R(B)),$$

where $T = A - B$ is the decomposition of $T$ into positive and negative parts from Exercise 16.1.3.

Because $A$ and $B$ are uniquely determined by $T$, $\tilde{f}$ is well-defined. However, it is not at all obvious that $\tilde{f}$ is linear. To prove linearity, we first show that $\tilde{f}$ preserves scalar multiplication. Let $\lambda \in \mathbb{R}$ and $T \in \mathrm{Lin}(H, H)_h$. Let $T = A - B$ be the decomposition of $T$ into positive and negative parts. If $\lambda = 0$, then $\tilde{f}(\lambda T) = \mathrm{tr}(0) \cdot f(R(0)) - \mathrm{tr}(0) \cdot f(R(0)) = 0 = \lambda \tilde{f}(T)$ as desired. Suppose $\lambda > 0$. Then $(\ker \lambda A)^\perp = (\ker A)^\perp$, $(\ker \lambda B)^\perp = (\ker B)^\perp$, and $\ker \lambda T = \ker T$. Since $\lambda A$ and $\lambda B$ are positive semidefinite, $\lambda T = \lambda A - \lambda B$ is the decomposition of $\lambda T$ into positive and negative parts. So $R(\lambda A) = A$ and $R(\lambda B) = B$, we conclude that

$$\tilde{f}(\lambda T) = \mathrm{tr}(\lambda A) f(R(\lambda A)) - \mathrm{tr}(\lambda B) f(R(\lambda B))$$

$$= \lambda \operatorname{tr}(A) f(R(A)) - \lambda \operatorname{tr}(B) f(R(B)) = \lambda \tilde{f}(T).$$

If $\lambda < 0$, then we can make the same argument, except that $-\lambda A$ is now the negative part of $\lambda T$, and $-\lambda B$ is the positive part. So we conclude that $\tilde{f}(\lambda T) = \lambda \tilde{f}(T)$ for all $\lambda \in \mathbb{R}$ and $T \in \operatorname{Lin}(H, H)_h$.

Next, we can show that $\tilde{f}$ preserves vector addition. Indeed, let $T_0 = T_1 + T_2$ for $T_1, T_2 \in \operatorname{Lin}(H, H)_h$. If $T_1 = T_2 = 0$, then $\tilde{f}(T_0) = 0 = \tilde{f}(T_1) + \tilde{f}(T_2)$ as desired, so we can assume that at least one of $T_1$ and $T_2$ is non-zero. Let $T_i = A_i - B_i$ be the decomposition of $T_i$ into positive and negative parts, $i = 0, 1, 2$. Note that it is not necessarily true that $A_0 = A_1 + A_2$ or $B_0 = B_1 + B_2$. However, since

$$A_0 - B_0 = A_1 - B_1 + A_2 - B_2,$$

we have that

$$A_0 + B_1 + B_2 = B_0 + A_1 + A_2.$$

Let $S = A_0 + B_1 + B_2$, and $\lambda = \operatorname{tr}(S)$. Since one of $T_1$ or $T_2$ is non-zero, at least one of at least one of $A_1$, $B_1$, $A_2$, or $B_2$ is non-zero, and hence at least one of $\operatorname{tr}(A_1)$, $\operatorname{tr}(B_1)$, $\operatorname{tr}(A_2)$, or $\operatorname{tr}(B_2)$ is strictly greater than zero. Since $\operatorname{tr}(A_i) \geq 0$ and $\operatorname{tr}(B_i) \geq 0$ for all $i = 0, 1, 2$, we conclude that $\lambda > 0$. Now $S$ is positive semidefinite by Exercise 14.3.6, so $S/\lambda$ is a density matrix. Since

$$\frac{1}{\lambda} S = \frac{\operatorname{tr}(A_0)}{\lambda} R(A_0) + \frac{\operatorname{tr}(B_1)}{\lambda} R(B_1) + \frac{\operatorname{tr}(B_2)}{\lambda} R(B_2),$$

and

$$\frac{\operatorname{tr}(A_0)}{\lambda} + \frac{\operatorname{tr}(B_1)}{\lambda} + \frac{\operatorname{tr}(B_2)}{\lambda} = \frac{\operatorname{tr}(A_0 + B_1 + B_2)}{\lambda} = 1,$$

we conclude that

$$f(S/\lambda) = \frac{\operatorname{tr}(A_0)}{\lambda} f(R(A_0)) + \frac{\operatorname{tr}(B_1)}{\lambda} f(R(B_1)) + \frac{\operatorname{tr}(B_2)}{\lambda} f(R(B_2)).$$

Similarly, since

$$\frac{1}{\lambda} S = \frac{\operatorname{tr}(B_0)}{\lambda} R(B_0) + \frac{\operatorname{tr}(A_1)}{\lambda} R(A_1) + \frac{\operatorname{tr}(A_2)}{\lambda} R(A_2),$$

we conclude that

$$f(S/\lambda) = \frac{\operatorname{tr}(B_0)}{\lambda} f(R(B_0)) + \frac{\operatorname{tr}(A_1)}{\lambda} f(R(A_1)) + \frac{\operatorname{tr}(A_2)}{\lambda} f(R(A_2)).$$

Putting our two expressions for $f(S/\lambda)$ together and clearing denominators, we get that

$$\operatorname{tr}(A_0) f(R(A_0)) + \operatorname{tr}(B_1) f(R(A_1)) + \operatorname{tr}(B_2) f(R(A_2))$$

$$= \operatorname{tr}(B_0)f(R(A_0)) + \operatorname{tr}(A_1)f(R(A_1)) + \operatorname{tr}(A_2)f(R(A_2)),$$

and hence

$$\begin{aligned}\tilde{f}(T_0) &= \operatorname{tr}(A_0)f(R(A_0)) - \operatorname{tr}(B_0)f(R(B_0)) \\ &= \operatorname{tr}(A_1)f(R(A_1)) + \operatorname{tr}(A_2)f(R(A_2)) - \operatorname{tr}(B_1)f(R(A_1)) - \operatorname{tr}(B_2)f(R(A_2)) \\ &= \tilde{f}(T_1) + \tilde{f}(T_1).\end{aligned}$$

Hence $\tilde{f}$ is linear. If $\rho$ is a density matrix, then $R(\rho) = \rho$, and $\tilde{f}(\rho) = \operatorname{tr}(\rho)f(\rho) = f(\rho)$. Finally, if $T = A - B$ is the decomposition of $T$ into positive and negative parts, then $T = \operatorname{tr}(A)R(A) - \operatorname{tr}(B)R(B)$, so $\mathrm{Density}(H)$ spans $\mathrm{Lin}(H,H)_h$. Hence any linear function is determined by its values on $\mathrm{Density}(H)$, so $\tilde{f}$ is the unique element of $\mathrm{Lin}(H,H)_h^*$ with $\tilde{f}|_{\mathrm{Density}(H)} = f$. □

Using Lemma 16.2.1, we can show that any "abstract destructive measurement" is equivalent to a POVM.

**Theorem 16.2.2.** *Let $H$ be a Hilbert space, $\mathcal{O}$ be a finite set, and $\{\mathcal{M}_i\}_{i\in\mathcal{O}}$ be a collection of functions $\mathcal{M}_i : \mathrm{Density}(H) \to \mathbb{R}$ such that*

*(1) $\mathcal{M}_i(\rho) \geq 0$ for all $i \in \mathcal{O}$ and $\rho \in \mathrm{Density}(H)$,*

*(2) if $\rho_1, \ldots, \rho_n \in \mathrm{Density}(H)$ and $\{\lambda_j\}_{j=1}^n$ is a probability distribution on $\{1, \ldots, n\}$, then*

$$\mathcal{M}_i(\lambda_1\rho_1 + \ldots + \lambda_n\rho_n) = \lambda_1\mathcal{M}_i(\rho_1) + \ldots + \lambda_n\mathcal{M}_i(\rho_n)$$

*for all $i$, and*

*(3) $\sum_{i\in\mathcal{O}} \mathcal{M}_i(\rho) = 1$ for all $\rho \in \mathrm{Density}(H)$.*

*Then there is a unique POVM $\{M_i\}_{i\in\mathcal{O}}$ on $H$ such that $\mathcal{M}_i(\rho) = \operatorname{tr}(M_i\rho)$ for all $i \in \mathcal{O}$.*

*Proof.* By Lemma 16.2.1, every function $\mathcal{M}_i$ can be extended to a linear function $\tilde{\mathcal{M}}_i \in \mathrm{Lin}(H,H)^*$. If $T \in \mathrm{Lin}(H,H)_+$, then either $T = 0$, in wich case $\tilde{\mathcal{M}}_i(T) = 0$, or $T/\operatorname{tr}(T) \in \mathrm{Density}(H)$, and $\tilde{\mathcal{M}}_i(T) = \operatorname{tr}(T)\tilde{\mathcal{M}}_i(T/\operatorname{tr}(T)) = \operatorname{tr}(T)\mathcal{M}_i(T/\operatorname{tr}(T)) \geq 0$. So $\tilde{\mathcal{M}}_i$ is positive. It follows from Theorem 16.1.5 that there is some $M_i \in \mathrm{Lin}(H,H)_+$ with $\tilde{\mathcal{M}}_i(T) = \operatorname{tr}(M_iT)$ for all $T \in \mathrm{Lin}(H,H)$.

Let $M = \sum_{i\in\mathcal{O}} M_i$. By condition (3), $\operatorname{tr}(M\rho) = 1$ for all $\rho \in \mathrm{Density}(H)$. We also know that $\operatorname{tr}(\mathbb{1} \cdot \rho) = \operatorname{tr}(\rho) = 1$ for all $\rho \in \mathrm{Density}(H)$. The function $\rho \mapsto 1$ satisfies the hypothesis of Lemma 16.2.1, and hence has a unique linear extension in $\mathrm{Lin}(H,H)$. Hence $T \mapsto \operatorname{tr}(MT)$ and $T \mapsto \operatorname{tr}(\mathbb{1} \cdot \rho)$ must be equal as elements of $\mathrm{Lin}(H,H)^*$, which means that $M = \mathbb{1}$. So $\{M_i\}_{i\in\mathcal{O}}$ is a POVM. □

## 16.3 Gleason's theorem for POVMs

In Section 16.1, we defined abstract states as linear functions on $\mathrm{Lin}(H, H)$. Linearity was justified by the fact that expectation functionals are linear in classical probability. In particular, if $X$ and $Y$ are classical random variables, then $\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y]$. The reason is that if $X$ takes value $X(i)$ on outcome $i$, and $Y$ takes value $Y(i)$ on outcome $i$, then $X + Y$ is the random variable which takes outcome $X(i)+Y(i)$ on outcome $i$. In other words, $X+Y$ is the random variable we get by taking the values of $X$ and $Y$ and adding them together.

Suppose $X$ and $Y$ are observables instead of random variables. If $X$ and $Y$ are jointly measurable, then there is a complete family of self-adjoint projections $\{P_1, \ldots, P_m\}$ and scalars $\alpha_1, \beta_1, \ldots, \alpha_m, \beta_m$ such that

$$X = \sum_{i=1}^{m} \alpha_i P_i \text{ and } Y = \sum_{i=1}^{m} \beta_i P_i.$$

We can think of $X$ as the observable which measures in projective measurement $\{P_1, \ldots, P_m\}$, and then returns $\alpha_i$ on outcome $i$. Similarly, $Y$ is the observable which measures in the same projective measurement, and returns $\beta_i$ on outcome $i$. Since

$$X + Y = \sum_{i=1}^{m} (\alpha_i + \beta_i) P_i,$$

we can think of $X + Y$ as the observable which measures both $X$ and $Y$, and returns the sum of the outcomes, just like with classical random variables.

Unfortunately, this description of $X+Y$ falls apart if $X$ and $Y$ aren't jointly measurable, since the spectral decomposition of $X + Y$ can be very different from the spectral decomposition of $X$ or $Y$. As a self-adjoint operator, $X + Y$ is still an observable, but it's not clear how it relates to the observables $X$ and $Y$. As a result, it's not clear at all that states should give rise to linear expectation functionals.

To explore this idea, let's try to define states as functions on POVMs, rather than on observables. Given a state and a POVM $\{M_i\}_{i=1}^n$ on a Hilbert space $H$, it should make sense to talk about the probability of getting outcome $i$. Let $\mathrm{POVM}_n(H)$ denote the set of POVMs on $H$ with outcome set $\{1, \ldots, n\}$. In this section, we'll write POVMs as vectors $M = (M_1, \ldots, M_n)$ of operators. Every state should give rise to a collection of functions $\{f_i^n : n \geq 1, 1 \leq i \leq n\}$, where $f_i^n : \mathrm{POVM}_n(H) \to \mathbb{R}$ sends a POVM $M$ to the probability

$f_i^n(M)$ of measuring outcome $i$. As in the previous sections, we can write down conditions that these functions need to satisfy. For instance, clearly we want $f_i^n(M) \geq 0$ and $\sum_{i=1}^n f_i^n(M) = 1$ for all $M \in \mathrm{POVM}_n(H)$. Suppose $M = (M_1, \ldots, M_n) \in \mathrm{POVM}_n(H)$, and

$$I : \{1, \ldots, n\} \to \{1, \ldots, m\}$$

is a surjective function. The collection $\{I^{-1}(i) : 1 \leq i \leq m\}$ is a partition of $\{1, \ldots, n\}$, and the coarse-graining of $M$ by this partition is the POVM $N = (N_1, \ldots, N_m) \in \mathrm{POVM}_m(H)$ with

$$N_i = \sum_{j \in I^{-1}(i)} M_j.$$

In this section, we'll also call $N$ the **coarse-graining of $M$ by the function $I$**. Since $N$ is just the measurement where we first measure $M$, and then return $I(j)$ where $j$ is the outcome of $M$, the probability $f_i^m(N)$ of measuring outcome $i$ with POVM $N$ should be

$$\sum_{j \in I^{-1}(i)} f_j^n(M),$$

the probability of measuring $j \in I^{-1}(i)$ with POVM $M$. This leads to the following definition:

**Definition 16.3.1.** *A **state datum on a Hilbert space** $H$ is a collection of functions*

$$\{f_i^n : n \geq 1, 1 \leq i \leq n\}$$

*such that*

*(1) $f_i^n$ is a function $\mathrm{POVM}_n(H) \to [0, +\infty) \subseteq \mathbb{R}$ for all $n \geq 1$, $1 \leq i \leq n$,*

*(2) $\sum_{i=1}^n f_i^n(M) = 1$ for all $n \geq 1$ and $M \in \mathrm{POVM}_n(H)$, and*

*(3) for all $n \geq m \geq 1$ and surjective functions $I : \{1, \ldots, n\} \to \{1, \ldots, m\}$, if $N \in \mathrm{POVM}_m(H)$ is the coarse-graining of $M \in \mathrm{POVM}_n(H)$ by $I$, then*

$$f_i^m(N) = \sum_{j \in I^{-1}(i)} f_j^n(M)$$

*for all $1 \leq i \leq m$.*

Since the functions $f_i^n$ aren't required to be linear in any way, it seems like this notion of state could be much more general than the abstract states we defined in Section 16.1. Gleason's theorem is that, in fact, every state datum has to come from an abstract state (and hence from a density matrix):

**Theorem 16.3.2** (Gleason's theorem for POVMs)**.** *Let $\{f_i^n\}$ be a state datum on a Hilbert space $H$. Then there is a unique abstract state $f$ on $H$ such that*

$$f_i^n((M_1, \dots, M_n)) = f(M_i)$$

*for all $n \geq 1$, $1 \leq i \leq n$, and $M = (M_1, \dots, M_n) \in \mathrm{POVM}_n(H)$.*

*Proof.* Let $X$ be the set of elements $M \in \mathrm{Lin}(H, H)_+$ which appear in a POVM, meaning that $M = M_i$ for some $n \geq 1$, $1 \leq i \leq n$, and POVM $(M_1, \dots, M_n) \in \mathrm{POVM}_n(H)$. Notice that if $M \in X$ is equal to $M_i$ for $(M_1, \dots, M_n) \in \mathrm{POVM}_n(H)$, then

$$\mathbb{1} - M = \sum_{j \neq i} M_j \in \mathrm{Lin}(H, H)_+.$$

Conversely, if $\mathbb{1} - M \in \mathrm{Lin}(H, H)_+$, then $(M, \mathbb{1} - M) \in \mathrm{POVM}_2(H)$. So $X = \{M \in \mathrm{Lin}(H, H)_+ : \mathbb{1} - M \in \mathrm{Lin}(H, H)_+\}$.

Define $g : X \to \mathbb{R}$ by $f(M) = f_1^2((M, \mathbb{1} - M))$. By the coarse-graining condition,

$$f_i^n((M_1, \dots, M_n)) = f_1^2((M_i, \mathbb{1} - M_i)) = g(M_i)$$

for all $n \geq 1$, $1 \leq i \leq n$, and $(M_1, \dots, M_n) \in \mathrm{POVM}_n(H)$. So we see already that a state datum reduces to the single function $g$.

If $M \in X$ and $0 \leq \lambda \leq 1$, then then $\mathbb{1} - \lambda M = (\mathbb{1} - M) + (1 - \lambda)M \in \mathrm{Lin}(H, H)_+$, so $\lambda M \in X$.

If $0 \leq \lambda \leq 1$ and $M \in X$, then $\mathbb{1} - \lambda M = (\mathbb{1} - M) + (1 - \lambda)M$, so $\lambda M \in X$. Furthermore, the coarse-graining condition implies that

$$\begin{aligned} g(M) = f_1^2((M, \mathbb{1} - M)) &= f_1^3((\lambda M, (1 - \lambda)M, \mathbb{1} - M)) + f_2^3((\lambda M, (1 - \lambda)M, \mathbb{1} - M)) \\ &= g(\lambda M) + g((1 - \lambda)M) \geq g(\lambda M). \end{aligned}$$

As another application of the coarse-graining condition, if $n \geq 1$ and $M \in X$, then

$$g(M) = f_1^2((M, \mathbb{1} - M)) = \sum_{j=1}^{n} f_j^{n+1}((\tfrac{1}{n}M, \dots, \tfrac{1}{n}M, \mathbb{1} - M)) = \sum_{j=1}^{n} g(\tfrac{1}{n}M) = ng(\tfrac{1}{n}M).$$

Hence $g(\frac{1}{n}M) = \frac{1}{n}g(M)$ for all $n \geq 1$ and $M \in X$. If $1 \leq m \leq n$, then

$$\tfrac{1}{n}g(M) = g(\tfrac{1}{n}M) = g(\tfrac{1}{m} \cdot \tfrac{m}{n}M) = \tfrac{1}{m}g(\tfrac{m}{n}M),$$

so $g(\frac{m}{n}M) = \frac{m}{n}g(M)$. In other words, $g(\lambda M) = \lambda g(M)$ for all $\lambda \in \mathbb{Q} \cap [0,1]$.

Suppose $\lambda \in [0,1]$ is an arbitrary real number, rather than a rational, and $M \in X$. Let $(p_n)_{n=1}^{\infty}$ and $(q_n)_{n=1}^{\infty}$ be two sequences in $\mathbb{Q} \cap [0,1]$ such that

$$\lim_{n \to +\infty} p_n = \lim_{n \to +\infty} q_n = \lambda,$$

and $p_n \leq \lambda \leq q_n$ for all $n \geq 1$. Since $p_n M = \frac{p_n}{\lambda} \cdot \lambda M$ and $\lambda M = \frac{\lambda}{q_n}M$, where and $0 \leq \frac{p_n}{\lambda}, \frac{\lambda}{q_n} \leq 1$, we get that

$$p_n g(M) = g(p_n M) \leq g(\lambda M) \leq g(q_n M) = q_n g(M)$$

for all $n \geq 1$. Taking limits, we see that $\lambda g(M) \leq g(\lambda M) \leq \lambda g(M)$. We conclude that $g(\lambda M) = \lambda g(M)$ for all $M \in X$ and $0 \leq \lambda \leq 1$.

We are close to being able to define $f$. Suppose $\rho$ is a density matrix, with spectral decomposition $\rho = \sum_{i=1}^{n} \lambda_i P_i$. Since $\rho$ is positive semidefinite with $\operatorname{tr} \rho = \sum_{i=1}^{n} \lambda_i \dim \operatorname{Im} P_i = 1$, we have $0 \leq \lambda_i \leq 1$ for all $i$. Hence $\mathbb{1} - \rho = \sum_{i=1}^{n}(1 - \lambda_i)P_i$ is positive semidefinite. We conclude that $\mathrm{Density}(H) \subseteq X$.

Suppose $\rho_1, \ldots, \rho_n \in \mathrm{Density}(H)$, and $\{\lambda_i\}_{i=1}^{n}$ is a probability distribution on $\{1, \ldots, n\}$. Let $\rho = \sum_{i=1}^{n} \lambda_i \rho_i$. Applying coarse-graining one final time,

$$g(\rho) = \sum_{i=1}^{n} f_i^{n+1}((\lambda_1\rho_1, \ldots, \lambda_n\rho_n, \mathbb{1} - \rho)) = \sum_{i=1}^{n} g(\lambda_i \rho_i) = \sum_{i=1}^{n} \lambda_i g(\rho_i).$$

By Lemma 16.2.1, there is a unique linear function $f \in \mathrm{Lin}(H,H)^*$ with $f(\rho) = g(\rho)$ for all $\rho \in \mathrm{Density}(H)$. Suppose $M \in \mathrm{Lin}(H,H)_+$. If $M = 0$, then $f(M) = g(M) = 0$. If $M \neq 0$, then $f(M) = \operatorname{tr}(M)f(M/\operatorname{tr}(M)) = \operatorname{tr}(M)g(M/\operatorname{tr}(M)) \geq 0$, so $f$ is positive. In addition, if $M \in X$ and $\operatorname{tr}(M) \leq 1$, then $\operatorname{tr}(M)g(M/\operatorname{tr}(M)) = g(\frac{\operatorname{tr}(M)}{\operatorname{tr}(M)}M) = g(M)$, while if $\operatorname{tr}(M) \geq 1$, then $0 \leq 1/\operatorname{tr}(M) \leq 1$ and $\operatorname{tr}(M)g(M/\operatorname{tr}(M)) = \frac{\operatorname{tr}(M)}{\operatorname{tr}(M)}g(M) = g(M)$. In both cases, we conclude that $f(M) = g(M)$ for all $M \in X$. In particular, $f(\mathbb{1}) = 1$, so $f$ is an abstract state, with

$$.f_i^n((M_1, \ldots, M_n)) = g(M_i) = f(M_i)$$

for any POVM $(M_1, \ldots, M_n)$ as desired. Any other abstract state $f'$ satisfying this condition must have $f'(\rho) = g(\rho)$ for all $\rho \in \mathrm{Density}(H)$, so $f$ is the unique abstract state satisfying this condition. □

As often happens in math, Gleason's theorem for POVMs is not due to Gleason, but rather to Busch and Caves, Fuchs, Manne, and Renes. Gleason's original theorem was for projective measurements, rather than POVMs. Strangely, the original version for projective measurements does not hold when $\dim H = 2$.

Gleason's theorem combined with Corollary 16.1.6 tells us that if the state of a system $\psi$ can be described by a state datum $\{f_i^n\}$, then there will be a unique mixed state $\rho$ such that the probability of measuring outcome $i$ with POVM $\{M_i\}_{i\in\mathcal{O}}$ is $\operatorname{tr}(M_i\rho)$. That means that if we perform a generalized measurement $A = \{A_i\}_{i\in\mathcal{O}}$, the probability of measuring outcome $i$ is $\operatorname{tr}(A_i^* A_i \rho)$. What about the state after performing the measurement $A$? Well, suppose we have another generalized measurement $B = \{B_j\}_{j\in\mathcal{O}'}$. Measuring $A$ followed by $B$ gives an outcome $(j, i) \in \mathcal{O}' \times \mathcal{O}$, and is described by the generalized measurement $\{B_j A_i\}_{(j,i)\in\mathcal{O}'\times\mathcal{O}}$. The probability of getting outcome $(j, i)$ from this measurement when the system is in state $\psi$ is

$$\operatorname{tr}(A_i^* B_j^* B_j A_i \rho) = \operatorname{tr}(B_j^* B_j A_i \rho A_i^*).$$

Assuming the probability $\operatorname{tr}(A_i^* A_i \rho)$ of getting outcome $i$ is non-zero, the probability of getting outcome $(j, i)$ given that we got outcome $i$ from measurement $A$ is

$$\operatorname{tr}(B_j^* B_j A_i \rho A_i^*)/\operatorname{tr}(A_i^* A_i \rho).$$

Let $\{g_i^n\}$ be the state datum describing the state of the system after getting outcome $i$ from measurement $A$. What we've shown is that

$$g_i^n((M_1, \dots, M_n)) = \operatorname{tr}(M_i A_i \rho A_i^*)/\operatorname{tr}(A_i^* A_i \rho).$$

It follows that the unique mixed state corresponding to state datum $\{g_i^n\}$ must be $A_i \rho A_i^*/\operatorname{tr}(A_i^* A_i \rho)$, which agrees with our formula for mixed states. So it's not possible to, for instance, define a notion of state where the outcome probabilities for a measurement can be described by a mixed state, but with a different rule for the state of the system after measurement.

# Chapter 17

# The unitary group and the quantum control question

In previous chapters, we've looked a lot at the question of what operations are possible in quantum theory. We first introduced measurement in a basis, then unitary operators, then projective measurement, and finally generalized measurements, which include both projective measurements and unitary time evolution. In doing this, we haven't considered at all what might be called the *quantum control question*: what operations can we actually create?

One of the things we showed is that time evolution operators have to be unitary. As the following exercise partially shows, we can reduce many cases of the quantum control question to the *unitary quantum control question*: what unitary operators can we implement as time evolution operators?

**Exercise 17.0.1.** *Let $H = \mathbb{C}X$. An observable $T$ on $H$ is said to be diagonal if the matrix $[T]_{\mathcal{B},\mathcal{B}}$ is diagonal, where $\mathcal{B}$ is the computational basis. Show that any observable on $H$ can be implemented as a unitary operation, followed by a diagonal observable, followed by another unitary operation.*

Of course, the answer to the quantum control question will depend on the physical system in question, and is not a question we can answer mathematically. However, in this chapter, we'll look at the concept of matrix groups, which is useful in thinking about the quantum control question conceptually.

## 17.1 Matrix groups

**Definition 17.1.1.** *A* ***matrix group*** *$G$ is a subset $G \subseteq \mathrm{Lin}(V, V)$ for some vector space $V$, such that:*

*(a) every element $g \in G$ is invertible, and if $g \in G$, then $g^{-1} \in G$;*

*(b) if $g, h \in G$, then the product $gh \in G$; and*

*(c) the identity map $\mathbb{1} \in G$.*

*A* ***subgroup*** *of a matrix group $G$ is a subset $G_0 \subset G$ which also satisfies properties (a)-(c).*

**Lemma 17.1.2.** *If $H$ is a Hilbert space, then the* ***group of unitary transformations***

$$U(H) = \{g \in \operatorname{Lin}(H, H) : g \text{ is unitary}\}$$

*is a matrix group.*

*Proof.* If $g, h$ are unitary, then $gh$ is unitary and so is $g^{-1} = g^*$. Finally, the identity matrix is unitary. □

Suppose we have a physical system $H$ where:

- we can leave the system unchanged, so $\mathbb{1}$ is a time evolution operator over any time range,
- we can compose time evolution operators, so if we can implement $g, h \in U(H)$ as time evolution operators, then we can implement $gh$, and
- if we can implement $g \in U(H)$, then we "run $g$ backwards" and implement $g^{-1}$.

Then the set of unitary operators we can implement forms a subgroup of $U(H)$.

Suppose we have a physical system in a lab, where we've built devices to implement certain unitaries $u \in X$, for some subset $X \subseteq U(H)$ (not necessarily a matrix group). We apply unitary $u \in X$ to our system by turning on the device corresponding to $u$, and $u^{-1}$ by running the same device backwards. By turning on and off our devices in sequence (only one device can run at a time), we can implement unitaries like $uvw$ or $uv^{-1}wuv$ for $u, v, w \in X$. What unitaries can we implement by switching on and off the unitaries in $X$? Well, the physical system we've described satisfies the list of conditions above, and hence the unitaries we can implement forms a matrix group. We can construct this matrix group as follows:

**Definition 17.1.3.** *If $X$ is a subgroup of $\operatorname{Lin}(V, V)$, such that every element of $X$ is invertible, then the* ***matrix group $\langle X \rangle$ generated by*** *$X$ is the set*

$$\bigcup_{n \geq 0} \{x_1^{\pm 1} \cdots x_n^{\pm 1} : x_1, \ldots, x_n \in X\}.$$

*The elements of $X$ are called the* ***generators*** *of $\langle X\rangle$.*

*A matrix group $G$ is* ***finitely-generated*** *if $G = \langle X\rangle$ for some finite set $X$.*

**Lemma 17.1.4.** *If $X$ is a subset of $\mathrm{Lin}(V,V)$ such that every element of $X$ is invertible, then $\langle X\rangle$ is a matrix group, and is the smallest matrix group containing $X$.*

*Proof.* The identity is contained in $\langle X\rangle$ by definition (it's the case $n = 0$ in the union). Suppose $g = x_1^{a_1}\cdots x_n^{a_n}$ and $h = y_1^{b_1}\cdots y_m^{b_m}$ are two elements of $\langle X\rangle$. Then

$$gh = x_1^{a_1}\cdots x_n^{a_n}y_1^{b_1}\cdots y_n^{b_n} \in \langle X\rangle,$$

and

$$g^{-1} = x_n^{-a_n}\cdots x_1^{-a_1} \in \langle X\rangle,$$

so $\langle X\rangle$ is a matrix group.

If $G$ is any matrix group in $\mathrm{Lin}(V,V)$ containing $X$, then we can prove by induction on $n$ that $G$ contains $x_1^{\pm 1}\cdots x_n^{\pm n}$ for all $n \geq 1$, so $G$ contains $\langle X\rangle$. □

Note that if $X \subseteq U(H)$, then since $\langle X\rangle$ is the smallest matrix group containing $X$, we must have $\langle X\rangle \subseteq U(H)$, so $\langle X\rangle$ is a subgroup of the unitary group.

**Proposition 17.1.5.** *If $X \subset \mathrm{Lin}(V,V)$ is a countable set of invertible operators, then $\langle X\rangle$ is countable (i.e. finite, or in bijection with $\mathbb{N}$).*

*Proof.* We give the proof for $X$ finite; the proof if $X$ is countable and infinite is a bit more complicated, but uses standard ideas about countable sets.

Consider the set of words

$$\mathcal{W} = \bigcup_{n\geq 1}\{x_1^{\pm 1}\cdots x_n^{\pm 1} : x_1,\dots,x_n \in X\},$$

where $x_1^{a_1}\cdots x_n^{a_n}$ for $a_1,\dots,a_n \in \{\pm 1\}$ does not denote the product of these matrices, but rather a "formal word" in the symbols $S = \{x, x^{-1} : x \in X\}$.

If $X$ is finite, then we can regard the elements of $S$ as the non-zero digits in a base $|S|+1$ number system. In this way, we get a bijection between $\mathcal{W}$ and the integers which can be expressed with no zero digits when written in base $|S|+1$. Thus $\mathcal{W}$ is countable. By mapping the word $x_1^{a_1}\cdots x_n^{a_n}$ to the product of the matrices, we get a surjection $\mathcal{W} \to \langle X\rangle$, so $\langle X\rangle$ is also countable. □

**Lemma 17.1.6.** *$U(H)$ is uncountable.*

*Proof.* $U(H)$ contains the linear transformations $e^{i\theta}\mathbb{1}$ for all $\theta \in \mathbb{R}$, and hence $[0, 2\pi)$ is in bijection with a subset of $U(H)$. Since $[0, 2\pi)$ is uncountable, $U(H)$ is uncountable. □

We don't typically expect to be able to build more than a finite number of devices in any lab. So in the above example physical system, we should think of the set of generators $X$ as being finite. This means that the set of unitaries $\langle X\rangle$ we can imagine implementing in almost any lab setting is countable. So given a finite set of generators, there are unitaries we can't implement. However, it turns out that this is a little misleading, because it doesn't matter if we can't implement a unitary exactly: it's good enough if we can approximate it. To study approximations of unitary matrices, we need to look at notions of distance between matrices.

## 17.2 The operator norm

A norm on a vector space $M_{nn}(\mathbb{F})$ or $\mathrm{Lin}(V, W)$ is called a **matrix norm**. Let's think of what norms are useful for measuring the distance between unitaries. Suppose $U$ and $V$ are two unitary operators. The unitary $V$ will be a good approximation to $U$ if $V|\psi\rangle$ is close to $U|\psi\rangle$ for all states $|\psi\rangle$. So $V$ is a good approximation to $U$ if there is some small number $\epsilon$ such that

$$\|(U - V)|\psi\rangle\| \leq \epsilon$$

for all states $|\psi\rangle$. This inspires the definition of a norm.

**Definition 17.2.1.** *If $T \in \mathrm{Lin}(H_1, H_2)$, where $H_i$ is a Hilbert space, $i = 1, 2$, then the **operator norm of** $T$ is*

$$\|T\|_{op} := \sup\{\|Tv\| : \|v\| = 1\}.$$

**Lemma 17.2.2.** *Let $H_i$, $i = 1, 2$ be Hilbert spaces. Then $\|\cdot\|_{op}$ is a norm on $\mathrm{Lin}(H_1, H_2)$. Furthermore, $\|\cdot\|_{op}$ can be calculated in a number of ways:*

$$\begin{aligned}\|T\|_{op} &= \sup\{\|Tv\| : v \in H_1, \|v\| \leq 1\}\\ &= \sup\left\{\frac{\|Tv\|}{\|v\|} : v \in H_1, v \neq 0\right\}\\ &= \inf\{c : \|Tv\| \leq c\|v\| \textit{ for all } v \in H_1\}\end{aligned}$$

*for any $T \in \mathrm{Lin}(H_1, H_2)$. Finally, $\|T\|_{op}$ is attained, meaning that there is a vector $v \in H_1$ such that $\|Tv\| = \|T\|_{op}$.*

*Proof.* To see that $\| \cdot \|_{op}$ is a norm, observe that

$$\begin{aligned}\|sT\|_{op} &= \sup\{\|sTv\| : \|v\| = 1\}\\ &= \sup\{|s|\|Tv\| : \|v\| = 1\}\\ &= |s| \sup\{\|Tv\| : \|v\| = 1\} = |s|\|T\|_{op}\end{aligned}$$

for all $s \in \mathbb{C}$ and $T \in \mathrm{Lin}(H_1, H_2)$.

Similarly,

$$\begin{aligned}\|T_1 + T_2\|_{op} &= \sup\{\|(T_1 + T_2)v\| : \|v\| = 1\}\\ &\leq \sup\{\|T_1 v\| + \|T_2 v\| : \|v\| = 1\}\\ &\leq \sup\{\|T_1 v\| : \|v\| = 1\} + \sup\{\|T_2 v\| : \|v\| = 1\} = \|T_1\|_{op} + \|T_2\|_{op}.\end{aligned}$$

Finally, if $\|T\|_{op} = 0$, this means that $\|Tv\| = 0$ for all $v$ with $\|v\| = 1$, so for any non-zero vector $v \in H_1$, we have that

$$\|Tv\| = \|v\|\|T\frac{v}{\|v\|}\| = 0,$$

meaning that $T = 0$. So $\| \cdot \|_{op}$ is a norm.

For the other reformulations of $\|\cdot\|_{op}$, we refer to an analysis class. Similarly, to see that $\|T\|_{op}$ is attained, note that the set of unit vectors in a finite-dimensional vector space is compact, and the function $v \mapsto \|Tv\|$ is continuous, so we can use the fact that the supremum of a continuous function on a compact set is always attained. □

The second way of calculating $\|T\|_{op}$ in Lemma 17.2.2 implies the useful inequality

$$\|Tv\| \leq \|T\|_{op}\|v\| \text{ for all } v \in V.$$

The third way of calculating $\|T\|_{op}$ implies that $\|T\|_{op}$ is the smallest constant with this property.

**Lemma 17.2.3.** *Let $H_i$ be a Hilbert space, and $U_i \in U(H_i)$, $i = 1, 2$. Then*

$$\|U_2 T\|_{op} = \|TU_1\|_{op} = \|T\|_{op}$$

*for all $T \in \mathrm{Lin}(V, V)$.*

*Proof.* A unitary operator preserves norm, so

$$\|U_2 T\|_{op} = \sup\{\|U_2 Tv\| : \|v\| = 1\} = \sup\{\|Tv\| : \|v\| = 1\} = \|T\|_{op}.$$

If $w \in H_1$ is a unit vector, then $w = U_1(U_1^* w)$, where $v = U_1^* w$ is a unit vector. So every vector $w \in H_1$ is a unit vector if and only if it is of the form $w = U_1 v$ for some unit vector $v$. Hence

$$\begin{aligned}\|TU_1\|_{op} &= \sup\{\|TU_1 v\| : \|v\| = 1\} = \sup\{\|Tw\| : w = U_1 v, \|v\| = 1\} \\ &= \sup\{\|Tw\| : \|w\| = 1\} = \|T\|_{op}.\end{aligned}$$

□

Elements of $U(H_i)$ are isomorphisms of $H_i$ to itself, so Lemma 17.2.3 is a special case of:

**Lemma 17.2.4.** *Let $T_i : H_i \to H_i'$ be Hilbert space isomorphisms, $i = 1, 2$. If $S \in \mathrm{Lin}(H_1, H_2)$, then*

$$\|S\|_{op} = \|T_2 S T_1^{-1}\|_{op}.$$

*Proof.* Similar to Lemma 17.2.3. □

If $\mathcal{B}_i$ be an orthonormal basis for Hilbert space $H_i$, $i = 1, 2$, and $n_i = \dim H_i$, then the coordinate maps $c_i : H_i \to \mathbb{C}^{n_i} : v \mapsto [v]_{\mathcal{B}_i}$ are Hilbert space isomorphisms, so we get that

$$\|T\|_{op} = \|c_2 T c_1^{-1}\|_{op} = \sup\{\|[T]_{\mathcal{B}_2, \mathcal{B}_1} v\| : v \in \mathbb{C}^n, \|v\| = 1\}. \tag{17.2.1}$$

for $T \in \mathrm{Lin}(H_1, H_2)$ as another special case of Lemma 17.2.4.

Recall that every matrix $M \in M_{mn}\mathbb{C}$ can be written as a product

$$M = U \Sigma V^*,$$

where $U$ and $V$ are $m \times m$ and $n \times n$ unitary matrices, and $\Sigma$ is a diagonal $m \times n$ matrix with numbers $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_\ell \geq 0$, where $\ell = \min\{m, n\}$. This decomposition is called the **singular value decomposition** of $M$. The unitary matrices $U$ and $V$ are not unique, but the **singular values** $\lambda_1, \ldots, \lambda_\ell$ are unique (when ordered in descending order). If $\Sigma$ is a diagonal $m \times n$ matrix, then $\Sigma^*$ is a diagonal $n \times m$ matrix, so

$$M^* = V \Sigma^* U^*.$$

is the singular value decomposition of $M^*$, and $M$ and $M^*$ have the same singular values. If $v_1, \ldots, v_n$ are the columns of $V$, and $u_1, \ldots, u_m$ are the rows of $M$, then

- $v_1, \ldots, v_n$ is an orthonormal basis of $\mathbb{C}^n$ such that either $Mv_i = \lambda_i u_i$ (if $1 \leq i \leq \ell$) or $Mv_i = 0$, and

- $u_1, \ldots, u_m$ is an orthonormal basis of $\mathbb{C}^m$ such that either $M^* u_i = \lambda_i v_i$ (if $1 \le i \le \ell$) or $M^* u_i = 0$.

The vectors $v_1, \ldots, v_n$ and $u_1, \ldots, u_m$ are called **right and left singular vectors** of $M$; they are not unique.

**Proposition 17.2.5.** *Let $\mathcal{B}_i$ be an orthonormal basis for Hilbert space $H_i$, $i = 1, 2$. If $T \in \operatorname{Lin}(H_1, H_2)$, then $\|T\|_{op}$ is the largest singular value of $[T]_{\mathcal{B}_2, \mathcal{B}_1}$.*

*Furthermore, if $v \in H_1$ is a vector such that $[v]_{\mathcal{B}_1}$ is a right singular vector for the largest singular value of $[T]_{\mathcal{B}_2, \mathcal{B}_1}$, then $\|Tv\| = \|T\|_{op}$.*

*Proof.* Let $M = [T]_{\mathcal{B}_2, \mathcal{B}_1}$, and let and let $M = U \Sigma V^*$ be the SVD of $M$. Then by Proposition 5.2.3 there are unitary operators $\hat{U} \in U(H_2)$ and $\hat{V} \in U(H_1)$ such that $[\hat{U}]_{\mathcal{B}_2, \mathcal{B}_2} = U$ and $[\hat{V}]_{\mathcal{B}_1, \mathcal{B}_1} = V$. Let $T' = \hat{U}^* T \hat{V}$, so that

$$[T']_{\mathcal{B}_2, \mathcal{B}_1} = [\hat{U}^* T \hat{V}]_{\mathcal{B}_2, \mathcal{B}_1} = [\hat{U}^*]_{\mathcal{B}_2, \mathcal{B}_2} [T]_{\mathcal{B}_2, \mathcal{B}_1} [\hat{V}]_{\mathcal{B}_1, \mathcal{B}_1} = U^* M V = \Sigma.$$

By Lemma 17.2.3, $\|T\|_{op} = \|T'\|_{op}$, so we just have to calculate this latter norm.

Suppose $\dim H_2 = m$ and $\dim H_1 = n$, so $\Sigma$ is an $m \times n$ diagonal matrix. Let $e_1, \ldots, e_m$ denote the standard basis vectors of $\mathbb{C}^m$, and let $\lambda_1 \ge \ldots \ge \lambda_l$ be the non-zero diagonal entries of $\Sigma$. If $v \in \mathbb{C}^n$, then

$$\Sigma v = \sum \lambda_i v_i e_i,$$

so

$$\|\Sigma v\|^2 = \sum_{i=1}^{l} |\lambda_i v_i|^2 = \sum_{i=1}^{l} \lambda_i^2 |v_i|^2 \le \lambda_1^2 \sum_{i=1}^{l} \le \lambda_1^2 \sum_{i=1}^{n} |v_i|^2 = \lambda_1^2 \|v\|^2.$$

So if $\|v\| = 1$, then $\|\Sigma v\| \le \lambda_1 v$. Also, $\|\Sigma e_1\| = \|\lambda_1 e_1\| = \lambda_1$, so by Equation (17.2.1),

$$\|T'\|_{op} = \sup\{\|\Sigma v\| : v \in \mathbb{C}^n, \|v\| = 1\} = \lambda_1.$$

Hence $\|T\|_{op}$ is the largest singular value of $M$.

Finally, if $v \in H_1$ is a vector such that $[v]_{\mathcal{B}_1}$ is a singular vector for the largest singular value of $M$, then $M[v]_{\mathcal{B}_1} = \lambda_1 u_1$ for some left singular vector $u_1$ of $M$. In particular, $u_1$ is a unit vector, so

$$\|Tv\| = \|M[v]_{\mathcal{B}_1}\| = \|\lambda_1 u_1\| = \lambda_1.$$

□

If an $n \times n$ matrix $M$ is unitarily diagonalizable, then there is a unitary matrix $U$ such that $M = UDU^*$, where $D$ is a diagonal matrix with the eigenvalues of $M$ on the diagonal. (In terms of Theorem 12.1.2, if $T$ is the linear transformation corresponding to multiplicaton by $M$, and $\mathcal{B}$ is the orthonormal basis such that $[T]_{\mathcal{B},\mathcal{B}} = D$ is diagonal, then $U$ is the change of basis from $\mathcal{B}$ to the standard basis.) If the eigenvalues of $M$ are real and non-negative (or in other words, if $M$ is positive semidefinite), then, up to reordering of the diagonal entries, $UDU^*$ is a singular value decomposition for $M$, and hence the eigenvalues of $M$ are the same as the singular values of $M$. In particular, for a positive semidefinite operator $H \to H$, the operator norm is the largest eigenvalue.

We can go a step further:

**Proposition 17.2.6.** *If $T : H \to H$ is unitarily diagonalizable with eigenvalues $\lambda_1, \ldots, \lambda_n$, then*

$$\|T\|_{op} = \max_{1 \le i \le n} |\lambda_i|.$$

*Proof.* For each $1 \le j \le n$, write $\lambda_j = r_j e^{i\theta_j}$ for some non-negative real numbers $r_j$, $\theta_j$. We may assume that $\lambda_1, \ldots, \lambda_n$ are ordered so that $r_1 \ge r_2 \ge \ldots \ge r_n$. Choose an orthonormal basis $\mathcal{B}$ for $H$, and let $M = [T]_{\mathcal{B},\mathcal{B}}$. Then there is a unitary matrix $U$ such that $M = UDU^*$, where $D$ is the diagonal matrix with $D_{ii} = \lambda_i$. Let $V$ and $\Sigma$ be the diagonal matrices with $V_{jj} = e^{i\theta_j}$ $\Sigma_{jj} = r_j$. Then $V$ is unitary, so $UV$ is also unitary, and hence $M = UV\Sigma U^*$ is a singular value decomposition of $M$. Since $|\lambda_i| = r_i$, the proposition follows. □

For any $M \in M_{mn}\mathbb{C}$, the matrices $M^*M$ and $MM^*$ are positive semidefinite. If $M$ has singular value decomposition $M = U\Sigma V^*$, then

$$M^*M = V\Sigma^*U^*U\Sigma V^* = V\Sigma^*\Sigma V^* \text{ and } MM^* = U\Sigma V^*V\Sigma^*U^* = U\Sigma\Sigma^*U^*. \tag{17.2.2}$$

If $\Sigma$ is diagonal with non-zero diagonal entries $\lambda_1, \ldots, \lambda_l$, then $\Sigma^*\Sigma$ and $\Sigma\Sigma^*$ are both diagonal with non-zero diagonal entries $\lambda_1^2, \ldots, \lambda_l^2$. Hence the squares $\lambda_1^2, \ldots, \lambda_l^2$ are the non-zero eigenvalues of $M^*M$ and $MM^*$. Since $\Sigma^*\Sigma$ and $\Sigma\Sigma^*$ can have different dimensions, the number of zero diagonal entries can differ, as the next example shows.

**Example 17.2.7.** *If*

$$\Sigma = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$$

*then*

$$\Sigma^*\Sigma = \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

*and*

$$\Sigma^*\Sigma = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix}$$

To summarize, the non-zero singular values of $M$ are the square roots of the non-zero eigenvalues of $M^*M$ (or equivalently, $MM^*$). Hence

**Corollary 17.2.8.** *If $T \in \mathrm{Lin}(H_1, H_2)$, where $H_1, H_2$ are Hilbert spaces, then*

$$\|T\|_{op} = \|T^*\|_{op} = \sqrt{\|T^*T\|_{op}} = \sqrt{\|TT^*\|_{op}}.$$

*Proof.* Follows from Propositions 17.2.5 and 17.2.6. □

## 17.3 Dense finitely generated subgroups

Now that we have the operator norm, we can properly formulate our "quantum control" question. Recall the definition of **closure** in a metric space $X$: a point $x$ is in the closure $\overline{S}$ of a set $S$ if for every $\epsilon > 0$, there is $y \in S$ such that $d(x, y) < \epsilon$. The closure of $S$ is the smallest closed set containing $S$; in particular, if $C$ is a closed subset of $X$ containing $S$, then $\overline{S} \subseteq C$. A set $S$ is dense in $C$ if $\overline{S} = C$.

For a normed vector space $(V, \|\cdot\|)$, the metric is given by $d(v, w) = \|v - w\|$. If $V$ is finite-dimensional, then all norms on $V$ are equivalent, so the topology[1] on $V$ doesn't depend on the choice of norm. The topology also doesn't depend on whether $V$ is regarded as a complex or real vector space. Also, all real isomorphic vector spaces have the same topology.

**Example 17.3.1.** *$\mathbb{C}^1$ and $\mathbb{R}^2$ are isomorphic as real vector spaces, and hence have the same topology. The function*

$$\mathbb{R}^2 \to \mathbb{R} : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto x^2y^3$$

*is continuous, since it is a polynomial function.*

[1] A topology on a set $X$ is a collection of **open sets** $\mathcal{O}$ satisfying certain axioms. The topology contains all the information needed to determine closed sets, closures, and limits.

*Similarly, the function*

$$\mathbb{C}^1 \to \mathbb{R} : x \mapsto x\overline{x} = (\operatorname{Re} x)^2 + (\operatorname{Im} x)^2$$

*is continuous, since it is a polynomial function of the real and imaginary parts of $x$.*

Any fact about the topology on $\mathbb{R}^n$ applies to every (finite-dimensional) normed vector space $V$. For instance, a subset of $V$ is compact if and only if it is closed and bounded.

When working with unitary operators, the underlying metric space is $\operatorname{Lin}(V, V)$ with the operator norm: $d(S, T) = \|S - T\|_{op}$. Since $\operatorname{Lin}(V, V)$ is a finite-dimensional vector space, the topology on $\operatorname{Lin}(V, V)$ is the same as the usual topology on $\mathbb{R}^{n^2}$, where $n = \dim V$.

**Lemma 17.3.2.** *$U(H)$ is a closed and bounded subset of $\operatorname{Lin}(H, H)$ in the operator norm.*

*Proof.* If $U$ is unitary, then $\|U\|_{op} \leq 1$, so $U(H)$ is bounded.

To prove $U(H)$ is closed, note that the function

$$f : \operatorname{Lin}(H, H) \to \operatorname{Lin}(H, H) : T \mapsto TT^*$$

is continuous (after all, if we identify $\operatorname{Lin}(H, H)$ with a space of matrices, then the function $f$ is a polynomial function of the real and imaginary parts of the matrix entries).

The set $U(H) = f^{-1}(\{\mathbb{1}\})$, and the singleton $\{\mathbb{1}\}$ is a closed set, so $U(H)$ is closed. □

Suppose $G$ is a subgroup of $U(H)$. Specializing the definition of closure to matrix groups, we see that $g \in U(H)$ is in the closure of $G$ if and only if, for all $\epsilon > 0$, there is an $h \in U(H)$ such that $\|g - h\|_{op} < \epsilon$. In other words, the closure $\overline{G}$ is the set of unitaries which can be approximated by elements of $G$. Hence, if we can implement all elements of $G$, then in a sense, we can also implement all elements of $\overline{G}$.

We showed in the first section that for any Hilbert space $H$, there is no finitely generated matrix group $G$ such that $G = U(H)$. But is it possible to have $\overline{G} = U(H)$ for some finitely-generated matrix group $G$? If so, it would mean that there's a finite set of generators $X$ such we can (approximately) implement all unitaries using just the elements of $X$. We'll answer this question affirmatively in the next chapter.

# Chapter 18

# Quantum circuits and universality

In the previous chapter, we discussed the following unitary quantum control question: is there a finite number of devices we can build that would allow us to implement (approximately) all unitaries on a Hilbert space $H$. In this section, we'll prove the following theorem, which shows that the answer to the question from a mathematical point of view is "yes".

**Theorem 18.0.1.** *If $H$ is a Hilbert space, then there is a finite set $X \subseteq U(H)$ such that $\overline{\langle X \rangle} = U(H)$.*

The set $\overline{\langle X \rangle}$ is the closure of $\langle X \rangle$, so this theorem states that there is a finite set $X$ such that every unitary can be approximated by products of the elements of $X$ and their inverses. We won't prove Theorem 18.0.1 in full generality; instead we'll concentrate on the case that $\dim H = 2^n$ for some $n \geq 1$.

Before we proceed to the proof, note that Theorem 18.0.1 provides a very limited answer to the question we posed. For instance, it says nothing at all about what the elements of $X$ are, or how we might implement them experimentally. Theorem 18.0.1 is also lacking from an information theory point of view. If $H = \mathbb{C}\{0, 1\}$ is a qubit register, then Theorem 18.0.1 states that there is a finite set of unitaries that we can use to approximate all elements of $U(H)$. But what if we want to approximate unitaries on the $n$-qubit register $H^{\otimes n} = \mathbb{C}\{0, 1\}^n$? The theorem guarantees that there will be a finite set of elements of $U(H^{\otimes n})$ that we can use to approximate all unitaries, but how does this set change with $n$? Do we have to consider more and more complicated unitaries for the generator set $X$, or can we build all unitaries in $U(H^{\otimes n})$ out of unitaries which act on just a few qubits?

In a mathematics course, we can't hope to say how we'll implement generators in $X$ experimentally. But we can answer the other questions in the last paragraph. So after we prove Theorem 18.0.1, we'll prove a stronger version of the theorem.

## 18.1 The one- and two-dimensional case

To prove Theorem 18.0.1, we need to think of how we can approximate infinitely many elements of $U(H)$ starting from only a finite number of unitaries. To see how we can do this, consider the case $H = \mathbb{C}$. The states in $H$ are the complex numbers $z$ of absolute value $|z| = 1$, and hence are all equivalent to 1 up to global phase. This means that, as a physical system, $H$ has only one state. It's not possible for such a system to change over time, and indeed the unitary group $U(H)$ consists of the multiplication operators by complex numbers $z$ of absolute value $|z| = 1$. These unitaries multiply states by a global phase, and hence don't really change the state. However, $U(H)$ is still infinite, and so this is a good test case for Theorem 18.0.1.

For the case $H = \mathbb{C}$, it turns out that $X$ only needs to contain one element. To understand why that is, observe that the elements of $U(H)$ can written uniquely as

$$e^{2\pi i\theta}$$

for $\theta \in [0, 1)$. If $z = e^{2\pi i\alpha}$ then

$$\langle z\rangle = \langle z^k : k \in \mathbb{Z}\rangle = \{e^{2\pi ik\alpha} : k \in \mathbb{Z}\}.$$

If $r$ is a real number, then the modulus of $r$ mod 1 is $r - \lfloor r\rfloor$, i.e. the part after the decimal in the decimal expansion of $r$. The complex number $e^{2\pi ik\alpha}$ depends only on this modulus of $k\alpha$. To approximate numbers $e^{2\pi i\theta}$, we'd like to pick $\alpha$ so that we can get the modulus $k\alpha - \lfloor k\alpha\rfloor$ arbitrarily close to any number $\theta$. This is possible if we pick $\alpha$ to be an irrational number.

**Lemma 18.1.1.** *Let $\alpha \in \mathbb{R}$ be irrational. Then the set*

$$\{k\alpha - \lfloor k\alpha\rfloor : k \in \mathbb{N}\}$$

*is dense in* $[0, 1]$.

*Proof.* The key fact is that the values $k\alpha - \lfloor k\alpha\rfloor$ are distinct for all $k \in \mathbb{N}$. Indeed, if

$$k_1\alpha - \lfloor k_1\alpha\rfloor = k_2\alpha - \lfloor k_2\alpha\rfloor$$

for some $k_1 \neq k_2$, then

$$\alpha = \frac{\lfloor k_2\alpha \rfloor - \lfloor k_1\alpha \rfloor}{k_2 - k_1},$$

contradicting the irrationality of $\alpha$.

Suppose $N \in \mathbb{N}$, and divide the interval $[0,1)$ into the subintervals $[j/N, (j+1)/N)$ for $j = 0, \ldots, N-1$. By the pigeon-hole principle, there must be $k_1 \neq k_2 \in \mathbb{N}$ such that $k_1\alpha - \lfloor k_1\alpha \rfloor$ and $k_2\alpha - \lfloor k_2\alpha \rfloor$ belong to the same interval $[j/N, (j+1)/N)$. Suppose without loss of generality that

$$k_1\alpha - \lfloor k_1\alpha \rfloor < k_2\alpha - \lfloor k_2\alpha \rfloor,$$

and let $M = \lfloor k_2\alpha \rfloor - \lfloor k_1\alpha \rfloor$. Then

$$0 < (k_2 - k_1)\alpha - M < \frac{1}{N},$$

and for each $j = 0, \ldots, N-1$, there is $N_j$ such that

$$\frac{j}{N} \leq N_j \left[(k_2 - k_1)\alpha - M\right] < \frac{j+1}{N}.$$

Let $k = N_j(k_2 - k_1)$. Because $N_jM < k\alpha < N_jM + 1$, and $N_jM \in \mathbb{N}$, we see that $\lfloor N_j(k_2 - k_1)\alpha \rfloor = N_jM$, and hence

$$\frac{j}{N} \leq k\alpha - \lfloor k\alpha \rfloor < \frac{j+1}{N}.$$

Thus if we divide $[0,1]$ into subintervals of size $1/N$, we can find elements of the form $k\alpha - \lfloor k\alpha \rfloor$ in every subinterval, so these elements are dense in $[0,1]$. □

**Corollary 18.1.2.** *Theorem 18.0.1 is true if $H = \mathbb{C}$.*

*Proof.* Choose $\alpha \in \mathbb{R}$ to be irrational, and let $X = \{e^{2\pi i\alpha}\}$. If $\theta \in [0,1)$, then choose a sequence $k_1, k_2, \ldots$ in $\mathbb{N}$ such that

$$\lim_{j\to+\infty} k_j\alpha - \lfloor k_j\alpha \rfloor = \theta.$$

Then

$$\lim_{j\to+\infty} e^{2\pi i k_j\alpha} = \lim_{j\to+\infty} e^{2\pi i(k_j\alpha - \lfloor k_j\alpha \rfloor)} = e^{2\pi i\theta}.$$

So

$$\overline{\langle X\rangle} = \overline{\{e^{2\pi i k\alpha} : k \in \mathbb{Z}\}} = U(H).$$

□

Although this proves Theorem 18.0.1 when $\dim H = 1$, it is not obvious that this same idea can be used in higher dimensions. To see that it can, recall that a **rotation matrix** is a matrix of the form

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

for some $\theta \in \mathbb{R}$. As a linear transformation, $R_\theta$ is rotation by $\theta$, and hence $R_\theta$ satisfies the following properties:

(1) $R_\theta$ is unitary,

(2) $R_\theta R_\psi = R_{\theta+\psi}$, and in particular,

(3) $R_\theta^k = R_{k\theta}$.

We get the following decomposition for $2 \times 2$ unitary matrices:

**Lemma 18.1.3.** *If $U$ is a $2\times2$ unitary matrix, then there are $\theta, \psi_1, \psi_2, \psi_3, \psi_4 \in \mathbb{R}$ such that*

$$U = \begin{pmatrix} e^{i\psi_1} & 0 \\ 0 & e^{i\psi_2} \end{pmatrix} \cdot R_\theta \cdot \begin{pmatrix} e^{i\psi_3} & 0 \\ 0 & e^{i\psi_4} \end{pmatrix}.$$

*Proof.* Since $U$ is unitary, if the first column of $U$ is $u_1 = ae_1 + be_2$, then the second column $u_2$ must be in $\operatorname{span}\{u_1\}^\perp = \operatorname{span}\{-\bar{b}e_1 + ae_2\}$. Thus we must have $u_2 = e^{i\gamma}(-\bar{b}e_1 + ae_2)$. Then we have

$$U = \begin{pmatrix} a & -\bar{b} \\ b & a \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & e^{i\gamma} \end{pmatrix},$$

where $|a|^2 + |b|^2 = 1$. From this last fact, we can write $a = e^{i\alpha}\cos\theta$ and $b = e^{i\beta}\sin\theta$. Thus we have

$$\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(\beta-\alpha)} \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\beta} \end{pmatrix},$$

so we can take $\psi_1 = 0$, $\psi_2 = \beta - \alpha$, $\psi_3 = \alpha$, and $\psi_4 = \gamma - \beta$. □

**Corollary 18.1.4.** *Theorem 18.0.1 is true if $H = \mathbb{C}^2$.*

*Proof.* □

## 18.2 The CS decomposition

To prove Theorem 18.0.1, we can use a remarkable generalization of Lemma 18.1.3 called the **CS decomposition** of a unitary matrix.

**Lemma 18.2.1.** *Let $M$ be an $n \times n$ matrix with orthogonal columns. Then there is a unitary matrix $U$ and a diagonal matrix $D$ with real non-negative entries such that $M = UD$.*

*Proof.* Let $v_1, \dots, v_n$ be the columns of $M$, and let

$$S = \left\{ \frac{v_i}{\|v_i\|} : 1 \leq i \leq n, v_i \neq 0 \right\}.$$

Since the columns of $M$ are orthogonal, $S$ is an orthonormal set of vectors, and hence is linearly independent. Thus we can extend $S$ to an orthonormal basis $\{u_1, \dots, u_n\}$ of $\mathbb{C}^n$, where we choose the order so that $u_i = v_i/\|v_i\|$ for all $1 \leq i \leq n$ with $v_i \neq 0$. Let $U$ be the unitary matrix with columns $u_1, \dots, u_n$, and let $D$ be the diagonal matrix with diagonal entries $D_{ii} = \|v_i\|$. Then $M = UD$. □

**Proposition 18.2.2** (CS decomposition)**.** *Suppose $M$ is a $2n \times 2n$ unitary matrix. Then there are $n \times n$ unitary matrices $U_1$, $U_2$, $V_1$, $V_2$, and diagonal real matrices $C, S$ with non-negative entries such that*

$$M = \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix} \begin{pmatrix} C & -S \\ S & C \end{pmatrix} \begin{pmatrix} V_1^* & 0 \\ 0 & V_2^* \end{pmatrix},$$

*and $C^2 + S^2 = \mathbb{1}$.*

If we decompose $M$ into $n \times n$ blocks

$$M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix},$$

then $U_1 C V_1^*$ is the SVD decomposition of $M_{11}$, $U_1(-S)V_2^*$ is the SVD decomposition of $M_{12}$, and so on. What this theorem says is that we can take the SVD decompositions of $M_{11}$, $M_{12}$, $M_{21}$, and $M_{22}$ with only four different unitaries.

*Proof.* As above, write

$$M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$$

for $n \times n$ matrices $M_{11}$, $M_{12}$, $M_{21}$, and $M_{22}$. Let $M_{11} = U_1 C V_1^*$ be the SVD decomposition of $M_{11}$, so $C$ is a real diagonal matrix with non-negative real numbers in decreasing order on the diagonal. Consider the matrix

$$Q = \begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{pmatrix} = \begin{pmatrix} U_1^* & 0 \\ 0 & \mathbb{1} \end{pmatrix} M \begin{pmatrix} V_1 & 0 \\ 0 & \mathbb{1} \end{pmatrix} = \begin{pmatrix} C & U_1^* M_{12} \\ M_{21} V_1 & M_{22} \end{pmatrix}.$$

Now $Q$ is unitary, $Q^*Q = \mathbb{1}$. In particular, if we look at the top left block of the product $Q^*Q$, we see that

$$Q_{11}^* Q_{11} + Q_{21}^* Q_{21} = \mathbb{1}.$$

Since $Q_{11} = C = Q_{11}^*$, we see that $Q_{21}^* Q_{21} = \mathbb{1} - C^2$. Since this last matrix is diagonal, the columns of $Q_{21}$ are orthogonal, and we can write $Q_{21} = U_2 S$ for some unitary matrix $U_2$ and diagonal matrix $S$ with real non-negative entries. Similarly, from the product $QQ^* = \mathbb{1}$, we see that $Q_{12} Q_{12}^* = \mathbb{1} - C^2$, so the columns of $Q_{12}^* = V_2 S'$ for some unitary $V_2$ and diagonal matrix $S'$ with real non-negative entries. It follows that

$$Q = \begin{pmatrix} C & S' V_2^* \\ U_2 S & M_{22} \end{pmatrix} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & U_2 \end{pmatrix} \begin{pmatrix} C & S' \\ S & U_2^* M_{22} V_2 \end{pmatrix} \begin{pmatrix} \mathbb{1} & 0 \\ 0 & V_2^* \end{pmatrix}.$$

Finally, let

$$Q' = \begin{pmatrix} C & S' \\ S & U_2^* M_{22} V_2 \end{pmatrix}.$$

Now $Q'$ is unitary, and using the fact that the columns of $Q'$ are unit vectors, we see that $C_{ii}^2 + S_{ii}^2 = 1$ for all $1 \leq i \leq n$. Since the rows of $Q'$ are also unit vectors, we get that $C_{ii}^2 + (S_{ii}')^2 = 1$ for all $1 \leq i \leq n$, so $C^2 + S^2 = \mathbb{1}$. Since the entries of $S$ and $S'$ are non-negative, we have that $S_{ii} = \sqrt{1 - C_{ii}^2} = S_{ii}'$ for all $1 \leq i \leq n$, so $S = S'$.

It remains to analyze $T := U_2^* M_{22} V_2$. For this, recall that the diagonal entries of $C_{ii}$ are in decreasing order. Since $Q'$ is unitary, no entry is larger than 1. Suppose $C_{ii} = 1$ for $1 \leq i \leq a$, and $C_{ii} = 0$ for $i > b$, where $a \geq 0$ and $b \leq n$. Since $S^2 = \mathbb{1} - C^2$, we must have $S_{ii} = 0$ for all $1 \leq i \leq a$, and $S_{ii} = 1$ for all $i > b$. Since $(Q')^* Q' = \mathbb{1}$, we have that $CS + ST = 0$. But since $C$ and $S$ are diagonal, $CS = SC$, so we get that

$$S(C + T) = 0.$$

Looking at the $ij$th entry of $S(C + T)$, we see that $S_{ii}(C_{ij} + T_{ij}) = 0$ for all $1 \leq i, j \leq n$. Since $S_{ii} > 0$ for all $a \leq i \leq n$, we see that $T_{ij} = -C_{ij}$ for all $a < i \leq n$ and $1 \leq j \leq n$. Similarly from the fact that $Q'(Q')^* = \mathbb{1}$, we get that $(C+T)S = SC+TS = 0$, so $T_{ij} = -C_{ij}$ for all $a < j \leq n$ and $1 \leq i \leq n$. So $T_{ij} = -C_{ij}$ for all pairs $(i,j)$ except possibly when $1 \leq i,j \leq a$. Thus

$$T = \begin{pmatrix} T' & 0 & 0 \\ 0 & -C' & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

where $T'$ is an $a \times a$ matrix, and $C'$ is the $(b-a) \times (b-a)$ matrix with $C'_{ii} = C_{i+a,i+a}$. For comparison, with the same block decomposition,

$$C = \begin{pmatrix} \mathbb{1} & 0 & 0 \\ 0 & C' & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & 0 & 0 \\ 0 & S' & 0 \\ 0 & 0 & \mathbb{1} \end{pmatrix},$$

where $(C')^2 + (S')^2 = \mathbb{1}$. Using the fact that $(Q')^*Q' = \mathbb{1}$ one more time, we get that $S^2 + T^*T = \mathbb{1}$. Using the block decomposition, this implies that $(T')^*T' = \mathbb{1}$, so $T'$ is unitary. We let

$$U_2' = U_2 \begin{pmatrix} -T' & 0 \\ 0 & \mathbb{1} \end{pmatrix}.$$

Note that $U_2'S = U_2S$ and $U_2'(-C) = U_2T$. Thus we have

$$\begin{aligned} M &= \begin{pmatrix} U_1 & 0 \\ 0 & \mathbb{1} \end{pmatrix} Q \begin{pmatrix} V_1^* & 0 \\ 0 & \mathbb{1} \end{pmatrix} = \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix} \begin{pmatrix} C & S \\ S & T \end{pmatrix} \begin{pmatrix} V_1^* & 0 \\ 0 & V_2^* \end{pmatrix} \\ &= \begin{pmatrix} U_1 & 0 \\ 0 & U_2' \end{pmatrix} \begin{pmatrix} C & S \\ S & -C \end{pmatrix} \begin{pmatrix} V_1^* & 0 \\ 0 & V_2^* \end{pmatrix} = \begin{pmatrix} U_1 & 0 \\ 0 & U_2' \end{pmatrix} \begin{pmatrix} C & -S \\ S & C \end{pmatrix} \begin{pmatrix} V_1^* & 0 \\ 0 & -V_2^* \end{pmatrix}. \end{aligned}$$

Since $(-V_2)^* = -V_2^*$ is unitary, this last factorization gives us the desired CS decomposition. □

Using the CS decomposition, we can prove Theorem 18.0.1 when $\dim H = 2^n$. Let $\pi \in S_n$ be a permutation of $\{1, \ldots, n\}$. The permutation matrix of $\pi$ is the matrix $P^\pi$ with $P^\pi_{ij} = \delta_{i\pi(j)}$ for all

**Lemma 18.2.3.** *If $\pi, \sigma$ are permutations of $\{1, \ldots, n\}$, then*

$$P_\pi P_\sigma = P_{\pi\sigma}.$$

*Also, $P^\pi$ is unitary and $(P^\pi)^* = P^{\pi^{-1}}$.*

*Proof.*

$$(P^\pi P^\sigma)_{ij} = \sum_k P^\pi_{ik} P^\sigma_{kj} = \delta_{i\pi(\sigma(k))}.$$

Also, $P^\pi$ has exactly one 1 in every row, and all other entries are non-zero, so $P^\pi$ is unitary. If $e$ is the identity permutation, $P^e = \mathbb{1}$, and $P^\pi P^{\pi^{-1}} = P^e = \mathbb{1}$, so $P^{\pi^{-1}}$ is the inverse of $P^\pi$. □

**Lemma 18.2.4.** *If $\pi \in S_n$, then*

$$(P_\pi M P_\sigma)_{ij} = M_{\pi^{-1}(i)\sigma(j)}.$$

*Proof.* Exercise. □

**Corollary 18.2.5.** *Theorem 18.0.1 is true if* $\dim H = 2^n$ *for some* $n \geq 1$.

*Proof.* The isomorphism $H \cong \mathbb{C}^{2^n}$ gives a bijection between $\mathcal{U}(H)$ and $\mathcal{U}(\mathbb{C}^{2^n})$ which preserves operator norms, so we can assume that $H = \mathbb{C}^{2^n}$.

Suppose Theorem 18.0.1 is true for $H' = \mathbb{C}^{2^{n-1}}$, and let $X'$ be a finite subset of $\mathcal{U}(H')$ such that

$$\overline{\langle X' \rangle} = \mathcal{U}(H').$$

Let

$$X = \left\{ \begin{pmatrix} A & 0 \\ 0 & \mathbb{1} \end{pmatrix} : A \in X' \right\} \cup \left\{ \begin{pmatrix} \mathbb{1} & 0 \\ 0 & A \end{pmatrix} : A \in X' \right\} \cup \{P^\pi\},$$

where $\pi$ is the permutation of $\{1, \ldots, 2n\}$ such that $\pi(2i) = n + i$ and $\pi(2i - 1) = i$ for all $1 \leq i \leq n$. Observe that if $A, B \in \langle X' \rangle$, then

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in \langle X \rangle,$$

since if $A = A_1^{a_1} \cdots A_k^{a_k}$ for $A_1, \ldots, A_k \in X'$ and $a_1, \ldots, a_k \in \{\pm 1\}$ and $B = B_1^{b_1} \cdots B_\ell^{b_\ell}$ for $B_1, \ldots, B_\ell \in X'$ and $b_1, \ldots, b_\ell \in \{\pm 1\}$, then

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ 0 & \mathbb{1} \end{pmatrix}^{a_1} \cdots \begin{pmatrix} A_k & 0 \\ 0 & \mathbb{1} \end{pmatrix}^{a_k} \begin{pmatrix} \mathbb{1} & 0 \\ 0 & B_1 \end{pmatrix}^{b_1} \cdots \begin{pmatrix} \mathbb{1} & 0 \\ 0 & B_\ell \end{pmatrix}^{b_\ell}.$$

Suppose $U \in \mathcal{U}(H)$, and let

$$U = \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix} \begin{pmatrix} C & -S \\ S & C \end{pmatrix} \begin{pmatrix} V_1^* & 0 \\ 0 & V_2^* \end{pmatrix}$$

be the CS decomposition of $U$. For each $i = 1, 2$, choose sequences of unitaries $(U_{ij})_{j=1}^\infty$ and $(V_{ij})_{j=1}^\infty$ in $\langle X' \rangle$ such that $U_{ij} \to U_i$ and $V_{ij} \to V_i$ as $j \to +\infty$. Let

$$A_j = \begin{pmatrix} U_{1j} & 0 \\ 0 & U_{2j} \end{pmatrix} \text{ and } B_j = \begin{pmatrix} V_{1j} & 0 \\ 0 & V_{2j} \end{pmatrix}.$$

Then

$$A_j \to \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix} \text{ and } B_j^* \to \begin{pmatrix} V_1^* & 0 \\ 0 & V_2^* \end{pmatrix}$$

as $j \to +\infty$.

Now let's look at the matrix

$$\begin{pmatrix} C & -S \\ S & C \end{pmatrix}.$$

Because $C^2 + S^2 = \mathbb{1}$, and the entries of $C$ and $S$ are real, there are angles $\theta_1, \ldots, \theta_n \in \mathbb{R}$ such that

$$\begin{pmatrix} C & -S \\ S & C \end{pmatrix} = \begin{pmatrix} \cos\theta_1 & 0 & \ldots & 0 & -\sin\theta_1 & 0 & \ldots & 0 \\ 0 & \cos\theta_2 & & 0 & 0 & -\sin\theta_2 & & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & \ldots & \cos\theta_n & 0 & 0 & \ldots & -\sin\theta_n \\ \sin\theta_1 & 0 & \ldots & 0 & \cos\theta_1 & 0 & \ldots & 0 \\ 0 & \sin\theta_2 & & 0 & 0 & \cos\theta_2 & & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & \ldots & \sin\theta_n & 0 & 0 & \ldots & \cos\theta_n \end{pmatrix}$$

So using Lemma 18.2.4,

$$(P^\pi)^* \begin{pmatrix} C & -S \\ S & C \end{pmatrix} P^\pi = \begin{pmatrix} R_{\theta_1} & 0 & \ldots & 0 \\ 0 & R_{\theta_2} & & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \ldots & R_{\theta_n} \end{pmatrix}.$$

Choose sequences $(X_i)_{i=1}^{+\infty}$ and $(Y_i)_{i=1}^{+\infty}$ in $\langle X' \rangle$ such that

$$X_i \to \begin{pmatrix} R_{\theta_1} & \ldots & 0 \\ 0 & \ddots & 0 \\ 0 & \ldots & R_{\theta_{n/2}} \end{pmatrix} \text{ and } Y_i \to \begin{pmatrix} R_{\theta_{n/2+1}} & \ldots & 0 \\ 0 & \ddots & 0 \\ 0 & \ldots & R_{\theta_n} \end{pmatrix}.$$

Let

$$Z_i := \begin{pmatrix} X_i & 0 \\ 0 & Y_i \end{pmatrix},$$

so

$$Z_i \to \begin{pmatrix} R_{\theta_1} & 0 & \ldots & 0 \\ 0 & R_{\theta_2} & & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \ldots & R_{\theta_n} \end{pmatrix}$$

as $i \to +\infty$.

$$(P^\pi)^* Z_i P^\pi \to \begin{pmatrix} C & -S \\ S & C \end{pmatrix}$$

as $i \to +\infty$.

Now $A_j$, $B_j$, $Z_j$, and $P^\pi$ belong to $X$. So $A_j(P^\pi)^* Z_j P^\pi B_j^* \in \langle X \rangle$, and

$$A_j(P^\pi)^* Z_j P^\pi B_j^* \to \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix} \begin{pmatrix} C & -S \\ S & C \end{pmatrix} \begin{pmatrix} V_1^* & 0 \\ 0 & V_2^* \end{pmatrix} = U$$

as $j \to +\infty$. So $U \in \overline{\langle X \rangle}$. We conclude that $\overline{\langle X \rangle} = \mathcal{U}(H)$. □

To evaluate the limits in this proof, we use the fact that, for sequences of matrices $(U_j)_{j=1}^{+\infty}$, $(V_j)_{j=1}^{+\infty}$, we have

$$\lim_{j \to +\infty} U_j V_j = \left( \lim_{j \to +\infty} U_j \right) \left( \lim_{j \to +\infty} V_j \right),$$

$$\lim_{j \to +\infty} U_j^* = \left( \lim_{j \to +\infty} U_j \right)^*, \text{ and}$$

$$\lim_{j \to +\infty} \begin{pmatrix} U_j & 0 \\ 0 & V_j \end{pmatrix} = \begin{pmatrix} \lim_{j \to +\infty} U_j & 0 \\ 0 & \lim_{j \to +\infty} V_j \end{pmatrix},$$

assuming all the limits exist. These identities are true because every matrix norm gives the same topology, so we use the same rule for limits in $M_{nn}\mathbb{F}$ with respect to the operator norm as we do for limits in $\mathbb{F}^{n^2}$. Thus we can take limits coordinate-wise.

However, for some applications, this argument is not sufficient. For instance, suppose that we have a procedure for approximating unitary matrices $U_1$ and $U_2$ using elements of a subgroup $G$. This means that for any given $i = 1, 2$, and $\epsilon > 0$, we can supply an element $V \in G$ with $\|U_i - V\|_{op} < \epsilon$. Now suppose we want to approximate $U_1 U_2$ to within $\epsilon$. We know that we can get elements of $G$ arbitrarily close to $U_1 U_2$ by picking $V_1$ and $V_2$ close to $U_1$ and $U_2$, and taking the product $V_1 V_2$. But how close do $V_1$ and $V_2$ need to be to $U_1$ and $U_2$ so that $\|U_1 U_2 - V_1 V_2\| < \epsilon$? This is answered by the next lemma:

**Lemma 18.2.6.** *Let $U_1, \ldots, U_k$, $V_1, \ldots, V_k$ be unitary matrices. Then:*

*(a)*

$$\|U_1 \cdots U_k - V_1 \cdots V_k\|_{op} \le \sum_{i=1}^{k} \|U_i - V_i\|_{op}.$$

*(b)*

$$\|U_1^* - V_1^*\|_{op} = \|U_1 - V_1\|_{op}.$$

*Proof.* Follows from properties of the operator norm (see homework). □

So to answer our question from before the lemma, if we take $V_1$ and $V_2$ so that $\|U_1 - V_1\| \leq \epsilon/2$ and $\|U_2 - V_2\| \leq \epsilon/2$, then

$$\|U_1U_2 - V_1V_2\| \leq \|U_1 - V_1\|_{op} + \|U_2 - V_2\|_{op} \leq \epsilon.$$

For the direct sum, we have

**Lemma 18.2.7.**

$$\left\|\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}\right\|_{op} = \max\{\|A\|_{op}, \|B\|_{op}\}.$$

*Proof.* If $A$ has singular values $\lambda_1, \ldots, \lambda_n$ and $B$ has singular values $\sigma_1, \ldots, \sigma_m$, then $A \oplus B$ has singular values (not ordered) $\lambda_1, \ldots, \lambda_n, \sigma_1, \ldots, \sigma_m$. □

Thus if we want to approximate $U_1 \oplus U_2$, we can take $V_i$ such that $\|U_i - V_i\|_{op} \leq \epsilon$, and then we will have

$$\left\|\begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix} - \begin{pmatrix} V_1 & 0 \\ 0 & V_2 \end{pmatrix}\right\|_{op} = \left\|\begin{pmatrix} U_1 - V_1 & 0 \\ 0 & U_2 - V_2 \end{pmatrix}\right\|_{op} \leq \max\{\|U_1 - V_1\|_{op}, \|U_2 - V_2\|_{op}\} \leq \epsilon.$$

## 18.3 Classical circuits

We would like a stronger version of Theorem 18.0.1 that shows us how to build up the elements of $U(\mathbb{C}\{0,1\}^n)$ from a small group of unitaries. To see how we might do this, it's helpful to think of how we solve this problem on a classical computer. Depending on our model of computation, we have a variety of ways to build up any given binary function $f : \{0,1\}^n \to \{0,1\}^m$ from simpler functions. One way is through circuits. To specify a logic circuit, we start by picking a list of primitive functions $f_i : \{0,1\}^{n_i} \to \{0,1\}^{m_i}$, $i = 1, \ldots, k$, which are referred to as **logic gates**. We then build up functions according to three rules:

(1) We can make the functions $f_i$, $i = 1, \ldots, k$ as well as two special gates

$$\text{SWAP} : \{0,1\}^2 \to \{0,1\}^2 : (x_1, x_2) \mapsto (x_2, x_1)$$

and

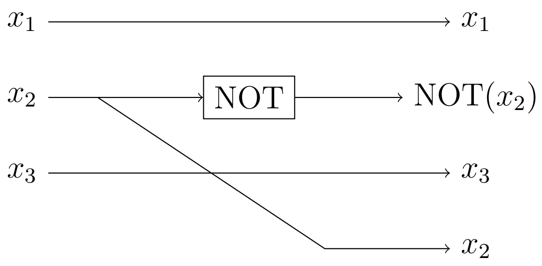
$$\text{COPY} : \{0,1\} \to \{0,1\}^2 : x \mapsto (x, x).$$

(2) If we can make functions $g : \{0,1\}^n \to \{0,1\}^m$ and $h : \{0,1\}^m \to \{0,1\}^p$, then we can make the composition $h \circ g$.

(3) If we can make a function $g : \{0,1\}^n \to \{0,1\}^m$, then for all $p \geq n$ and $1 \leq i \leq p - n + 1$, we can make the function

$$\{0,1\}^p \to \{0,1\}^{p-n+m} : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{i-1}, f(x_i, \ldots, x_{i+n-1}), x_{i+n}, \ldots, x_n).$$

A **circuit** is a type of diagram we draw to illustrate the process of building up a function according to these rules. For instance, take as a primitive gate the NOT function $\{0,1\} \to \{0,1\}$, which sends $0 \mapsto 1$ and $1 \mapsto 0$. To show how to build up the function $g : (x_1, x_2, x_3) \mapsto (x_1, \text{NOT}(x_2), x_3, x_2)$ according to the above rules, we can draw the circuit



In this circuit, the NOT gate is represented by a square box, while the COPY gate is represented by a forked arrow, and the SWAP gate is represented by two crossing arrows. Thus the above circuit diagram shows that we can build up the function $g$ form a NOT gate, a COPY gate, and a SWAP gate, as well as several applications of the other two rules.

It turns out that we can build every function $g : \{0,1\}^n \to \{0,1\}^m$ using the above rules, using only a small list of functions $f_1, \ldots, f_k$. For instance, we can take $k = 2$, $f_1 = \text{NOT}$, and $f_2 = \text{AND}$, where AND is the function $\{0,1\}^2 \to \{0,1\}$ defined by $\text{AND}(x_1, x_2) = 1$ if $x_1 = x_2 = 1$, and $\text{AND}(x_1, x_2) = 0$ otherwise. We say that NOT and AND form a **universal set of classical logic gates**. (This assumes that we include the COPY and SWAP gates. The SWAP gates alone allow us to build the function

$$\{0,1\}^n \to \{0,1\}^n : (x_1, \ldots, x_n) \mapsto \big(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\big)$$

for any $n \geq 1$ and permutation $\sigma \in S_n$.)

## 18.4 Quantum gates

To generalize the notion of classical circuits to quantum circuits, we need a notion of a quantum logic gate. The quantum analog of an $n$-bit string

$x \in \{0,1\}^n$ is a state in the quantum register $\mathbb{C}\{0,1\}^n = \mathbb{C}\{0,1\}^{\otimes n}$. Since time evolution must be reversible, there is no true analog of a general function $f : \{0,1\}^n \to \{0,1\}^m$ in a closed quantum system. However, the analog of a bijection $f : \{0,1\}^n \to \{0,1\}^n$ is a unitary transformation $\mathbb{C}\{0,1\}^n \to \mathbb{C}\{0,1\}^n$. Thus we make the following definition:

**Definition 18.4.1.** *An $n$-**qubit quantum gate** is a unitary transformation*

$$U : \mathbb{C}\{0,1\}^{\otimes n} \to \mathbb{C}\{0,1\}^{\otimes n}.$$

**Example 18.4.2.** *If $f : \{0,1\}^n \to \{0,1\}^n$ is a bijection, then we can turn $f$ into a quantum gate $U_f$ via the isomorphism $\mathbb{C}\{0,1\}^{\otimes n} \to \mathbb{C}\{0,1\}^n$ by taking*

$$U_f : \mathbb{C}\{0,1\}^n \to \mathbb{C}\{0,1\}^n : |x\rangle \mapsto |f(x)\rangle\,, x \in \{0,1\}^n$$

*and extending linearly. Since $f$ is a bijection, $U_f$ sends an orthonormal basis to an orthonormal basis, and hence $U_f$ is unitary.*

**Example 18.4.3.** *The* SWAP *and* NOT *gates define quantum gates. For instance, the* SWAP *gate is the same as the natural isomorphism*

$$\mathbb{C}\{0,1\} \otimes \mathbb{C}\{0,1\} \to \mathbb{C}\{0,1\} \otimes \mathbb{C}\{0,1\} : v \otimes w \mapsto w \otimes v.$$

*The* NOT *gate $\mathbb{C}\{0,1\} \to \mathbb{C}\{0,1\}$ sends*

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

**Example 18.4.4.** *If $U$ is an $n$-qubit quantum gate, then we defined the controlled-$U$ gate to be the $(n+1)$-qubit gate that performs $U$ conditioned on another register. Thus the controlled-$U$ gate is defined by*

$$U' : \mathbb{C}\{0,1\} \otimes \mathbb{C}\{0,1\}^n \mapsto \mathbb{C}\{0,1\} \otimes \mathbb{C}\{0,1\}^n : |a\rangle\,|x\rangle \mapsto \begin{cases} |a\rangle\,|x\rangle & a = 0 \\ |a\rangle\, U\,|x\rangle & a = 1 \end{cases}.$$

*To see that $U'$ is unitary, note that it sends the orthonormal basis*

$$\{|a\rangle\,|x\rangle : a \in \{0,1\}, x \in \{0,1\}^n\}$$

*for $\mathbb{C}\{0,1\} \otimes \mathbb{C}\{0,1\}^n$ to the orthonormal basis*

$$\{|0\rangle\,|x\rangle : x \in \{0,1\}^n\} \cup \{|1\rangle\, U\,|x\rangle : x \in \{0,1\}^n\}.$$

*To see that this latter set is an orthonormal basis, we note that it is an orthonormal set, with size equal to the dimension of $\mathbb{C}\{0,1\} \otimes \mathbb{C}\{0,1\}^n$, and hence must be a basis.*

**Example 18.4.5.** *The classical* COPY *operation goes from* $\{0,1\}$ *to* $\{0,1\}^2$*, so it doesn't give us a classical gate. We know from the no-cloning theorem that there's no true way to copy a quantum state, so copying is not a feature we can include in quantum circuits.*

*However, the controlled-*NOT *gate* CNOT *does work a bit similarly to the classical* COPY *gate, since*

$$\mathrm{CNOT}\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle \;\; \textit{and} \;\; \mathrm{CNOT}\,|1\rangle\,|0\rangle = |1\rangle \otimes \mathrm{NOT}\,|0\rangle = |1\rangle\,|1\rangle\,.$$

*So a* CNOT *gate copies classical bits into a register initialized with* $|0\rangle$*. The behaviour is different from true copying when we consider states in superposition: if* $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$*, then*

$$\mathrm{CNOT}\,|\psi\rangle\,|0\rangle = \mathrm{CNOT}\,(a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|0\rangle) = a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|1\rangle\,.$$

**Example 18.4.6.** *The* ***Hadamard gate*** *is the unitary transformation* $H : \mathbb{C}\{0,1\} \to \mathbb{C}\{0,1\}$ *which sends* $|a\rangle \mapsto |0\rangle + (-1)^a\,|1\rangle$ *for* $a \in \{0,1\}$*. In other words,* $H\,|0\rangle = |+\rangle$ *and* $H\,|1\rangle = |-\rangle$*. Since* $H$ *creates superpositions,* $H$ *is a very important gate in quantum information.*

**Example 18.4.7.** *Let* $\theta \in \mathbb{R}$*. The phase shift gate* $P_\theta : \mathbb{C}\{0,1\} \to \mathbb{C}\{0,1\}$ *sends*

$$|0\rangle \mapsto |0\rangle \;\; \textit{and} \;\; |1\rangle \mapsto e^{i\theta}\,|1\rangle\,.$$

## 18.5 Quantum circuits

The key idea behind classical circuits is that if we have a gate with $n$ inputs, we can apply it to a substring of any $p$-bit string with $p \geq n$. We can do the same thing with quantum gates. If $U$ is an $n$-qubit gate, $p \geq n$, and $1 \leq i \leq p-n+1$, then the unitary which applies $U$ to the $i$th to $(i+n-1)$th qubits is

$$\mathbb{1}^{\otimes i-1} \otimes U \otimes \mathbb{1}^{p-n-i+1}$$

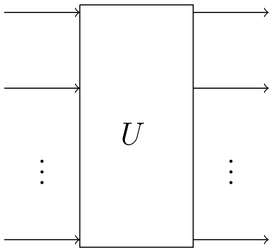
where $\mathbb{1}$ is the identity operator $\mathbb{C}\{0,1\} \to \mathbb{C}\{0,1\}$.

**Example 18.5.1.** *If we apply the* CNOT *gate to the* 2 *and* 3 *qubit of a* 4*-qubit register, we get the unitary operation* $\mathbb{1} \otimes \mathrm{CNOT} \otimes \mathbb{1} : \mathbb{C}\{0,1\}^{\otimes 4} \to \mathbb{C}\{0,1\}^{\otimes 4}$*. This sends*

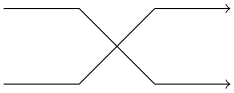
$$|a0bc\rangle \mapsto |a0bc\rangle\,, |a10c\rangle \mapsto |a11c\rangle\,, \;\; \textit{and} \;\; |a11c\rangle \mapsto |a10c\rangle$$

*for all* $a, b, c \in \{0,1\}$*.*

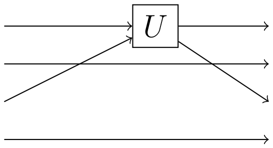
With this convention, we can write down and work with quantum circuits in the same way that we work with classical circuits. A wire in a classical circuit corresponds to a bit register, so a wire in a quantum circuit corresponds to a qubit register. We denote an $n$-qubit gate $U$ by a rectangle with $n$ wires entering and leaving:



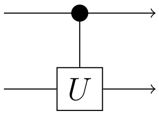
While we don't have COPY gates, we still have the SWAP gates, and these are still represented by crossing wires as before:



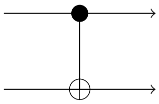
By taking $\mathbb{1} \otimes U \otimes \mathbb{1}$, we can apply an $n$-qubit gate to a consecutive substring of qubits of a $p$-qubit register for any $p \geq n$. Using swap gates, we can apply $U$ to any subset of qubits. For instance, to apply a two qubit gate $U$ to the first and third qubit of a 4-qubit register, we can take the circuit



Other gates also have special notation. For instance, the controlled $U$ gate is written as



The CNOT gate is drawn as



From a circuit, we can compile a unitary $U$. We are not going to explicitly define how to turn a circuit into a unitary, although hopefully this is clear from examples. However, we can give a formal definition for the unitaries that arise in this way:

**Definition 18.5.2.** *A unitary $U \in U(\mathbb{C}\{0,1\}^{\otimes n}$ can be* ***constructed from a quantum circuit with gates*** *$U_1, \dots, U_k$, where $U_i \in U(\mathbb{C}\{0,1\}^{\otimes n_i})$, if either*

*(1) $U$ is one of $U_1, \dots, U_k$, or the* SWAP *gate $\mathbb{C}\{0,1\}^{\otimes 2} \to \mathbb{C}\{0,1\}^{\otimes 2}$,*

*(2) $U = V_1V_2$, where $V_1$ and $V_2$ are unitaries which can be constructed from a quantum circuit using $U_1, \dots, U_k$, or*

*(3) $n = a + m + b$ for $a, m, b \geq 0$, and $U = \mathbb{1}_1 \otimes U' \otimes \mathbb{1}_2$, where $U' \in U(\mathbb{C}\{0,1\}^{\otimes m}$ can be constructed from a quantum circuit using $U_1, \dots, U_k$, and $\mathbb{1}_1$ and $\mathbb{1}_2$ are the identity maps $\mathbb{C}\{0,1\}^{\otimes a} \to \mathbb{C}\{0,1\}^{\otimes a}$ and $\mathbb{C}\{0,1\}^{\otimes b} \to \mathbb{C}\{0,1\}^{\otimes b}$ respectively.*

Although this definition doesn't refer to diagrams, the diagrams are the most important part of the concept of quantum circuits. Diagrams of this form are sometimes called **tensor diagrams** or **wiring diagrams**, and are used throughout mathematics.

Note that there can be more than one way to get any given unitary from a circuit. For instance, we can get a permutation of registers in multiple ways by taking different combinations of SWAP gates.

**Lemma 18.5.3.** *Let $S$ be a set of gates which is closed under taking inverses. Then the $n$-qubit unitaries which can be constructed from $S$ form a matrix subgroup of $U(\mathbb{C}\{0,1\}^{\otimes n})$.*

**Definition 18.5.4.** *We say that a set of gates $S$ is* ***universal*** *if there is some $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, the subgroup of $n$-qubit unitaries which can be constructed from gates in $S$ and their inverses is dense in $U(\mathbb{C}\{0,1\}^{\otimes n}$.*

*A set of gates $S$ is* ***universal up to global phase*** *if there is some $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ and $U \in \mathcal{U}(\mathbb{C}\{0,1\}^{\otimes n})$, such that the closure of the subgroup of $n$-qubit unitaries which can be constructed from gates in $S$ and their inverses contains $e^{i\theta U}$ for some $\theta \in \mathbb{R}$.*

There are different notions of universality. These are two of them. We'll look at a stronger notion of universality in the next section.

**Theorem 18.5.5.** *The Hadamard gate $H$,* CNOT *gate, and $\pi/8$ gate $T := P_{\pi/4}$ are universal, up to global phase.*

The point of Theorem 18.5.5 is that very small sets of gates can be universal. We won't prove Theorem 18.5.5, but we will prove the following:

**Theorem 18.5.6.** *Let $\alpha$ and $\theta$ be irrational numbers. Then the gates* CNOT*, $R_{\pi\theta}$,* NOT*, and $P_{\pi\alpha}$ are universal, with $n_0 = 1$.*

## 18.6 Exact universality of CNOT and one-qubit gates

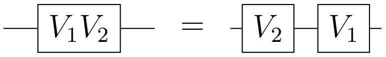
To prove Theorem 18.5.5, we first look at a stronger notion of universality.

**Definition 18.6.1.** *We say that a set of gates $S$ is* ***exactly universal*** *if for every $n \geq 1$ and $U \in \mathcal{U}(\mathbb{C}\{0,1\}^n)$, the unitary $U$ can be constructed from a quantum circuit using gates from $S$.*

**Theorem 18.6.2.** *The set of all one-qubit gates along with* CNOT *is exactly universal.*

**Just for this section**, we let $S$ be the set of one-qubit gates plus CNOT, and we say that a unitary can be **constructed** if it can be constructed from a quantum circuit using gates from $S$.

We'll build up to the proof of Theorem 18.6.2 in a sequence of lemmas. Note that one of the basics of quantum circuits (reflected in part (2) of Definition 18.5.2 is that if $V_1$ and $V_2$ are two elements in $U(\mathbb{C}\{0,1\}^n)$ which can be constructed from quantum circuits using gates from $S$, then $V_1V_2$ can be constructed from a quantum circuit using gates from $S$. To depict this pictorially, we say that

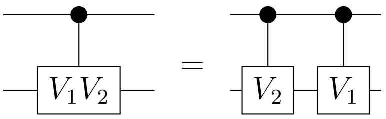


Although the input to the gates in this diagram should consist of $n$ wires, for convenience we often draw many wires as a single wire. We can think of the single wire as carrying $n$-qubits, rather than a single qubit. To construct the circuit for $V_1V_2$, we can replace the boxes on the right in the above diagram by the circuits for $V_2$ and $V_1$.

Our first lemma shows that we can do something similar for Controlled-$U$ operations.

**Lemma 18.6.3.** *Suppose we can construct Controlled-$V_1$ and Controlled-$V_2$ for $V_1, V_2 \in \mathcal{U}(\mathbb{C}\{0,1\}^{\otimes n})$. Then we can construct Controlled-$V_1V_2$.*

*Proof.*



□

We won't really use the following lemma, but while we're covering basic facts, we note:

**Lemma 18.6.4.** *If we can construct $U$, then we can construct $U^*$.*

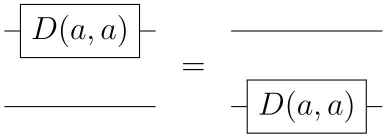
*Proof.* The CNOT gate is its one inverse, while the set of one-qubit gates is closed under taking inverses. So given a circuit for $U$, we can make a circuit for $U^*$ by reversing the circuit, and replacing every one-qubit gate with its inverse. □

Let $R_\theta$ and $D(a,b)$ denote the one-qubit gates with matrices

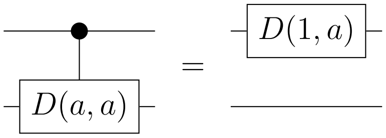
$$\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix} \text{ and } \begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}$$

in computational basis $\{|0\rangle, |1\rangle\}$. When referring to $D(a,b)$, we assume that $a$ and $b$ are complex numbers with $|a| = |b| = 1$, so that $D(a,b)$ is unitary.

**Lemma 18.6.5.** *$D(a,a)$ commutes with any other one-qubit gate. Also*



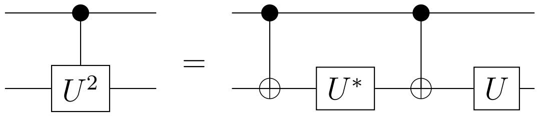
*and*



*In particular, we can construct Controlled-$D(a,a)$.*

**Lemma 18.6.6.** *Suppose $U$ is a one-qubit gate such that* $\mathrm{NOT}\, U^*\, \mathrm{NOT} = U$*. Then we can construct Controlled-$U^2$.*

*Proof.*



□

Since $\mathrm{NOT}^* = \mathrm{NOT}$, note that $\mathrm{NOT}\, U^*\, \mathrm{NOT} = U$ if and only if $\mathrm{NOT}\, U\, \mathrm{NOT} = U^*$. The matrix of NOT in the computational basis is

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Also, since $R_\theta R_{-\theta} = R_0 = \mathbb{1}$, $R_\theta^* = R_{-\theta}$.

**Lemma 18.6.7.** $\mathrm{NOT}\, R_\theta\, \mathrm{NOT} = R_{-\theta} = R_\theta^*$ *and* $\mathrm{NOT}\, D(a,a^{-1})\, \mathrm{NOT} = D(a^{-1},a) = D(a,a^{-1})^*$*. As a result, we can construct Controlled-$R_\theta$ for any $\theta \in \mathbb{R}$ and and Controlled-$D(a,a^{-1})$ for any complex number $a$ of norm $1$.*

*Proof.* The first part of the lemma follows immediately from looking at matrices: conjugating by NOT switches the rows and columns (this is a special case of Lemma 18.2.4).

For the second part of the lemma, suppose we are given $\theta \in \mathbb{R}$. Then using the first part of the lemma, NOT $R^*_{\theta/2}$ NOT $= R_{\theta/2}$, so we can construct Controlled-$R^2_{\theta/2}$ by Lemma 18.6.6. But $R^2_{\theta/2} = R_\theta$.

Similarly, if $a$ is a complex number of norm 1, then $a$ has a square root $\sqrt{a}$. Using the first part of this lemma as well as Lemma 18.6.6, we see that we can implement Controlled-$D(\sqrt{a}, \sqrt{a}^{-1})^2$, and $D(\sqrt{a}, \sqrt{a}^{-1})^2 = D(a, a^{-1})$. □

**Corollary 18.6.8.** *We can construct Controlled-$U$ for any* 1*-qubit gate* $U$*.*

*Proof.* By Lemma 18.1.3, if $U$ is a one-qubit gate, then there are $\theta, \psi_1, \psi_2, \psi_3, \psi_4 \in \mathbb{R}$ such that

$$U = D(e^{i\psi_1}, e^{i\psi_2}) \cdot R_\theta \cdot D(e^{i\psi_3}, e^{i\psi_4}).$$

If we set $a = e^{i(\psi_1+\psi_2)/2}$, and $b = e^{i(\psi_1-\psi_2)/2}$, then

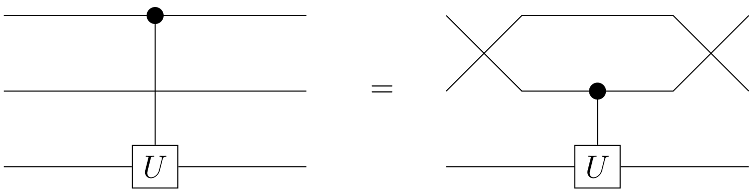
$$D(e^{i\psi_1}, e^{i\psi_2}) = D(a, a)D(b, b^{-1}).$$

Similarly, if $c = e^{i(\psi_3+\psi_4)}$ and $d = e^{i(\psi_3-\psi_4)}$, then

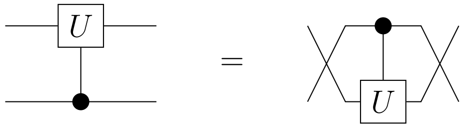
$$D(e^{i\psi_3}, e^{i\psi_4}) = D(c, c)D(d, d^{-1}).$$

By Lemmas 18.6.5 and 18.6.7, we can construct Controlled-$V$ for $V = D(a, a)$, $D(b, b^{-1})$, $R_\theta$, $D(c, c)$, and $D(d, d^{-1})$. By Lemma 18.6.3, we can construct Controlled-$U$. □

When working with Controlled-$U$ gates, we allow ourselves to place the $U$ and control gate on any wires, as we can turn any such circuit into a standard Controlled-$U$ gate by using SWAP gates. For instance, we have



and



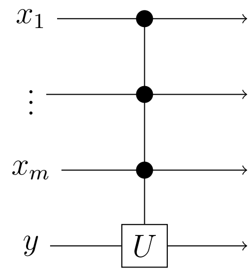
We can also generalize Controlled-$U$ gates to add more control bits.

**Definition 18.6.9.** *Let $U$ be an $n$-qubit gate. The Controlled(m)-$U$ gate is an $(m+n)$-qubit gate that sends*

$$|x\rangle\,|y\rangle \mapsto \begin{cases} |x\rangle\,U\,|y\rangle & x_1 = x_2 = \ldots = x_m = 1 \\ |x\rangle\,|y\rangle & \text{otherwise} \end{cases}$$

*for all $x \in \{0,1\}^m$ and $y \in \{0,1\}^n$.*

Clearly the usual Controlled-$U$ gate is Controlled(1)-$U$. The Controlled(m)-$U$ gate is represented by the following diagram:

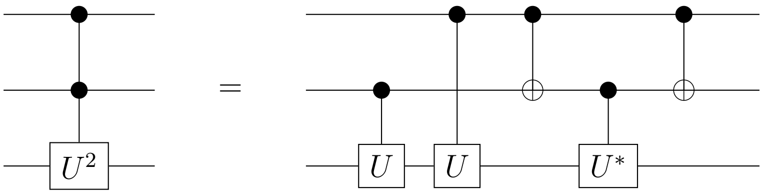


**Lemma 18.6.10.** *Let $U$ be an $n$-qubit gate.*

*(a) For every $m \geq 2$, we have*

$$\textit{Controlled}(m) - U = \textit{Controlled} - (\textit{Controlled}(m-1)(U)).$$

*(b)*



*Proof.* Both parts are clear. □

If $M$ is a matrix, then a square root of $M$ is a matrix $X$ such that $X^2 = M$.

**Lemma 18.6.11.** *All unitary matrices $U \in \mathcal{U}(H)$ have square roots.*

*Proof.* We can assume that $H = \mathbb{C}^n$ for some $n$. Since $U$ is unitary, $U$ is normal, so $U$ is unitarily diagonalizable. This means that there is a unitary matrix $V$ such that $V^*UV = D$, where $D$ is a diagonal matrix. Since $D$ is unitary, $D$ must be of the form

$$D = \begin{pmatrix} e^{i\theta_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & e^{i\theta_n} \end{pmatrix}$$

for some real numbers $\theta_1, \ldots, \theta_n$. Set

$$F = \begin{pmatrix} e^{i\theta_1/2} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & e^{i\theta_n/2} \end{pmatrix},$$

so $F^2 = D$, and let $X = VFV^*$. Then

$$X^2 = VFV^*VFV^* = VF^2V^* = VDV^* = U.$$

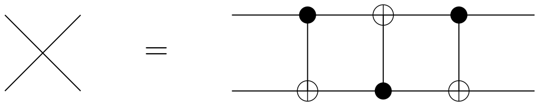
□

**Lemma 18.6.12.** *We can construct Controlled(2)-U for any one-qubit gate $U$.*

*Proof.* By Lemma 18.6.11, $U$ has a square root $V$. Since $V$ is a one-qubit gate, we can construct Controlled-$V$ and Controlled-$V^*$ by Lemma 18.6.8. By Lemma 18.6.10, part(b), we can construct Controlled(2)-$V^2$, and $V^2 = U$. □

We are almost ready to prove our main intermediate step. We need one more lemma about Controlled-$U$ gates:

**Lemma 18.6.13.**



*As a result, we can construct Controlled-SWAP.*

*Proof.* The CNOT gate in the usual configuration sends $|a\rangle\,|b\rangle$ to $|a\rangle\,|a \oplus b\rangle$, where $a \oplus b$ denotes $a + b \mod 2$. As a result, if we plug $|a\rangle\,|b\rangle$ into the circuit on the right, we get $|a\rangle\,|a \oplus b\rangle$ after the first CNOT, $|b\rangle\,|a \oplus b\rangle$ after the second CNOT, and $|b\rangle\,|a\rangle$ after the third CNOT. So the three CNOT gates give us the SWAP gate.

Now using Lemma 18.6.3, Controlled-SWAP is the product of three Controlled(2)-NOT gates. By Lemma 18.6.12, we can construct ControlledS(2)-NOT. □

Note a subtlety of Lemma 18.6.13 is that we need SWAP gates to construct Controlled-SWAP; we can't completely replace SWAP with CNOT gates. This is because we use SWAP gates implicitly in Lemma 18.6.12 to implement CNOT gates on non-adjacent wires. We also need SWAP gates to implement the upside-down CNOT in Lemma 18.6.13. However, when constructing Controlled-SWAP, if we replace the upside-down CNOT with SWAP gates and a regular CNOT before applying Lemma 18.6.12, we get a circular argument. Thus we first use Lemma 18.6.12 to construct a Controlled(2)-NOT with one of the controls on the bottom wire. Then we put the SWAP gates in at the end to get a regular CNOT gate.

We are now ready for the main step of our proof.

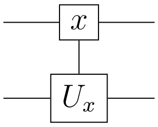
**Proposition 18.6.14.** *If we can construct $U$, then we can construct Controlled(m)-$U$ for any $m \geq 1$.*

*Proof.* By Lemma 18.6.10, part (a), it is enough to show that we can construct Controlled-$U$. For this, suppose we have a circuit representing $U$, made up of one-qubit gates, SWAP gates, and CNOT gates. Applying Lemma 18.6.3 in reverse, we get a circuit for Controlled-$U$ consisting of controlled one-qubit gates, SWAP gates, and CNOT gates. By Lemmas 18.6.8, 18.6.12, and 18.6.13, we can construct the controlled versions of all of these gates, so we get a circuit for Controlled-$U$. □

If we apply this proof naively to construct circuits for Controlled(m)-$U$, we get very large circuits. This is because to construct Controlled-$U$, we replace every SWAP gate in the circuit for $U$ with 3 CNOT gates, and then expand the resulting Controlled(2)-NOT gates into a circuit which involves lots of SWAPs. When we make Controlled(2)-$U$, we then have to replace all the new SWAPs with 3 CNOT gates, and the circuit expands accordingly. To minimize the number of SWAP gates we create, we can construct a circuit for Controlled(m)-$U$ which uses CNOT gates on non-adjacent wires, and then add in the SWAP gates at the end.

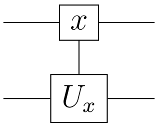
We need one more concept to finish the proof.

**Definition 18.6.15.** *Let $\{U_x\}_{x \in \{0,1\}^m}$ be a family of $n$-qubit unitaries, indexed by $m$-bit strings. The multiplexed gate*

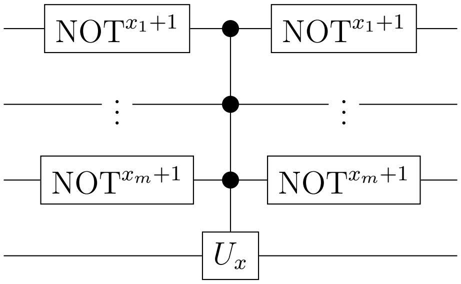


*is the $(m+n)$-qubit gate sending $|x\rangle\,|y\rangle \mapsto |x\rangle\,U_x\,|y\rangle$.*

**Lemma 18.6.16.** *Let $\{U_x\}_{x\in\{0,1\}^m}$ be a family of $n$-qubit unitaries indexed by $m$-bit strings, and suppose we can construct Controlled(m)-$U_x$ for every $x \in \{0,1\}^m$. Then we can construct the multiplexed gate*



*Proof.* Let NOT$^a$ denote the linear operator NOT taken to the $a$th power, where $a \in \{0,1\}$. Then



sends

$$|z\rangle\,|y\rangle \mapsto \begin{cases} |x\rangle\, U_x\, |y\rangle & z = x \\ |z\rangle\,|y\rangle & z \neq x \end{cases}.$$

By concatenating these circuits, we can form the multiplexed gate for $\{U_x\}$. □

*Proof of Theorem 18.6.2.* The proof is by induction on $n$, the number of qubits. Clearly we can construct any one-qubit gate. Suppose $U \in \mathcal{U}(\mathbb{C}\{0,1\}^n)$, and that we can construct any element of $\mathcal{U}(\mathbb{C}\{0,1\}^{n-1})$. Let $\mathcal{B}$ be the computational basis of $\mathbb{C}\{0,1\}^n$, ordered in increasing lexicographic order (this is the same order we get if we regard $n$-bit strings as integers expressed in binary, and order them in increasing order). Let

$$[U]_{\mathcal{B}} = \begin{pmatrix} U_0 & 0 \\ 0 & U_1 \end{pmatrix} \begin{pmatrix} C & -S \\ S & C \end{pmatrix} \begin{pmatrix} V_0^* & 0 \\ 0 & V_1^* \end{pmatrix}$$

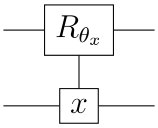
be the CS decomposition of $U$. Consider the matrix $L = \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix}$. Note that the blocks of this matrix correspond to the decomposition of $\mathcal{B}$ into the sets $\{|0\rangle\,|x\rangle : x \in \{0,1\}^{n-1}\}$ and $\{|1\rangle\,|x\rangle : x \in \{0,1\}^{n-1}\}$. Abusing notation, we can regard $U_0$ and $U_1$ as unitary transformations of $\mathbb{C}\{0,1\}^{n-1}$, and the matrix

$L$ is then the matrix of the multiplexed gate for the family $\{U_0, U_1\}$. Similarly, $\begin{pmatrix} V_0^* & 0 \\ 0 & V_1^* \end{pmatrix}$ is the multiplexed gate for the family $\{V_0^*, V_1^*\}$ on $\mathbb{C}\{0,1\}^{n-1}$. By the inductive hypothesis, we can construct $U_0$, $U_1$, $V_0^*$, and $V_1^*$. By Proposition 18.6.14 and Lemma 18.6.16, we can construct the multiplexed gate for the families $\{U_0, U_1\}$ and $\{V_0^*, V_1^*\}$.

Recall that we can write

$$\begin{pmatrix} C & -S \\ S & C \end{pmatrix} = \begin{pmatrix} \cos\theta_0 & 0 & \dots & 0 & -\sin\theta_0 & 0 & \dots & 0 \\ 0 & \cos\theta_1 & & 0 & 0 & -\sin\theta_1 & & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & \cos\theta_{2^{n-1}-1} & 0 & 0 & \dots & -\sin\theta_{2^{n-1}-1} \\ \sin\theta_0 & 0 & \dots & 0 & \cos\theta_0 & 0 & \dots & 0 \\ 0 & \sin\theta_1 & & 0 & 0 & \cos\theta_1 & & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & \sin\theta_{2^{n-1}-1} & 0 & 0 & \dots & \cos\theta_{2^{n-1}-1}\} \end{pmatrix}.$$

The row and columns of this matrix involving $\theta_1$ correspond to the basis elements $|0\rangle\,|0\cdots 0\rangle$ and $|1\rangle\,|0\cdots 0\rangle$. Similarly, the rows and colums of the matrix involving $\theta_2$ correspond to the basis elements $|0\rangle\,|0\cdots 01\rangle$ and $|1\rangle\,|0\cdots 01\rangle$, and in general, the rows and columns involving $\theta_x$ correspond to the basis elements $|0\rangle\,|x\rangle$ and $|1\rangle\,|x\rangle$, where the number $x$ is expressed as an $(n-1)$-bit string in binary. Abusing notation again, let $R_{\theta_x}$ denote the unitary transformation of $\mathbb{C}\{0,1\}$ with matrix $R_{\theta_x}$. Then we see that the matrix $\begin{pmatrix} C & -S \\ S & C \end{pmatrix}$ corresponds to the multiplexed gate



Thus we can construct this gate as well. □

*Proof of Theorem 18.5.6.* We've already shown that $R_{\pi\theta}$, NOT, and $P_{\alpha\pi}$ generate a dense subgroup of $U(\mathbb{C}\{0,1\})$. Given $U \in U(\mathbb{C}\{0,1\}^n)$, find a circuit for $U$ consisting of CNOT's and one-qubit gates. Since we can approximate each one-qubit gate in this circuit with $R_{\pi\theta}$, NOT, and $P_{\alpha\pi}$, we can approximate $U$ with these gates and CNOT. □